

# Contents

## Microsoft compliance offerings

### Microsoft compliance offerings

#### Global

CIS Benchmark

CSA-STAR attestation

CSA-STAR certification

CSA-STAR self-assessment

ISO - Recommended action plan

ISO 20000-1-2011

ISO 22301

ISO 27001

ISO 27017

ISO 27018

ISO 27701

ISO-9001

SOC

WCAG

#### US Government

CJIS

CNSSI 1253

DFARS

DoD DISA L2,L4,L5

DoE 10 CFR Part 810

EAR (US Export Admin. Reg.)

FedRAMP

FIPS 140-2

IRS 1075

ITAR

NIST - Recommended action plan

NIST 800-171

NIST CSF

Section 508 VPATS

## Industry

Education

FERPA

Energy

NERC

Financial

23 NYCRR Part 500

AFM + DNB (Netherlands)

APRA (Australia)

AMF and ACPR (France)

CFTC 1.31 (US)

EBA (EU)

FCA (UK)

FFIEC (US)

FINMA (Switzerland)

FINRA 4511

FISC (Japan)

FSA (Denmark)

GLBA

KNF (Poland)

MAS + ABS (Singapore)

NBB + FSMA (Belgium)

OSFI (Canada)

PCI DSS

RBI + IRDAI (India)

SEC 17a-4

SEC Regulation SCI

SOC

SOX

TruSight

## Health

HDS (France)

HIPAA/HITECH

HITRUST

MARS-E

NEN-7510 (Netherlands)

## Manufacturing

FDA CFR Title 21 Part 11

GxP

TISAX (Germany)

## Media

CDSA

DPP (UK)

FACT (UK)

MPAA

## Retail

23 NYCRR Part 500

AFM + DNB (Netherlands)

AMF and ACPR (France)

CDSA

CIS Benchmark

CSA-STAR attestation

DoE 10 CFR Part 810

DPP (UK)

EAR (US Export Admin. Reg.)

ENISA IAF (EU)

EU Model Clauses

EBA (EU)

EU U.S. Privacy Shield

FACT (UK)

FCA (UK)

FFIEC (US)  
FINMA (Switzerland)  
GLBA  
HITRUST  
IRS 1075  
ISO 27018  
ISO-9001  
ITAR  
KNF (Poland)  
MARS-E  
MPAA  
NBB + FSMA (Belgium)  
NIST CSF  
PCI DSS  
Section 508 VPATS  
Shared Assessments  
SOC  
LOPD (Spain)  
Cyber Essentials Plus (UK)  
G-Cloud (UK)

## Regional

### Asia

ABS OSPAR (Singapore)  
CS Mark (Gold) (Japan)  
DJCP (China)  
GB 18030 (China)  
ISMS (Korea)  
MeitY (India)  
MTCS (Singapore)  
My Number (Japan)  
TRUCS (China)

### Australia / Pacific

APRA (Australia)

IRAP (Australia)

NZ CC Framework (New Zealand)

## Europe

BIR 2012 (Netherlands)

C5 (Germany)

Cyber Essentials Plus (UK)

EN 301 549 (EU)

ENS (Spain)

ENISA IAF (EU)

EU Model Clauses

EU U.S. Privacy Shield

G-Cloud (UK)

IDW PS 951 (Germany)

IT Grundschutz Workbook (Germany)

LOPD (Spain)

PASF (UK)

Personal Data Localization (Russia)

## North America

California Consumer Privacy Act (CCPA)

Canadian Privacy Laws

## South America

PDPA (Argentina)

## General Data Protection Regulation (GDPR)

GDPR overview

Recommended action plan for GDPR

Information protection for GDPR

Microsoft's data protection officer

Accountability readiness checklists

Accountability readiness checklists

Azure and Dynamics 365

Microsoft Support & Professional Services

Office 365

Data subject requests

Data subject requests

Manage data subject requests with the DSR case tool

Azure

Azure DevOps services

Dynamics 365

Intune

Microsoft Support & Professional Services

Office 365

Visual Studio family

Windows Enterprise

Breach notification

Breach notification

Azure & Dynamics 365

Microsoft Support & Professional Services

Office 365

Windows Enterprise

Data protection impact statements

Data protection impact assessments

Azure

Dynamics 365

Microsoft Support & Professional Services

Office 365

Windows Enterprise

GDPR for on-premises Office servers

GDPR for on-premises Office servers

GDPR for SharePoint Server

GDPR for Exchange Server

GDPR for Skype for Business Server & Lync Server

GDPR for Project Server

GDPR for Office Web Apps Server & Office Online Server

[GDPR for on-premises Windows Server file shares](#)

[Additional steps to export data](#)

[GDPR for Office 365 dev/test environments](#)

[California Consumer Privacy Act \(CCPA\)](#)

[CCPA - Frequently asked questions](#)





# Center for Internet Security (CIS) Benchmarks

2/5/2021 • 4 minutes to read • [Edit Online](#)

## About CIS Benchmarks

The [Center for Internet Security](#) is a nonprofit entity whose mission is to 'identify, develop, validate, promote, and sustain best practice solutions for cyberdefense.' It draws on the expertise of cybersecurity and IT professionals from government, business, and academia from around the world. To develop standards and best practices, including CIS benchmarks, controls, and hardened images, they follow a consensus decision-making model.

[CIS benchmarks](#) are configuration baselines and best practices for securely configuring a system. Each of the guidance recommendations references one or more [CIS controls](#) that were developed to help organizations improve their cyberdefense capabilities. CIS controls map to many established standards and regulatory frameworks, including the NIST Cybersecurity Framework (CSF) and NIST SP 800-53, the ISO 27000 series of standards, PCI DSS, HIPAA, and others.

Each benchmark undergoes two phases of consensus review. The first occurs during initial development when experts convene to discuss, create, and test working drafts until they reach consensus on the benchmark. During the second phase, after the benchmark has been published, the consensus team reviews the feedback from the internet community for incorporation into the benchmark.

CIS benchmarks provide two levels of security settings:

- **Level 1** recommends essential basic security requirements that can be configured on any system and should cause little or no interruption of service or reduced functionality.
- **Level 2** recommends security settings for environments requiring greater security that could result in some reduced functionality.

[CIS Hardened Images](#) are securely configured virtual machine images based on CIS Benchmarks hardened to either a Level 1 or Level 2 CIS benchmark profile. Hardening is a process that helps protect against unauthorized access, denial of service, and other cyberthreats by limiting potential weaknesses that make systems vulnerable to cyberattacks.

## Microsoft and the CIS Benchmarks

The Center for Internet Security (CIS) has published benchmarks for Microsoft products and services including the Microsoft Azure and Microsoft 365 Foundations Benchmarks, the Windows 10 Benchmark, and the Windows Server 2016 Benchmark.

CIS benchmarks are internationally recognized as security standards for defending IT systems and data against cyberattacks. Used by thousands of businesses, they offer prescriptive guidance for establishing a secure baseline configuration. System and application administrators, security specialists, and others who develop solutions using Microsoft products and services can use these best practices to assess and improve the security of their applications.

Like all CIS benchmarks, the Microsoft benchmarks were created using a consensus review process based on input from subject matter experts with diverse backgrounds spanning software development, audit and compliance, security research, operations, government, and law. Microsoft was an integral partner in these CIS efforts. For example, Office 365 was tested against the listed services, and the resulting Microsoft 365 Foundations Benchmark covers a broad range of recommendations for setting appropriate security policies that cover account and authentication, data management, application permissions, storage, and other security policy

areas.

In addition to the benchmarks for Microsoft products and services, CIS has also published [CIS Hardened Images for use on Azure virtual machines](#) configured to meet CIS benchmarks. These include the CIS Hardened Image for Microsoft Windows Server 2016 certified to run on Azure. CIS states that, 'All CIS hardened images that are available on the [Azure Marketplace](#) are certified to run on Azure. They have been pre-tested for readiness and compatibility with the Azure public cloud, the Microsoft Cloud Platform hosted by service providers through the Cloud OS Network, and on-premise private cloud Windows Server Hyper-V deployments managed by customers.'

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- [Office and Microsoft 365](#)
- SQL Server
- Windows 10
- Windows Server 2016

## Audits, reports, and certificates

Get a [complete list of CIS benchmarks](#) for Microsoft products and services.

- [CIS Azure Foundations Benchmark](#)
- [CIS Microsoft 365 Foundations Benchmark](#)
- [Windows 10 Benchmark](#)
- [Windows Server 2016 Benchmark](#)

## How to implement

- [CIS Benchmark for Azure](#): Get prescriptive guidance for establishing a secure baseline configuration for Azure.
- [Microsoft 365 security roadmap](#): Minimize the potential of a data breach or compromised account by following this roadmap.
- [Windows security baselines](#): Follow these guidelines for effective use of security baselines in your organization.
- [CIS Controls Cloud Companion Guide](#): Get guidance on applying security best practices in CIS Controls Version 7 to cloud environments.

## Frequently asked questions

### Will following CIS Benchmark settings ensure the security of my applications?

CIS benchmarks establish the basic level of security for anyone adopting in-scope Microsoft products and services. However, they should not be considered as an exhaustive list of all possible security configurations and architecture but as a starting point. Each organization must still evaluate its specific situation, workloads, and compliance requirements and tailor its environment accordingly.

### How often are CIS Benchmarks updated?

The release of revised CIS Benchmarks changes depending on the community of IT professionals who developed it and on the release schedule of the technology the benchmark supports. CIS distributes monthly reports that announce new benchmarks and updates to existing benchmarks. To receive these, register for the [CIS Workbench](#) (it's free) and check Receive newsletter in your profile.

## Who contributed to the development of Microsoft CIS Benchmarks?

CIS notes that its 'Benchmarks are developed through the generous volunteer efforts of subject matter experts, technology vendors, public and private CIS Benchmark community members, and the CIS Benchmark Development team.' For example, you'll find a list of Azure contributors on [CIS Microsoft Azure Foundations Benchmark v1.0.0 Now Available](#).

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [CIS best practices for securely using Microsoft 365](#)
- [Windows 10 security policy settings](#)
- [Windows 10 enterprise security](#)
- [Compliance on the Microsoft Trust Center](#)

# Cloud Security Alliance (CSA) STAR attestation

2/17/2021 • 3 minutes to read • [Edit Online](#)

## CSA STAR attestation overview

The Cloud Security Alliance (CSA) maintains the Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry where cloud service providers (CSPs) can publish their CSA-related assessments. STAR consists of three levels of assurance aligned with control objectives in the CSA Cloud Controls Matrix (CCM). (The CCM covers fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a cloud service.):

- Level 1: STAR Self-Assessment
- Level 2: STAR Attestation, STAR Certification, and C-STAR Assessment (which are based on audits by third parties)
- Level 3: STAR Continuous Monitoring (program requirements are still under development by CSA)

STAR Attestation involves a rigorous independent audit of a cloud provider's security posture based on a SOC 2 Type 2 audit with CCM criteria. The independent auditor that evaluates a cloud provider's offerings for STAR Attestation must be a certified public accountant (CPA) and is required to have the CSA Certificate in Cloud Security Knowledge (CCSK).

A SOC 2 Type 2 audit is based on American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria, including security, availability, confidentiality, and processing integrity, and the criteria in the CCM. STAR Attestation provides an auditor's findings on the design suitability and operating effectiveness of SOC 2 controls in Microsoft cloud services. The objective is to meet both the AICPA criteria mentioned above and requirements set forth in the CCM.

## Microsoft in-scope cloud services

Microsoft Azure and Microsoft Intune have been awarded CSA STAR Attestation. STAR Attestation provides an auditor's findings on the design suitability and operating effectiveness of SOC 2 controls in Microsoft cloud services.

- [Azure and Azure Government](#)
- [Azure Germany](#)
- Microsoft Cloud App Security
- Microsoft Graph
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI

## Audits, reports, and certificates

- [CSA STAR Attestation and Certification](#)

# Frequently asked questions

## Which industry standards does the CSA CCM align with?

The CCM corresponds to industry-accepted security standards, regulations, and control frameworks such as ISO/IEC 27001, PCI DSS, HIPAA, AICPA SOC 2, NERC CIP, FedRAMP, NIST, and many more. For the most current list, visit the [CSA website](#).

## Where can I see the CSA STAR Attestation for Microsoft cloud services?

You can download the [CSA STAR Attestation](#) for Azure, which also covers Intune, from the CSA Registry.

## Which CSA STAR levels of assurance have Microsoft business cloud services attained?

- **Level 1: CSA STAR Self-Assessment:** Azure, Microsoft Dynamics 365, and Microsoft Office 365. The [Self-Assessment](#) is a complimentary offering from cloud service providers to document their security controls to help customers assess the security of the service.
- **Level 2: CSA STAR Certification:** Azure, Microsoft Cloud App Security, Intune, and Microsoft Power BI. STAR Certification is based on achieving ISO/IEC 27001 certification and meeting criteria specified in the CCM. It is awarded after a rigorous third-party assessment of the security controls and practices of a cloud service provider.
- **Level 2: CSA STAR Attestation:** Azure and Intune. CSA and the AICPA have collaborated to provide guidelines for CPAs to use in conducting SOC 2 engagements, using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA CCM. [STAR Attestation](#) is based on these guidelines and is awarded after rigorous independent assessments of cloud providers.

# Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Azure standard response for request for information](#)
- [Azure Cloud Security Alliance CAIQ](#)
- [Office 365 Mapping of CSA Cloud Control Matrix](#)
- [Cloud Security Alliance](#)
- [CSA Security, Trust & Assurance Registry \(STAR\)](#)
- [SOC 1, 2, and 3 Reports](#)
- [Cloud Controls Matrix \(CCM\)](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Compliance on the Microsoft Trust Center](#)

# Cloud Security Alliance (CSA) STAR certification

2/17/2021 • 3 minutes to read • [Edit Online](#)

## CSA STAR certification overview

The Cloud Security Alliance (CSA) maintains the Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry where cloud service providers can publish their CSA-related assessments. STAR consists of three levels of assurance aligned with the control objectives in the CSA Cloud Controls Matrix (CCM). (The CCM covers fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a cloud service.)

- Level 1: STAR Self-Assessment
- Level 2: STAR Certification, STAR Attestation, and C-STAR Assessment
- Level 3: STAR Continuous Monitoring (program requirements are still under development by CSA)

## Microsoft and CSA STAR certification

Microsoft Azure, Microsoft Intune, and Microsoft Power BI have obtained STAR Certification, which involves a rigorous independent third-party assessment of a cloud provider's security posture. This STAR certification is based on achieving ISO/IEC 27001 certification and meeting criteria specified in the CCM. It demonstrates that a cloud service provider conforms to the applicable requirements of ISO/IEC 27001, has addressed issues critical to cloud security as outlined in the CCM, and has been assessed against the STAR Capability Maturity Model for the management of activities in CCM control areas.

During the assessment, an accredited CSA certification auditor assigns a Maturity Capability score to each of the 16 CCM control areas. The average score is then used to assign the overall level of maturity and the corresponding Bronze, Silver, or Gold award. Azure, Intune, Power BI, and Microsoft Cloud App Security were awarded Cloud Security Alliance (CSA) STAR Certification at the Gold level.

Learn how to accelerate your CSA STAR Certification deployment with our Azure Security and Compliance Blueprints: [Download the Microsoft Azure Responses to CSA Consensus Assessments Initiative Questionnaire](#)

## Microsoft in-scope cloud services

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- Microsoft Graph
- Microsoft Healthcare Bot
- Intune
- [Microsoft Managed Desktop](#)
- Microsoft Defender Advanced Threat Protection
- OMS Service Map
- Power Automate (formerly Microsoft Flow): cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- PowerApps cloud service: either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI: The cloud service portion of Power BI offered as a standalone service or as included in an Office 365 branded plan or suite
- Power BI Embedded

- [Microsoft Stream](#)

## Audits, reports, and certificates

- [Azure, Dynamics 365, and Online Services – CSA STAR Certificate](#)

## Frequently asked questions

### Which industry standards does the CSA CCM align with?

The CCM corresponds to industry-accepted security standards, regulations, and control frameworks, such as ISO 27001, PCI DSS, HIPAA, AICPA SOC 2, NERC CIP, FedRAMP, NIST, and many more. For the most current list, visit the [CSA website](#).

### Where can I view the CSA STAR Certification for Microsoft cloud services?

You can view the [CSA STAR Certification](#) for Azure, which also covers Dynamics 365, Intune and, Power BI from the CSA Registry.

### What maturity level did Microsoft cloud services achieve?

Azure, Microsoft Cloud App Security, Intune, and Power BI have achieved the highest possible Gold Award for the Maturity Capability assessment.

### Which CSA STAR levels of assurance have Microsoft business cloud services attained?

- **Level 1: CSA STAR Self-Assessment:** Azure, Dynamics 365, and Office 365. The [Self-Assessment](#) is a complimentary offering from cloud service providers to document their security controls to help customers assess the security of the service.
- **Level 2: CSA STAR Certification:** Azure, Microsoft Cloud App Security, Intune, and Power BI. STAR Certification is based on achieving ISO/IEC 27001 certification and meeting criteria specified in the CCM. It is awarded after a rigorous third-party assessment of the security controls and practices of a cloud service provider.
- **Level 2: CSA STAR Attestation:** Azure and Intune. CSA and the AICPA have collaborated to provide guidelines for CPAs to use in conducting SOC 2 engagements, using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA CCM. [STAR Attestation](#) is based on these guidelines and is awarded after rigorous independent assessments of cloud providers.

## Resources

- [Azure standard response for request for information](#)
- [Azure Cloud Security Alliance CAIQ](#)
- [Office 365 Mapping of CSA Cloud Control Matrix](#)
- [Cloud Security Alliance](#)
- [CSA Security, Trust & Assurance Registry \(STAR\)](#)
- [About CSA STAR certification](#)
- [Cloud Controls Matrix \(CCM\)](#)
- [ISO/IEC 27001](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Compliance on the Microsoft Trust Center](#)

# Cloud Security Alliance (CSA) STAR self-assessment

11/30/2020 • 3 minutes to read • [Edit Online](#)

## CSA STAR self-assessment overview

The Cloud Security Alliance (CSA) is a nonprofit organization led by a broad coalition of industry practitioners, corporations, and other important stakeholders. It is dedicated to defining best practices to help ensure a more secure cloud computing environment, and to helping potential cloud customers make informed decisions when transitioning their IT operations to the cloud.

In 2010, the CSA published a suite of tools to assess cloud IT operations: the CSA Governance, Risk Management, and Compliance (GRC) Stack. It was designed to help cloud customers assess how cloud service providers (CSPs) follow industry best practices and standards and comply with regulations.

In 2013, the CSA and the British Standards Institution launched the Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry in which CSPs can publish their CSA-related assessments.

CSA STAR is based on two key components of the CSA GRC Stack:

- Cloud Controls Matrix (CCM): a controls framework covering fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a CSP.
- The Consensus Assessments Initiative Questionnaire (CAIQ): a set of more than 140 questions based on the CCM that a customer or cloud auditor may want to ask of CSPs to assess their compliance with CSA best practices.

STAR provides three levels of assurance; CSA-STAR Self-Assessment is the introductory offering at Level 1, which is free and open to all CSPs. Going further up the assurance stack, Level 2 of the STAR program involves third-party assessment-based certifications, and Level 3 involves certifications based on continuous monitoring.

## Microsoft and CSA STAR self-assessment

As part of the STAR Self-Assessment, CSPs can submit two different types of documents to indicate their compliance with CSA best practices: a completed CAIQ, or a report documenting compliance with CCM. For the CSA STAR Self-Assessment, Microsoft publishes both a CAIQ and a CCM-based report for Microsoft Azure, and CCM-based reports for Microsoft Dynamics 365 and Microsoft Office 365.

Learn how to accelerate your CSA STAR Self-Assessment deployment with our Azure Security and Compliance Blueprint: [Download Azure response to the CSA Consensus Assessments](#)

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- [Dynamics 365 CSA STAR Self-Assessment](#)

## Audits, reports, and certificates

- [Azure standard response for request for information](#)
- [Azure Cloud Security Alliance CAIQ](#)
- [Azure responses to the CSA CAIQ v3.0.1](#)

## Frequently asked questions



## Which industry standards does the CSA CCM align with?

The CCM corresponds to industry-accepted security standards, regulations, and control frameworks such as ISO 27001, PCI DSS, HIPAA, AICPA SOC 2, NERC CIP, FedRAMP, NIST, and many more. For the most current list, visit the [CSA website](#).

## Why is the CSA STAR Self-Assessment important?

It enables CSPs to document compliance with CSA published best practices in a transparent manner. Self-assessment reports are publicly available, thereby helping cloud customers gain visibility into the security practices of CSPs, and compare various CSPs using the same baseline.

## Which CSA STAR levels of assurance have Microsoft business cloud services attained?

- **Level 1: CSA STAR Self-Assessment:** Azure, Dynamics 365, and Office 365. The Self-Assessment is a complimentary offering from cloud service providers to document their security controls to help customers assess the security of the service.
- **Level 2: CSA STAR Certification:** Azure, Microsoft Cloud App Security, Intune, and Power BI. STAR Certification is based on achieving ISO/IEC 27001 certification and meeting criteria specified in the CCM. It is awarded after a rigorous third-party assessment of the security controls and practices of a cloud service provider.
- **Level 2: CSA STAR Attestation:** Azure and Intune. CSA and the AICPA have collaborated to provide guidelines for CPAs to use in conducting SOC 2 engagements, using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA CCM. STAR Attestation is based on these guidelines and is awarded after rigorous independent assessments of cloud providers.

## Resources

- [Cloud Security Alliance](#)
- [Cloud Controls Matrix \(CCM\)](#)
- [Consensus Assessments Initiative Questionnaire \(CAIQ\)](#)
- [CSA Security, Trust & Assurance Registry \(STAR\)](#)
- [Compliance on the Microsoft Trust Center](#)

## Microsoft CSA STAR self-assessments

- [Azure](#)
- [Dynamics 365](#)

# Microsoft 365 ISO 27001 action plan — Top priorities for your first 30 days, 90 days, and beyond

2/5/2021 • 9 minutes to read • [Edit Online](#)

The International Organization for Standardization (ISO) is an independent nongovernmental developer of voluntary international standards. The International Electrotechnical Commission (IEC) leads the preparation and publication of international standards for electrical, electronic, and related technologies. The ISO/IEC 27000 family of standards outlines controls and mechanisms that help maintain the security of information assets.

ISO/IEC 27001 is the international standard for implementing an information security management system (ISMS). An ISMS describes the necessary methods used and evidence associated with requirements that are essential for the reliable management of information asset security in any type of organization.

This article includes a prioritized action plan you can follow as you work to meet the requirements of ISO/IEC 27001. This action plan was developed in partnership with Protiviti, a Microsoft partner specializing in regulatory compliance. Learn more about how to use this action plan at Microsoft Ignite by attending this session: [Chart your Microsoft 365 compliance path and information protection strategy](#), presented by Maithili Dandige (Microsoft) and Antonio Maio (Protiviti).

## Action plan outcomes

These recommendations are provided across three phases in a logical order with the following outcomes:

PHASE	OUTCOMES
-------	----------

PHASE	OUTCOMES
30 days	<p><b>Understand your ISO 27001 governance and compliance requirements.</b></p> <ul style="list-style-type: none"> <li>• Conduct a risk assessment and align risk management and mitigation to that assessment's outcomes.</li> <li>• Assess and manage your compliance risks by using Microsoft Compliance Manager.</li> <li>• Establish standard operating procedures (SOPs) for each of the 14 ISO 27001 groups.</li> </ul> <p><b>Start planning a roll out of an information classification and retention policies and tools to the organization to help users identify, classify, and protect sensitive data and assets.</b></p> <ul style="list-style-type: none"> <li>• Learn how the Azure Information Protection application and policies can help users easily apply visual sensitivity markings and metadata to documents and emails. Develop your organization's information classification schema, along with an education and roll out plan.</li> <li>• Consider rolling out Labels to the organization to help users easily apply record retention and protection policies to content. Plan your organization's labels in accordance with your legal requirements for information record retention, along with an education and roll out plan.</li> </ul> <p><b>Ensure that records related to information security are protected from loss, deletion, modification, or unauthorized access by creating Audit and Accountability policies as part of your Standard Operating Procedures (SOPs).</b></p> <ul style="list-style-type: none"> <li>• Enable audit logging (including mailbox auditing) to monitor Microsoft 365 for potentially malicious activity and to enable forensic analysis of data breaches.</li> <li>• On a regular cadence, search your company's audit logs to review changes that have been made to the tenant's configuration settings.</li> <li>• Enable alert policies for sensitive activities, such as when an elevation of privileges occurs on a user account.</li> <li>• For long-term storage of audit log data, use the Office 365 Management Activity API reference to integrate with a security information and event management (SIEM) tool.</li> </ul> <p><b>Define administrative and security roles for the organization, along with appropriate policies related to segregation of duties.</b></p> <ul style="list-style-type: none"> <li>• Utilize the Microsoft 365 administrative roles to enable separation of administration duties.</li> <li>• Segment permissions to ensure that a single administrator does not have greater access than necessary.</li> </ul>

PHASE	OUTCOMES
90 days	<p><b>Use Microsoft 365 security capabilities to control access to the environment, and protect organizational information and assets according to your defined standard operating procedures (SOPs).</b></p> <ul style="list-style-type: none"> <li>• Protect administrator and end-user accounts by enabling identity and authentication solutions, such as multi-factor authentication and modern authentication.</li> <li>• Establish strong password policies to manage and protect user account credentials.</li> <li>• Configure and roll out message encryption capabilities to help end users comply with your organization's SOPs when sending sensitive data via email.</li> <li>• Protect against malicious code and implement data breach prevention and response procedures.</li> <li>• Configure Data Loss Prevention (DLP) policies to identify, protect, and control access to sensitive data.</li> <li>• Ensure that sensitive data is stored and accessed according to corporate policies.</li> <li>• Prevent the most common attack vectors including phishing emails and Office documents containing malicious links and attachments.</li> </ul>
Beyond 90 days	<p><b>Use Microsoft 365 advanced data governance tools and information protection to implement ongoing governance programs for personal data.</b></p> <ul style="list-style-type: none"> <li>• Automatically identify personal information in documents and emails</li> <li>• Protect sensitive data stored and accessed on mobile devices across the organization, and ensure that compliant corporate devices are used to data.</li> </ul> <p><b>Monitor ongoing compliance across Microsoft 365 and other Cloud applications.</b></p> <ul style="list-style-type: none"> <li>• To evaluate performance against standard operating procedures (SOPs), utilize Compliance Manger to perform regular assessments of the organization's information security policies and their implementation.</li> <li>• Review and monitor the information security management system on an on-going basis.</li> <li>• Control and perform regular reviews of all users and groups with high levels of permissions (i.e. privileged or administrative users).</li> <li>• Deploy and configure Microsoft 365 capabilities for protecting privileged identities and strictly controlling privileged access.</li> <li>• As part of your standard operating procedures (SOPs), search the audit logs to review changes that have been made to the tenant's configuration settings, elevation of end-user privileges and risky user activities.</li> <li>• Monitor your organization's usage of cloud applications and implement advanced alerting policies.</li> <li>• Track risky activities, to identify potentially malicious administrators, to investigate data breaches, or to verify that compliance requirements are being met.</li> </ul>

## 30 days — Powerful Quick Wins

These tasks can be accomplished quickly and have low impact to users.

AREA	TASKS
Understand your ISO 27001 governance and compliance requirements.	<ul style="list-style-type: none"> <li>Assess and manage your compliance risks by using the <a href="#">Compliance Manager</a> to conduct an ISO 27001:2013 assessment of your organization. Establish standard operating procedures (SOPs) for each of the 14 ISO 27001 groups.</li> </ul>
Start planning a roll out of an information classification and retention policies and tools to the organization to help users identify, classify, and protect sensitive data and assets.	<ul style="list-style-type: none"> <li>Help users easily identify and classify sensitive data, according to your information protection policies and standard operating procedures (SOPs), by rolling out classification policies and the <a href="#">Azure Information Protection</a> application. Develop your organization's information classification schema (policies), along with an education and roll out plan.</li> <li>Help users easily apply record retention and protection policies to content by rolling out <a href="#">Microsoft 365 Labels</a> to the organization. Plan your organization's labels in accordance with your legal requirements for information record retention, along with an education and roll out plan.</li> </ul>
Ensure that records related to information security are protected from loss, deletion, modification, or unauthorized access by creating Audit and Accountability policies as part of your Standard Operating Procedures (SOPs).	<ul style="list-style-type: none"> <li>Enable <a href="#">audit logging</a> and <a href="#">mailbox auditing</a> (for all Exchange mailboxes) to monitor Microsoft 365 for potentially malicious activity and to enable forensic analysis of data breaches.</li> <li>On a regular cadence, search your company's audit logs to review changes that have been made to the tenant's configuration settings.</li> <li>Enable <a href="#">Microsoft 365 Alert Policies</a> in the Microsoft 365 security or compliance center for sensitive activities, such as when an elevation of privileges occurs on a user account.</li> <li>For long-term storage of audit log data, use the <a href="#">Office 365 Management Activity API reference</a> to integrate with a security information and event management (SIEM) tool.</li> </ul>
Define administrative and security roles for the organization, along with appropriate policies related to segregation of duties.	<ul style="list-style-type: none"> <li>Utilize the <a href="#">Microsoft 365 administrative roles</a> to enable separation of administration duties. Note: many administrator roles have a corresponding role in Exchange Online, SharePoint Online, and Skype for Business Online.</li> <li>Segment permissions to ensure that a single administrator does not have greater access than necessary.</li> </ul>

## 90 days — Enhanced Protections

These tasks take a bit more time to plan and implement but greatly increase your security posture.

AREA	TASKS
------	-------

AREA	TASKS
<p>Use Microsoft 365 security capabilities to control access to the environment, and protect organizational information and assets according to your defined standard operating procedures (SOPs).</p>	<ul style="list-style-type: none"> <li>• Protect administrator and end-user accounts by implementing <a href="#">identity and device access policies</a>, including enabling multi-factor authentication (MFA) for all user accounts and modern authentication for all apps.</li> <li>• Establish <a href="#">strong password policies</a> to manage and protect user account credentials.</li> <li>• Set up <a href="#">Office 365 Message Encryption (OME)</a> to help end users comply with your organization's SOPs when sending sensitive data via email.</li> <li>• Deploy <a href="#">Windows Defender Advanced Threat Protection (ATP)</a> to all desktops for protection against malicious code, as well as data breach prevention and response.</li> <li>• Configure, test, and deploy <a href="#">Data Loss Prevention (DLP) policies</a> to identify, monitor and <a href="#">automatically protect</a> over 80 common sensitive data types within documents and emails, including financial, medical, and personally identifiable information.</li> <li>• Automatically inform email senders that they may be about to violate one of your policies — even before they send an offending message by configuring <a href="#">Policy Tips</a>. Policy Tips can be configured to present a brief note in Outlook, Outlook on the web, and OWA for devices, that provides information about possible policy violations during message creation.</li> <li>• Implement <a href="#">Office 365 Advanced Threat Protection (ATP)</a> to help prevent the most common attack vectors including phishing emails and Office documents containing malicious links and attachments.</li> </ul>

## Beyond 90 Days — Ongoing Security, Data Governance, and Reporting

Secure personal data at rest and in transit, detect and respond to data breaches, and facilitate regular testing of security measures. These are important security measures that build on previous work.

AREA	TASKS
<p>Use Microsoft 365 advanced data governance tools and information protection to implement ongoing governance programs for personal data.</p>	<ul style="list-style-type: none"> <li>• Use <a href="#">Office 365 Advanced Data Governance</a> to identify personal information in documents and emails by automatically applying Microsoft 365 Labels.</li> <li>• Use <a href="#">Microsoft Intune</a> to protect sensitive data stored and accessed on mobile devices across the organization, and ensure that compliant corporate devices are used to data.</li> </ul>

AREA	TASKS
<p>Monitor ongoing compliance across Microsoft 365 and other Cloud applications.</p>	<ul style="list-style-type: none"> <li>• To evaluate performance against standard operating procedures (SOPs), use <a href="#">Compliance Manager</a> on an ongoing basis to perform regular ISO 27001:2013 assessments of the organization's information security policies and their implementation.</li> <li>• Review and monitor the information security management system on an on-going basis.</li> <li>• Use <a href="#">Azure AD Privileged Identity Management</a> to control and perform regular reviews of all users and groups with high levels of permissions (i.e. privileged or administrative users).</li> <li>• Deploy and configure <a href="#">Privileged Access Management in Office 365</a> to provide granular access control over privileged admin tasks in Office 365. Once enabled, users need to request just-in-time access to complete elevated and privileged tasks through an approval workflow that is highly scoped and time-bound.</li> <li>• As part of your standard operating procedures (SOPs), search the audit logs to review changes that have been made to the tenant's configuration settings, elevation of end-user privileges and risky user activities.</li> <li>• Audit <a href="#">non-owner mailbox access</a> to identify potential leaks of information and to proactively review non-owner access on all Exchange Online mailboxes.</li> <li>• Use <a href="#">Microsoft 365 Alert Policies, data loss prevention reports and Microsoft Cloud App Security</a> to monitor your organization's usage of cloud applications and implement advanced alerting policies based on heuristics and user activity.</li> <li>• Use <a href="#">Microsoft Cloud App Security</a> to automatically track risky activities, to identify potentially malicious administrators, to investigate data breaches, or to verify that compliance requirements are being met.</li> </ul>

## Learn more

- Microsoft Trust Center: [ISO/IEC 27001:2013 Information Security Management Standards](#)

# ISO/IEC 20000-1:2011 Information Technology Service Management

2/17/2021 • 2 minutes to read • [Edit Online](#)

## ISO/IEC 20000-1:2011 overview

The International Organization for Standardization (ISO) is an independent nongovernmental organization and the world's largest developer of voluntary international standards. The International Electrotechnical Commission (IEC) is the world's leading organization for the preparation and publication of international standards for electrical, electronic, and related technologies.

Published under the joint ISO/IEC subcommittee in 2005 and revised in 2011, ISO 20000-1:2011 is an international standard for the establishment, implementation, operation, monitoring, and review of an Information Technology Service Management System (SMS). It is the only standard in the ISO 20000 family that results in a formal certification. The standard is based on requirements for designing, transitioning, delivering, and improving services to fulfill agreed service requirements and to provide value to both customers and service providers. ISO 20000-1 helps organizations provide assurance to customers that their service requirements will be fulfilled.

## Microsoft and ISO/IEC 20000-1:2011

Obtaining the ISO 20000-1:2011 certification is a logical step for Microsoft Azure. We lead the industry with the most comprehensive compliance coverage, enabling customers to meet a wide range of regulatory obligations. The ISO 20000-1 certification complements our current catalog of ISO certifications including ISO 27001:2013 and ISO 9001:2015, which validate that a process of continual improvement is in place helping Microsoft Azure deliver a secure and reliable cloud service platform for our customers.

An independent third-party auditing firm performed a rigorous examination of Microsoft Azure and several Microsoft online services for adherence to the requirements established in the ISO 20000-1:2011 standard. The available ISO 20000-1 certificate demonstrates that Azure and covered Microsoft online services have implemented the right IT service management procedures to deliver efficient and reliable IT services that are subject to regular monitoring, review, and improvement.

## Microsoft in-scope cloud services

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- Microsoft Defender Advanced Threat Protection
- Microsoft Graph
- Microsoft Healthcare Bot
- Intune
- [Microsoft Managed Desktop](#)
- Office 365 Operated by 21Vianet
- Microsoft PowerApps
- Power Automate (formerly Microsoft Flow)
- Power BI
- Power BI Embedded



# Audits, reports, and certificates

ISO 20000-1 documentation as follows:

- [Azure, Dynamics 365, and Online Services: ISO20000-1 Certificate](#)
- [Azure, Dynamics 365, and Online Services: ISO20000-1 Assessment Report](#)
- [Azure, Dynamics 365, and Online Services: ISO20000-1 Statement of Availability \(SOA\)](#)

## Frequently asked questions

### **Where can I get the ISO 20000-1:2011 audit reports and scope statements for Microsoft services?**

The Service Trust Portal provides independently audited compliance reports. You can use the portal to request reports so that your auditors can compare Microsoft's cloud services results with your own legal and regulatory requirements. The FY17 Microsoft Azure ISO 20000-1 Assessment Report and the FY17 Microsoft Azure ISO 20000-1 Certificate are both available.

### **Does Microsoft run annual tests for infrastructure failures?**

Yes. The ISO 20000-1:2011 annual assessment includes the underlying physical infrastructure datacenter. Review the certificate for the coverage details.

### **Where can I view Microsoft's compliance information for ISO 20000-1:2011?**

You can download the ISO 20000-1:2011 certificate for Azure and additional services that are in scope of this assessment.

### **Can I use the compliance of Microsoft services to ISO 20000-1:2011 in my organization's certification process?**

Yes. If your business is seeking certification for implementations deployed on in-scope services, you can use the relevant Microsoft certifications in your compliance assessment. However, you are responsible for engaging an assessor to evaluate your implementation for compliance, and for the controls and processes within your own organization.

## Resources

- [ISO 20000-1:2011—Service management](#) (requirements for purchase)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

# ISO 22301:2012 Business Continuity Management Standard

2/17/2021 • 3 minutes to read • [Edit Online](#)

## ISO 22301 overview

The International Organization for Standardization (ISO) is an independent nongovernmental organization and the world's largest developer of voluntary international standards. The ISO formed the TC 223 Societal Security technical committee to develop standards for protecting society, including organizations, if catastrophes such as a natural disaster, major terrorist attack, or the shutdown of power grids occur.

Published in 2012 by the technical committee, ISO 22301:2012 is the first international standard for management systems that help ensure business continuity. ISO 22301 is the premium standard for business continuity, and certification demonstrates conformance to rigorous practices to prevent, mitigate, respond to, and recover from disruptive incidents.

## Microsoft and ISO 22301

Microsoft is the first hyperscale cloud service provider to receive the ISO 22301 certification for business continuity management. An independent certification body awarded this certification to Microsoft Azure, Microsoft Azure Government, Microsoft Office 365 (including Commercial, Government, and Education offerings), Microsoft Cloud App Security, Microsoft Intune, and Microsoft Power BI after a stringent audit covering all aspects of their business continuity processes. The audit covered the in-scope services listed below and Azure management features, the Azure Portal, and the systems used to monitor, operate, and update the in-scope services.

## Microsoft in-scope cloud services

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- Dynamics 365, Dynamics 365 Government, and Dynamics 365 Germany
- Microsoft Defender Advanced Threat Protection
- Microsoft Graph
- Microsoft Healthcare Bot
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- [Office 365 Commercial, Government, and Education](#)
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- Power BI Embedded

## Audits, reports, and certificates

- [Azure, Dynamics 365, and Online Services: ISO22301 Certificate](#)

- [Azure, Dynamics 365, and Online Services: ISO22301 Assessment Report](#)
- [BSI 22301 Microsoft Office 365 Certificate](#)
- [BSI 22301 Microsoft Office 365 Stage 2 Addendum](#)
- [Office 365 ISO 22301 Stage 2 Report](#)

## Frequently asked questions

### Why is Microsoft compliance with ISO 22301 important?

ISO 22301 is a certification used by enterprises and governmental organization to show their commitment to serving their customers by achieving the highest available international standard for business continuity management. ISO 22301 is a comprehensive standard that demonstrates the highest level of commitment to business continuity and disaster preparedness.

### Where can I get the ISO 22301 audit reports and scope statements for Microsoft services?

The [Service Trust Portal](#) provides independently audited compliance reports, so that your auditors can compare Microsoft's cloud services results with your own legal and regulatory requirements.

### Can I use ISO 22301 compliance of Microsoft services in my organization's certification?

Yes. If your business requires ISO 22301 certification for implementations deployed on Microsoft services, you can use the Azure and Office 365 certifications in your compliance assessment. You are responsible, however, for engaging an assessor to evaluate the controls, processes, and implementation for ISO 22301 compliance within your own organization and for your own applications.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [ISO 22301:2012 standard](#) (for purchase)
- [Azure resiliency technical guidance](#) (Explains the Azure shared responsibility model for business continuity.)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Microsoft Online Services Terms](#)
- [Microsoft Enterprise Business Continuity Management Program Description](#)
- [Compliance Score](#)
- [Compliance on the Microsoft Trust Center](#)

# ISO/IEC 27001:2013 Information Security Management Standards

2/18/2021 • 4 minutes to read • [Edit Online](#)

## ISO/IEC 27001 overview

The International Organization for Standardization (ISO) is an independent nongovernmental organization and the world's largest developer of voluntary international standards. The International Electrotechnical Commission (IEC) is the world's leading organization for the preparation and publication of international standards for electrical, electronic, and related technologies.

Published under the joint ISO/IEC subcommittee, the ISO/IEC 27000 family of standards outlines hundreds of controls and control mechanisms to help organizations of all types and sizes keep information assets secure. These global standards provide a framework for policies and procedures that include all legal, physical, and technical controls involved in an organization's information risk management processes.

ISO/IEC 27001 is a security standard that formally specifies an Information Security Management System (ISMS) that is intended to bring information security under explicit management control. As a formal specification, it mandates requirements that define how to implement, monitor, maintain, and continually improve the ISMS. It also prescribes a set of best practices that include documentation requirements, divisions of responsibility, availability, access control, security, auditing, and corrective and preventive measures. Certification to ISO/IEC 27001 helps organizations comply with numerous regulatory and legal requirements that relate to the security of information.

## Microsoft and ISO/IEC 27001

The international acceptance and applicability of ISO/IEC 27001 is the key reason why certification to this standard is at the forefront of Microsoft's approach to implementing and managing information security. Microsoft's achievement of ISO/IEC 27001 certification points up its commitment to making good on customer promises from a business, security compliance standpoint. Currently, both Azure Public and Azure Germany are audited once a year for ISO/IEC 27001 compliance by a third-party accredited certification body, providing independent validation that security controls are in place and operating effectively.

Learn about the benefits of ISO/IEC 27001 on the Microsoft Cloud: [Download the ISO/IEC 27001:2013](#)

## Microsoft in-scope cloud services

- [Azure, Azure Government, and Azure Germany](#)
- Azure DevOps Services
- Microsoft Cloud App Security
- Microsoft Defender Advanced Threat Protection
- [Dynamics 365, Dynamics 365 Government, and Dynamics 365 Germany](#)
- Microsoft Graph
- Microsoft Healthcare Bot
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite

- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)
- Office 365 Germany
- OMS Service Map
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- Power BI Embedded
- Power Virtual Agents
- [Microsoft Professional Services](#)
- Microsoft Stream
- Microsoft Threat Expert
- Microsoft Translator

## Audits, reports, and certificates

Audit cycle: Microsoft cloud services are audited at least annually against the ISO 27001:2013 standard.

### Azure

- [Azure, Dynamics 365, and Online Services: ISO27001 Certificate](#)

### Office 365

- [Office 365—Global and Germany ISO 27001: Information Security Management Standards Certificate](#)

### Azure DevOps Services

- [Azure DevOps Services](#)

### Microsoft Professional Services

- [Microsoft Professional Services](#)

## Assessments and reports

### Azure

- [Azure, Dynamics 365, and Online Services: ISO 27001, 27018 and 27701 Audit Assessment Report](#)
- [Azure, Dynamics 365, and Online Services: 27001, 27018, 27701 Statement of Applicability \(SOA\)](#)

### Office 365

- [Office 365: ISO 27001, 27018, and 27017 Audit Assessment Report](#)
- [Office 365: Information Security Management System \(ISMS\)—Statement Of Applicability for Security and Privacy](#)
- [Office 365 Germany: ISO 27001, 27017, and 27018 Audit Assessment Report](#)
- [Yammer: ISO27001 Audit Assessment Report](#)

### Azure DevOps Services

- [Azure DevOps Services ISO 27001 Certificate IS 619017](#)

[See additional audit reports](#)

## Frequently asked questions

### Why is Microsoft compliance with ISO/IEC 27001 important?

Compliance with these standards, confirmed by an accredited auditor, demonstrates that Microsoft uses internationally recognized processes and best practices to manage the infrastructure and organization that

support and deliver its services. The certificate validates that Microsoft has implemented the guidelines and general principles for initiating, implementing, maintaining, and improving the management of information security.

#### Where can I get the ISO/IEC 27001 audit reports and scope statements for Microsoft services?

The [Service Trust Portal](#) provides independently audited compliance reports. You can use the portal to request reports so that your auditors can compare Microsoft's cloud services results with your own legal and regulatory requirements.

#### Does Microsoft run annual tests for infrastructure failures?

Yes. The annual ISO/IEC 27001 certification process for the Microsoft Cloud Infrastructure and Operations group includes an audit for operational resiliency. To preview the latest certificate, click the link below.

- Microsoft Azure: [ISO/IEC 27001:2013 certificate for Microsoft Cloud Infrastructure and Operations](#)
- Azure German: [ISO/IEC 27001:2013 certificate for Microsoft Cloud Infrastructure and Operations](#)

#### Where do I start my organization's own ISO/IEC 27001 compliance effort?

Adopting ISO/IEC 27001 is a strategic commitment. As a starting point, consult the [ISO/IEC 27000 Directory](#).

#### Can I use the ISO/IEC 27001 compliance of Microsoft services in my organization's certification?

Yes. If your business requires ISO/IEC 27001 certification for implementations deployed on Microsoft services, you can use the applicable certification in your compliance assessment. You are responsible, however, for engaging an assessor to evaluate the controls and processes within your own organization and your implementation for ISO/IEC 27001 compliance.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager has a pre-built assessment for this regulation for Enterprise E5 customers. Find the template for building the assessment in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Mapping Microsoft Cyber Offerings to: NIST Cybersecurity \(CSF\), CIS Controls, and ISO27001:2013 Frameworks](#)
- [The ISO/IEC 27000 Directory](#)
- [ISO/IEC 27001: 2013 standard](#) (for purchase)
- [Microsoft sets a high bar for information security](#) (BSI case study)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Microsoft Online Services Terms](#)
- [Microsoft Cloud for Government](#)
- [Compliance on the Microsoft Trust Center](#)

## White papers

- [Azure DevOps Services data protection overview](#)
- [13 effective Azure security controls for ISO 27001 compliance](#)

# ISO/IEC 27017:2015 Code of Practice for Information Security Controls

2/17/2021 • 3 minutes to read • [Edit Online](#)

## ISO-IEC 27017 Overview

The ISO/IEC 27017:2015 code of practice is designed for organizations to use as a reference for selecting cloud services information security controls when implementing a cloud computing information security management system based on ISO/IEC 27002:2013. It can also be used by cloud service providers as a guidance document for implementing commonly accepted protection controls.

This international standard provides additional cloud-specific implementation guidance based on ISO/IEC 27002, and provides additional controls to address cloud-specific information security threats and risks referring to clauses 5-18 in ISO/IEC 27002: 2013 for controls, implementation guidance, and other information. Specifically, this standard provides guidance on 37 controls in ISO/IEC 27002, and it also features seven new controls that are not duplicated in ISO/IEC 27002. These new controls address the following important areas:

- Shared roles and responsibilities within a cloud computing environment
- Removal and return of cloud service customer assets upon contract termination
- Protection and separation of a customer's virtual environment from environments of other customers
- Virtual machine hardening requirements to meet business needs
- Procedures for administrative operations of a cloud computing environment
- Enabling customers to monitor relevant activities within a cloud computing environment
- Alignment of security management for virtual and physical networks

## Microsoft and ISO/IEC 27017

ISO/IEC 27017 is unique in providing guidance for both cloud service providers and cloud service customers. It also provides cloud service customers with practical information on what they should expect from cloud service providers. Customers can benefit directly from ISO/IEC 27017 by ensuring they understand the shared responsibilities in the cloud.

## Microsoft in-scope cloud services

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- [Dynamics 365, Dynamics 365, and Dynamics 365 Germany](#)
- Microsoft Defender Advanced Threat Protection
- Microsoft Graph
- Microsoft Healthcare Bot
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Office 365, Office 365 U.S. Government, Office 365 U.S. Government Defense, and Office 365 Germany
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite

- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- Power BI Embedded
- Microsoft Stream
- See a [detailed list](#) of covered services in Office 365

## Audits, reports, and certificates

Microsoft cloud services are audited once a year for the ISO/IEC 27017:2015 code of practice as part of the certification process for ISO/IEC 27001:2013.

- [Azure ISO 27017 Certificate](#)
- [Azure ISO 27017 Assessment report](#)
- [Office 365: ISO 27001, 27018, and 27017 Audit Assessment Report](#)

## Frequently asked questions

To whom does the standard apply?

This code of practice provides controls and implementation guidance for both cloud service providers and cloud service customers. It is structured in a format similar to ISO/IEC 27002:2013.

### **Where can I view Microsoft's compliance information for ISO/IEC 27017:2015?**

You can download the [ISO/IEC 27017:2015 certificate](#) for Azure, Intune, and Power BI.

### **Can I use the ISO/IEC 27017 compliance of Microsoft services in my organization's certification process?**

Yes. If your business is seeking certification for implementations deployed on any Microsoft in-scope enterprise cloud services, you can use Microsoft's relevant certifications in your compliance assessment. However, you are responsible for engaging an assessor to evaluate your implementation for compliance, and for the controls and processes within your own organization.

### **How can I get copies of the applicable audit reports?**

The [Service Trust Portal](#) provides independent, third-party audit reports and other related documentation. You can use the portal to download and review this documentation for assistance with your own regulatory requirements.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [ISO/IEC 27017:2015 code of practice](#)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)



# ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud

2/17/2021 • 5 minutes to read • [Edit Online](#)

## ISO/IEC 27018 overview

The International Organization for Standardization (ISO) is an independent nongovernmental organization and the world's largest developer of voluntary international standards. The ISO/IEC 27000 family of standards helps organizations of every type and size keep information assets secure.

In 2014, the ISO adopted ISO/IEC 27018:2014, an addendum to ISO/IEC 27001, the first international code of practice for cloud privacy. Based on EU data-protection laws, it gives specific guidance to cloud service providers (CSPs) acting as processors of personally identifiable information (PII) on assessing risks and implementing state-of-the-art controls for protecting PII.

### Microsoft and ISO/IEC 27018

At least once a year, Microsoft Azure and Azure Germany are audited for compliance with ISO/IEC 27001 and ISO/IEC 27018 by an accredited third-party certification body, providing independent validation that applicable security controls are in place and operating effectively. As part of this compliance verification process, the auditors validate in their statement of applicability that Microsoft in-scope cloud services and commercial technical support services have incorporated ISO/IEC 27018 controls for the protection of PII in Azure. To remain compliant, Microsoft cloud services must be subject to annual third-party reviews.

By following the standards of ISO/IEC 27001 and the code of practice embodied in ISO/IEC 27018, Microsoft (the first major cloud provider to incorporate this code of practice) demonstrates that its privacy policies and procedures are robust and in line with its high standards.

- **Customers of Microsoft cloud services know where their data is stored.** Because ISO/IEC 27018 requires certified CSPs to inform customers of the countries in which their data may be stored, Microsoft cloud service customers have the visibility they need to comply with any applicable information security rules.
- **Customer data won't be used for marketing or advertising without explicit consent.** Some CSPs use customer data for their own commercial ends, including for targeted advertising. Because Microsoft has adopted ISO/IEC 27018 for its in-scope enterprise cloud services, customers can rest assured that their data will never be used for such purposes without explicit consent, and that consent cannot be a condition for use of the cloud service.
- **Microsoft customers know what's happening with their PII.** ISO/IEC 27018 requires a policy that allows for the return, transfer, and secure disposal of personal information within a reasonable period of time. If Microsoft works with other companies that need access to your customer data, Microsoft proactively discloses the identities of those sub-processors.
- **Microsoft complies only with legally binding requests for disclosure of customer data.** If Microsoft must comply with such a request (as in the case of a criminal investigation), it will always notify the customer unless it is prohibited by law from doing so.

## Microsoft in-scope cloud services

- [Azure, Azure Government, and Azure Germany](#)
- Azure DevOps Services
- Microsoft Cloud App Security

- Dynamics 365, Dynamics 365, and Dynamics 365 Germany
- Microsoft Professional Services: Premier and On Premises for Azure, Dynamics 365, Intune, and for medium business and enterprise customers of Microsoft 365 for business
- Microsoft Graph
- Microsoft Healthcare Bot
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow): cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)
- Office 365 Germany
- OMS Service Map
- PowerApps cloud service: either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service: either as a standalone service or as included in an Office 365 branded plan or suite
- Power BI Embedded
- Power Virtual Agents
- Microsoft Threat Experts
- Microsoft Stream
- Windows Defender ATP: Endpoint Detection & Response, Automatic Investigation & Remediation, Secure Score

## Audits, reports, and certificates

### Audit cycle

Microsoft cloud and commercial technical support services are audited once a year for the ISO/IEC 27018 code of practice as part of the certification process for ISO/IEC 27001.

### Audits and reports

- [Azure, Dynamics 365, and Online Services: ISO27018 Certificate](#)
- [Azure, Dynamics 365, and Online Services: ISO27018 Assessment Report](#)
- [Azure Germany: ISO27018 Code of Practice for Protecting Personal Data in the Cloud Certificate](#)

### Office 365

- [Office 365: ISO 27001, 27018, and 27017 Audit Assessment Report](#)
- [Yammer ISO 27018 Audit Assessment Report](#)

### Azure DevOps Services

- [Azure DevOps Services: ISO27018 Certificate PII 665918](#)

## Frequently asked questions

### To whom does ISO/IEC 27018 apply?

This code of practice applies to CSPs that process PII under contract for other organizations. At Microsoft, it also applies to the support of these CSPs.

### What is the difference between 'personal information controllers' and 'personal information processors'?

In the context of ISO/IEC 27018:

- 'Controllers' control the collection, holding, processing, or use of personal information; they include those who control it on another company's behalf.
- 'Processors' process information on behalf of controllers; they do not make decisions as to how to use the information or the purposes of the processing. In providing its enterprise cloud services, Microsoft (as a vendor to you) is an information processor.

### Where can I view Microsoft compliance information for ISO/IEC 27018?

- You can review the ISO/IEC 27018 certificates from BSI for [Azure](#), [Microsoft Professional Services](#), and [Power BI](#).
- You can also review ISO/IEC 27001 certificates from BSI upon which ISO/IEC 27018 certification is based for [Dynamics 365](#), [Office 365](#), and [Azure DevOps Services](#).
- To review the BSI reports, the independent auditor that validated Microsoft compliance with ISO/IEC 27018, visit the [Service Trust Portal](#).

### Can I use Microsoft's compliance in my organization's certification process?

Yes. If compliance with ISO/IEC 27018 is important for your business and implementations deployed on any of Microsoft in-scope enterprise cloud services, you can use Microsoft's attestation of compliance with ISO/IEC 27018 with Microsoft's certification for ISO/IEC 27001 in your compliance assessment.

However, you are responsible for engaging an assessor to evaluate your implementation for compliance, and for the controls and processes within your own organization.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [ISO/IEC 27018:2014 code of practice](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Data access policies for Microsoft enterprise cloud and technical services](#)
- [Microsoft Online Services Terms](#)
- [Microsoft Government Cloud](#)
- [Compliance on the Microsoft Trust Center](#)

# ISO/IEC 27701 Privacy Information Management System (PIMS)

2/17/2021 • 5 minutes to read • [Edit Online](#)

## Privacy Information Management System (PIMS) overview

The European Union's General Data Protection Regulation (GDPR), has ushered in a new era of privacy regulatory and compliance globally. More privacy regulations, many modeled after the GDPR, have been enacted in different jurisdictions (be that market/industry, or physical location). As a result, organizations must implement policies and procedures to assure compliance with the growing list of privacy regulations. In addition, we are collectively in the midst of rapid digital transformation where data collection and processing are increasing dramatically. The simultaneous growth in data volume and regulatory requirements pertaining to that data makes compliance increasingly complex for organizations of all types.

The new international standard [ISO/IEC 27701 Privacy Information Management System \(PIMS\)](#) (formerly known as ISO/IEC 27552 during drafting period), helps organizations reconcile privacy regulatory requirements. The standard outlines a comprehensive set of operational controls that can be mapped to various regulations, including the GDPR. Once mapped, the PIMS operational controls are implemented by privacy professionals and audited by internal or third-party auditors resulting in a certification and comprehensive evidence of conformity.

## Compliance challenges

Expecting vendors to certify against PIMS will be effective for establishing responsible privacy practices by suppliers and partners no matter the size of your organization. ISO/IEC 27701 addresses three key compliance challenges:

- **Too many regulatory requirements to juggle:** Reconciling multiple regulatory requirements through the use of a universal set of operational controls enables consistent and efficient implementation.
- **Too costly to audit regulation-by-regulation:** Auditors, both internal and third party, can assess regulatory compliance using a universal operational control set within a single audit cycle.
- **Promise of compliance without proof is potentially risky:** Commercial agreements involving movement of personal information may warrant certification of compliance.

## Too many regulatory requirements to juggle

ISO/IEC 27701 includes an annex containing the operational controls of the standard that are mapped against relevant requirements in GDPR for controllers and processors. This mapping is just an example of how privacy regulations can be operationalized with the ISO framework. As additional mappings with other regulations become available and are validated, the operational controls from the standard can be transferred directly from regulatory review to implementation. This universal framework allows organizations to reliably operationalize the relevant regulatory requirements without 'reinventing the wheel.' A pending open-source project is underway to enable the privacy community to map other regulations and validate existing mappings. Stay tuned for announcement.

## Too costly to audit regulation-by-regulation

Let's go back to our opening statement on the current landscape. As more privacy regulations come into force in various jurisdictions, the pressure to provide evidence of compliance will also increase. But the costs of disparate regulatory certifications become prohibitive if every regulation calls for its own unique audit. By outlining a set

of universal operational controls, PIMS also outlines a universal compliance framework to audit against, and potentially certify, for multiple regulatory requirements.

It is important to recognize that an official GDPR certification requires pending approval decisions to be made by the European regulators. While the alignment between PIMS and GDPR is evident, a PIMS certification should be taken as evidence of GDPR compliance, not as an official GDPR certification until regulatory decisions are finalized.

## Promises of compliance without proof is potentially risky

Modern organizations engage in complex data transfers with a deep network of business partners including partner organizations or co-controllers, processors such as cloud providers, and sub-processors such as vendors who support those same processors. Failure to comply with regulations in any part of this network may lead to cascading compliance issues across the supply chain. This is where a verification of compliance can be valuable beyond the assurance provided by contractual terms between these organizations. Since the global economy dictates that most of these organizations are spread out around the world, it is practical to use an international standard from ISO to manage compliance across the network.

This reliance on compliance increases the importance of certification to the standard. While not all companies and organizations need to earn such certification, most will benefit from partners and vendors who do, especially when sensitive or high volumes of data processing are involved.

## Building blocks of the standard

PIMS is built on top of one of the most widely adopted international standards for information security management, [ISO/IEC 27001](#). If your organization is already familiar with ISO/IEC 27001, it is logical and more efficient to integrate the new privacy controls of PIMS. This means the implementation and audit of both will be less expensive and easier to achieve.

Key points on ISO/IEC 27001 and PIMS:

- ISO/IEC 27001 is one of the most used ISO standards in the world, with many companies already certified to it.
- PIMS includes new controller- and processor-specific controls that help bridge the gap between privacy and security and provides a point of integration between what may be two separate functions in organizations.
- Privacy depends on security. Likewise, PIMS depends on ISO/IEC 27001 for security management. Certification for PIMS must be obtained as an extension of an ISO/IEC 27001 certification and cannot be obtained independently.

## What should your organization do with PIMS?

No matter the size of your organization and whether it is a controller or a processor, your organization should consider pursuing certification, either for your own organization, or requesting it from vendors or suppliers based on your business requirements. This applies especially for processors, sub-processors, and co-controllers that are processing sensitive or high volumes of personal data. In any case, your organization should assess its business needs to determine if certification for its own products and services is suitable.

## Microsoft in-scope cloud services

- Azure, Azure Government, and Azure Germany
- Azure DevOps Services
- Microsoft Cloud App Security
- Dynamics 365, Dynamics 365 Government, and Dynamics 365 Germany
- Microsoft Graph

- Microsoft Healthcare Bot
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow)
- PowerApps
- Power BI
- Power BI Embedded
- Power Virtual Agents
- Microsoft Stream
- Microsoft Threat Experts
- Windows Defender Advanced Threat Protection

## Audits, reports, and certificates

- [Azure, Dynamics 365, and Online Services:ISO27701 certification](#)
- [Azure, Dynamics 365, and Online Services:ISO27701 assessment report](#)

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [ISO/IEC 27701 \(PIMS\) for purchase](#)
- [BSI whitepaper and content about PIMS](#)
- [PIMS introductory video](#)
- [Compliance on the Microsoft Trust Center](#)

# ISO 9001:2015 Quality Management Systems Standards

2/17/2021 • 2 minutes to read • [Edit Online](#)

## ISO 9001 overview

ISO 9001:2015 is an international standard that establishes the criteria for a quality management system. It is the only standard in the ISO 9000 family that results in a formal certification. The standard is based on several quality management principles, including clear focus on meeting customer requirements, strong corporate governance and leadership commitment to quality objectives, process-driven approach to meeting objectives, and focus on continuous improvement. ISO 9001:2015 helps organizations improve customer satisfaction by focusing on the consistency and quality of products and services provided to customers.

## Microsoft and ISO 9001:2015

An independent third-party auditing firm performed a rigorous examination of Microsoft Azure and several Microsoft online services for adherence to the quality management principles established by ISO 9001:2015. The available third-party certification provides independent confirmation that Azure and covered Microsoft online services meet the ISO 9001:2015 requirements.

## Microsoft in-scope cloud services

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- Dynamics 365, Dynamics 365 Government, and Dynamics 365 Germany
- Microsoft Graph
- Intune
- Microsoft Defender Advanced Threat Protection
- Microsoft Healthcare Bot
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- Power BI Embedded
- Microsoft Stream

## Audits, reports, and certificates

- [Azure, Dynamics 365, and Online Services: ISO9001 Certificate](#)
- [Azure, Dynamics 365, and Online Services: ISO9001 Assessment Report](#)
- [Azure, Dynamics 365, and Online Services: ISO9001 Statement of Applicability \(SOA\)](#)

## Frequently asked questions

To whom does the standard apply?

This standard of practice provides guidance and tools for cloud service providers and cloud service customers to ensure that cloud products and services consistently meet customers' requirements. It is structured in a format similar to ISO 27001:2013.

### **Where can I get the ISO 9001:2015 audit reports and scope statements for Microsoft services?**

The [Service Trust Portal](#) provides independently audited compliance reports. You can use the portal to request reports so that your auditors can compare Microsoft's cloud services results with your own legal and regulatory requirements. The [FY17 Microsoft Azure ISO 9001 Assessment Report](#) and the [FY17 Microsoft Azure ISO 9001 Certificate](#) are both available.

### **Does Microsoft run annual tests for infrastructure failures?**

Yes. The ISO 9001:2015 annual assessment includes the underlying physical infrastructure datacenter. [Review the certificate](#) for the coverage details.

### **Where can I view Microsoft's compliance information for ISO 9001:2015?**

You can download the [ISO 9001:2015 certificate](#) for Azure and additional services that are in scope of this assessment.

## Resources

- [ISO 9001:2015—Quality management](#)
- [ISO 9001: 2015 standard](#) (requirements for purchase)
- [ISO 9000: 2015](#) (fundamentals and vocabulary for purchase)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)



# Service Organization Controls (SOC)

2/17/2021 • 5 minutes to read • [Edit Online](#)

## SOC 1, 2, and 3 Reports overview

Increasingly, businesses outsource basic functions such as data storage and access to applications to cloud service providers (CSPs) and other service organizations. In response, the American Institute of Certified Public Accountants (AICPA) has developed the Service Organization Controls (SOC) framework, a standard for controls that safeguard the confidentiality and privacy of information stored and processed in the cloud. This aligns with the International Standard on Assurance Engagements (ISAE), the reporting standard for international service organizations.

Service audits based on the SOC framework fall into two categories — SOC 1 and SOC 2 — that apply to in-scope Microsoft cloud services.

A SOC 1 audit, intended for CPA firms that audit financial statements, evaluates the effectiveness of a CSP's internal controls that affect the financial reports of a customer using the provider's cloud services. The Statement on Standards for Attestation Engagements (SSAE 18) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) are the standards under which the audit is performed, and is the basis of the SOC 1 report.

A SOC 2 audit gauges the effectiveness of a CSP's system based on the AICPA Trust Service Principles and Criteria. An Attest Engagement under Attestation Standards (AT) Section 101 is the basis of SOC 2 and SOC 3 reports.

At the conclusion of a SOC 1 or SOC 2 audit, the service auditor renders an opinion in a SOC 1 Type 2 or SOC 2 Type 2 report, which describes the CSP's system and assesses the fairness of the CSP's description of its controls. It also evaluates whether the CSP's controls are designed appropriately, were in operation on a specified date, and were operating effectively over a specified time period.

Auditors can also create a SOC 3 report — an abbreviated version of the SOC 2 Type 2 audit report — for users who want assurance about the CSP's controls but don't need a full SOC 2 report. A SOC 3 report can be conferred only if the CSP has an unqualified audit opinion for SOC 2.

## Microsoft and SOC 1, 2, and 3 Reports

Microsoft covered cloud services are audited at least annually against the SOC reporting framework by independent third-party auditors. The audit for Microsoft cloud services covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.

Microsoft has achieved SOC 1 Type 2, SOC 2 Type 2, and SOC 3 reports. In general, the availability of SOC 1 and SOC 2 reports is restricted to customers who have signed nondisclosure agreements with Microsoft; the SOC 3 report is publicly available.

## Microsoft in-scope cloud services

### Covered services for SOC 1 and SOC 2

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- [Dynamics 365 and Dynamics 365 U.S. Government](#)
- Microsoft Graph

- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- Microsoft Stream
- Azure DevOps Services

### **Covered services for SOC 3**

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- Microsoft Graph
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)
- Power BI
- Microsoft Stream

## Audits, reports, and certificates

### **Audit cycle**

Microsoft cloud services are audited at least annually against SOC 1 (SSAE18, ISAE 3402), SOC 2 (AT Section 101), and SOC 3 standards.

### **Azure, Dynamics 365, Microsoft Cloud App Security, Flow, Microsoft Graph, Intune, Power BI, PowerApps, Microsoft Stream, and Microsoft Datacenters**

- [Azure + Dynamics 365 and Azure + Dynamics 365 Government SOC 1 Type 2 Report](#)
- [Azure + Dynamics 365 and Azure + Dynamics 365 Government SOC 2 Type 2 Report](#)
- [Azure + Dynamics 365 and Azure + Dynamics 365 Government SOC 3 Report](#)

### **Office 365**

- [Office 365 Core - SSAE 18 SOC 1 Report](#)
- [Office 365 Core - SSAE 18 SOC 2 Report](#)
- [Office 365 Core - SSAE 18 SOC 3 Report](#)
- [Office 365 Microservices T1-SSAE 18 SOC2 Type I Report](#)
- [Customer Lockbox SOC 1 SSAE 16 Audit Report](#)
- [Yammer SOC 2 AT 101 Type I Audit Report](#)
- [Yammer SOC 2 Type II Report](#)
- [See bridge letters and additional audit reports](#)

## Frequently asked questions

How can I get copies of the SOC reports?

With the reports, your auditors can compare Microsoft business cloud services results with your own legal and regulatory requirements.

- You can see all SOC reports through the [Service Trust Platform](#).
- Azure DevOps Service customers that can't access [Service Trust Platform](#) can email [Azure DevOps](#) for its SOC 1 and SOC 2 reports. This email is to request Azure DevOps SOC reports only.

#### How often are Azure SOC reports issued?

SOC reports for Azure, Microsoft Cloud App Security, Flow, Microsoft Graph, Intune, Power BI, PowerApps, Microsoft Stream, and Microsoft Datacenters are based on a rolling 12-month run window (audit period) with new reports issued semi-annually (period ends are March 31 and September 30). Bridge letters are issued each quarter to cover the prior three month period. For example, the January letter covers 10/1-12/31, the April letter covers 1/1-3/31, the July letter covers 4/1-6/30, and the October letter covers 7/1-9/30. Customers can [download](#) the latest reports from the Service Trust Portal.

#### Do I need to conduct my own audit of Microsoft datacenters?

No. Microsoft shares the independent audit reports and certifications with customers so that they can verify Microsoft compliance with its security commitments.

#### Can I use Microsoft's compliance in my organization's certification process?

Yes. When you migrate your applications and data to covered Microsoft cloud services, you can build on the audits and certifications that Microsoft holds. The independent reports attest to the effectiveness of controls that Microsoft has implemented to help maintain the security and privacy of your data.

#### Where do I start with my organization's own compliance effort?

The [SOC Toolkit for Service Organizations](#) is a helpful resource for understanding SOC reporting processes and promoting your organization's use of them.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Better protect your data by using Microsoft cloud services](#)
- [Service Organization Control \(SOC\) Reports](#)
- [SSAE 16 Overview](#)
- [ISAE 3402 Overview](#)
- [Microsoft Online Services Terms](#)
- [Microsoft Government Cloud](#)
- [Compliance on the Microsoft Trust Center](#)

# Web Content Accessibility Guidelines

11/30/2020 • 2 minutes to read • [Edit Online](#)

## About WCAG

The Web Content Accessibility Guidelines (WCAG) provide a framework for making web content more accessible for people with disabilities. WCAG version 2.0 was published in 2008 by the World Wide Web Consortium (W3C), an international organization dedicated to creating web standards, and updated to WCAG 2.1 in June 2018. In 2012, WCAG 2.0 was also published by the International Organization for Standardization (ISO) as ISO/IEC 40500:2012.

Content that conforms to WCAG 2.1 also conforms to WCAG 2.0. For policies requiring conformance to WCAG 2.0, WCAG 2.1 can provide an alternate means of conformance.

Microsoft is a major software and cloud-services provider to consumers, businesses, and governments around the world. To assist customers in making purchasing decisions, Microsoft publishes Accessibility Conformance Reports describing the extent to which our products and services support the WCAG criteria. This information can help Microsoft customers determine whether a particular product or service will meet their specific needs.

## Microsoft and WCAG

Microsoft's consideration of the WCAG standard in the development of products and services points to its commitment to making technology and data accessible for all customers.

Microsoft publishes WCAG reports that reflect the complete product or service. It generally does not create reports for individual features or components. Sometimes, Microsoft might release a new component for an existing product, or a new version of an existing component, which users can choose to install separately, and Microsoft might also publish a WCAG report for that component.

[Download the WCAG \(ISO/IEC 40500\) accessibility standards](#)

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Azure DevOps Services
- Dynamics 365 and Dynamics 365 U.S. Government
- Intune
- Office 365 and Office 365 U.S. Government
- Office 365 U.S. Government Defense
- Windows Server 2016

## Microsoft accessibility conformance reports

Read WCAG reports for [all our products and services](#).

## Resources

- [Microsoft accessibility site](#): Get information on using accessibility features and explore the ways Microsoft innovates to help everyone achieve more.
- [Office 365 Accessibility Center](#): Office 365 resources for people with disabilities.

- [Enterprise Disability Answer Desk](#): Dedicated support for enterprise customers with accessibility questions about our products and services or compliance.
- [Compliance on the Microsoft Trust Center](#)

# Criminal Justice Information Services (CJIS) Security Policy

2/17/2021 • 4 minutes to read • [Edit Online](#)

## CJIS overview

The Criminal Justice Information Services (CJIS) Division of the US Federal Bureau of Investigation (FBI) gives state, local, and federal law enforcement and criminal justice agencies access to criminal justice information (CJI) — for example, fingerprint records and criminal histories. Law enforcement and other government agencies in the United States must ensure that their use of cloud services for the transmission, storage, or processing of CJI complies with the [CJIS Security Policy](#), which establishes minimum security requirements and controls to safeguard CJI.

The CJIS Security Policy integrates presidential and FBI directives, federal laws, and the criminal justice community's Advisory Policy Board decisions, along with guidance from the National Institute of Standards and Technology (NIST). The Policy is periodically updated to reflect evolving security requirements.

The CJIS Security Policy defines 13 areas that private contractors such as cloud service providers must evaluate to determine if their use of cloud services can be consistent with CJIS requirements. These areas correspond closely to NIST 800-53, which is also the basis for the [Federal Risk and Authorization Management Program \(FedRAMP\)](#), a program under which Microsoft has been certified for its Government Cloud offerings.

In addition, all private contractors who process CJI must sign the CJIS Security Addendum, a uniform agreement approved by the US Attorney General that helps ensure the security and confidentiality of CJI required by the Security Policy. It also commits the contractor to maintaining a security program consistent with federal and state laws, regulations, and standards, and limits the use of CJI to the purposes for which a government agency provided it.

## Microsoft and CJIS Security Policy

Microsoft signs the CJIS Security Addendum in states with CJIS Information Agreements. These tell state law enforcement authorities responsible for compliance with CJIS Security Policy how Microsoft's cloud security controls help protect the full lifecycle of data and ensure appropriate background screening of operating personnel with access to CJI. Microsoft continues to work with state governments to enter into CJIS Information Agreements.

Microsoft has assessed the operational policies and procedures of Microsoft Azure Government, Microsoft Office 365 U.S. Government, and Microsoft Dynamics 365 U.S. Government, and will attest to their ability in the applicable services agreements to meet FBI requirements for the use of in-scope services.

Learn about the benefits of CJIS Security policy on the Microsoft Cloud: [Read how Genetec cleared criminal investigations](#)

## Microsoft in-scope cloud services

- [Azure Government](#)
- [Dynamics 365 U.S. Government](#)
- [Office 365 U.S. Government](#)
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

# Audits, reports, and certificates

The FBI does not offer certification of Microsoft compliance with CJIS requirements. Instead, a Microsoft attestation is included in agreements between Microsoft and a state's CJIS authority, and between Microsoft and its customers.

[Microsoft CJIS Cloud Requirements](#)

## CJIS status in the United States (current as of 11/5/2020)

44 states and the District of Columbia with management agreements, highlighted on the map in green include:

Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and the District of Columbia.

Microsoft's commitment to meeting the applicable CJIS regulatory controls allows Criminal Justice organizations to implement cloud-based solutions and be compliant with CJIS Security Policy V5.8.

## Frequently asked questions

### Where can I request compliance information?

Contact your Microsoft account representative for information on the jurisdiction you are interested in. Contact [cjis@microsoft.com](mailto:cjis@microsoft.com) for information on which services are currently available in which states.

### How does Microsoft demonstrate that its cloud services enable compliance with my state's requirements?

Microsoft signs an Information Agreement with a state CJIS Systems Agency (CSA); you may request a copy from your state's CSA. In addition, Microsoft provides customers with in-depth security, privacy, and compliance information. Customers may also review security and compliance reports prepared by independent auditors so they can validate that Microsoft has implemented security controls (such as ISO 27001) appropriate to the relevant audit scope.

### Where do I start with my agency's compliance effort?

[CJIS Security Policy](#) covers the precautions that your agency must take to protect CJ. In addition, your Microsoft account representative can put you in touch with those familiar with the requirements of your jurisdiction

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Criminal Justice Information Services](#)
- [CJIS Security Policy](#)
- [CJIS implementation guidelines for Azure Government](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Microsoft Government Cloud](#)

- [Compliance on the Microsoft Trust Center](#)



# Committee on National Security Systems Instruction No. 1253 (CNSSI 1253)

2/5/2021 • 2 minutes to read • [Edit Online](#)

## About CNSS Instruction 1253

The Committee on National Security Systems (CNSS) is a governmental organization that sets national cybersecurity policy for US government departments and agencies. The [CNSS Instruction No. 1253](#), "Security Categorization and Control Selection for National Security Systems," provides guidance on the security standards that federal agencies should apply to categorize national security information and systems at appropriate security levels.

The CNSSI 1253 builds on NIST SP 800-53, which provides the control baseline for the FedRAMP High authorization. There are, however, some key differences between the CNSSI 1253 and NIST publications.

For example, the CNSSI 1253 approach explicitly defines the associations of Confidentiality, Integrity, and Availability with security controls, and refines the use of security control overlays for the national security community. The CNSS uses a separate Low, Medium, and High category for each of these three security objectives. This results in categorizations such as Moderate-Moderate-Low — Moderate Confidentiality, Moderate Integrity, and Low Availability. CNSSI 1253 then provides the appropriate security baselines for each possible system categorization using controls from NIST SP 800-53.

## Microsoft and CNSSI 1253

A FedRAMP-approved third-party assessment organization (3PAO), Kratos SecureInfo, has independently validated the compliance of the Microsoft Azure Government system with the CNSSI 1253 High-High-High Baseline. Kratos SecureInfo attests that the CNSSI 1253 Security Assessment Report (SAR) of Azure Government provides a complete assessment of the applicable security controls stipulated in the Security Assessment Plan (SAP). The SAR documents the testing conducted to validate Azure Government against a selection of CNSSI 1253 security controls for systems requiring High Confidentiality, High Integrity, and High Availability.

Azure Government currently possesses a FedRAMP High Provisional Authorization to Operate (P-ATO) issued by the Joint Authorization Board (JAB), and a Department of Defense Provisional Authorization (PA) at Impact Level 5 of the Cloud Computing Security Requirements Guide (SRG). Using these authorizations, Kratos SecureInfo analyzed the security controls that were tested in the previous assessments to determine which additional CNSSI 1253 security controls to test to ensure compliance with the CNSSI 1253 High-High-High baseline. Kratos SecureInfo examined evidence and conducted interviews to validate the successful implementation of 43 applicable security controls and published the results of its complete testing in the CNSSI 1253 SAR.

The compliance of Azure Government with the demanding CNSSI 1253 requirements means that Azure can offer public sector customers in the United States a rich array of services compliant with CNSSI 1253, enabling them to benefit from the cost savings and rigorous security of the Microsoft Cloud.

## Microsoft in-scope cloud services

- [Azure Government](#)

## Audits, reports, and certificates

Azure Government CNSSI 1253 attestation of compliance with the CNSSI 1253 High-High-High baseline

## How to implement

- [Azure government documentation](#): Tutorials and how-to guides help developers deploy and manage services using Azure Government.

## Frequently asked questions

**To whom does CNSSI 1253 apply?**

Customers with national security systems (NSS) must comply with CNSSI 1253 requirements and controls.

**Which Azure environments have been tested against CNSSI 1253 security controls?**

Azure Government (FedRAMP package ID F1603087869) has been tested against these controls.

## Resources

- [What is Azure Government?](#)
- [Azure Government](#)
- [Microsoft and FedRAMP](#)
- [Microsoft and DoD Provisional Authorization](#)
- [Microsoft Government Cloud](#)
- [Compliance on the Microsoft Trust Center](#)

# Defense Federal Acquisition Regulation Supplement (DFARS)

2/5/2021 • 4 minutes to read • [Edit Online](#)

## DFARS overview

On October 21, 2016, the Department of Defense (DoD) issued its Final Rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) and imposing safeguarding and cyber incident reporting obligations on defense contractors whose information systems process, store, or transmit covered defense information (CDI).

The final DFARS clause 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) specifies safeguards to include cyber incident reporting requirements and additional considerations for cloud service providers. Per DFARS 252.204-7012, all DoD contractors and the defense industrial base are required to comply with DFARS requirements for adequate security 'as soon as practical, but not later than December 31, 2017.'

## Microsoft and DFARS

Microsoft Government Cloud services help the United States defense industrial base and defense contractor customers meet the DFARS requirements as enumerated in the DFARS clauses of 252.204-7012 that apply to cloud service providers. When defense contractors are required to comply with DFARS clause 252.204-7012 in contracts, Microsoft can support the requirements applicable to cloud service providers for Azure Government and Office 365 U.S. Government Defense services. Both services demonstrate support for the capabilities necessary for customers to comply with the DFARS 7012 clauses through their L5 accreditation to the Department of Defense Security Requirements Guide.

Learn how to accelerate your DFARS deployment with our Azure Security and Compliance Blueprint: [Download the Azure — Blueprint DFARS Customer Responsibilities Matrix](#)

## Microsoft in-scope cloud services

Covered services for DoD Impact Level 5

- [Azure and Azure Government](#)
- [Office 365 U.S. Government and Office 365 U.S. Government Defense](#)

## Audits, reports, and certificates

- [Microsoft Cloud Services Authorizations](#)
- [Azure P-ATO Letter Signed March 3, 2017](#)
- [See additional audit reports](#)

## Frequently asked questions

**Which DFARS requirements are supported by Microsoft Azure Government and Office 365 U.S. Government Defense?**

Azure Government and Office 365 U.S. Government Defense allow our defense industrial base and defense contractor customers to meet the DFARS requirements as enumerated in the DFARS clauses of 252.204-7012

that apply to cloud service providers.

### **Has an independent assessor validated that Azure Government and Office 365 U.S. Government Defense supports DFARS requirements?**

Yes, a third-party assessment organization has attested that the Azure Government and Office 365 U.S. Government Defense cloud service offering meets the applicable requirements of DFARS Clause 252.204-7012 (Safeguarding Unclassified Controlled Technical Information).

### **What is the relationship between Controlled Unclassified Information (CUI) and covered defense information (CDI)?**

CUI is information that requires safeguarding or disseminating controls according to law, regulation, or government-wide policy. The [CUI Registry](#) identifies approved CUI categories and subcategories.

CDI is controlled technical information or other information (as described in the CUI Registry) that requires safeguarding or dissemination controls and is either:

- Marked or otherwise identified in the contract, task order, or delivery order, and provided to the contractor by or on behalf of DoD in connection with the performance of the contract or
- Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract

### **Do all Microsoft services meet the 'adequate security' requirements applicable to 'covered defense information' under the DFARS regulation?**

In October 2016, the Department of Defense (DoD) promulgated a final rule implementing Defense Federal Acquisition Regulation Supplement (DFARS) clauses that apply to all DoD contractors who process, store, or transmit 'covered defense information' through their information systems. The rule states that such systems must meet the security requirements set forth in NIST SP 800-171, [Protecting Controlled Unclassified Information in nonfederal information systems and organizations](#), or an 'alternative, but equally effective, security measure' that is approved by the DoD contracting officer. And where a DoD contractor uses an external cloud service provider to process, store, or transmit covered defense information, such provider must meet security requirements that are equivalent to the FedRAMP Moderate baseline.

The following Microsoft cloud services have received a FedRAMP moderate authorization and are adequate for DFARS: Azure Government, Dynamics 365 U.S. Government, Office 365 U.S. Government, and Office 365 U.S. Government Defense.

Also, Microsoft offerings outside the FedRAMP-certified boundary that could potentially be used by DoD contractors to process, store, or transmit 'covered defense information' are undergoing a review to meet a December 31, 2017, compliance deadline. Microsoft is working to document how these internal and customer-facing services comply with NIST SP 800-171 or an acceptable security equivalent, to meet the DFARS relevant clauses.

## **Use Microsoft Compliance Manager to assess your risk**

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## **Resources**

- [Defense Federal Acquisition Regulation Supplement \(DFARS\)](#)
- [Microsoft Cloud for Government](#)

- [Online Services Terms](#)
- [Controlled Unclassified Information \(CUI\)](#)
- [Compliance on the Microsoft Trust Center](#)

# US Department of Defense (DoD) Provisional Authorization at Impact Levels 2, 4, and 5

2/5/2021 • 5 minutes to read • [Edit Online](#)

## DoD and DISA overview

The Defense Information Systems Agency (DISA) is a combat support agency of the US Department of Defense (DoD). It provides an enterprise information infrastructure, communications support, and a secure, resilient enterprise cloud environment for the DoD, the White House, and any other organization that plays a role in the defense of the United States.

To implement its mandate, DISA developed the DoD Cloud Computing Security Requirements Guide (SRG). The SRG defines the baseline security requirements for cloud service providers (CSPs) that host DoD information, systems, and applications, and for DoD's use of cloud services. It replaces the DoD Cloud Security Model, and maps to the DoD Risk Management Framework and NIST 800-37/53.

DoD Cloud Service Support defines the policies, security controls, and other requirements in the SRG, which it publishes and maintains. It guides DoD agencies and departments in planning and authorizing the use of a cloud service provider. Cloud Service Support also evaluates CSP offerings for compliance with the SRG — an authorization process whereby CSPs can provide attestations of compliance with DoD standards. It issues DoD Provisional Authorizations (PAs) when appropriate, so DoD agencies and supporting organizations can use cloud services without having to go through a full approval process on their own, saving time and effort.

## Microsoft and US DoD Provisional Authorization

Microsoft's government cloud services meet the demanding requirements of the US Department of Defense, from impact levels 2 through 5, enabling U.S. defense agencies to benefit from the cost savings and rigorous security of the Microsoft Cloud. By deploying protected services including Azure Government, Office 365 U.S. Government, and Dynamics 365 Government, defense agencies can use a rich array of compliant services.

- Learn how to accelerate your DoD DISA L2, L4 deployment with our [Azure DoD Blueprint](#)

## DoD Impact Level 5 Provisional Authorization

DISA Cloud Service Support has granted a DoD Impact Level 5 PA for Microsoft Azure Government for DoD. DISA has also granted Office 365 U.S. Government Defense a DoD Impact Level 5 PA. Impact Level 5 covers Controlled Unclassified Information (CUI) deemed by law, other government regulations, or the agency that owns the information and needs a higher level of protection than Level 4 provides. It also covers unclassified National Security Systems.

## DoD Impact Level 4 Provisional Authorization

DISA Cloud Service Support has granted a DoD Impact Level 4 PA for Microsoft Azure Government. This was based on a review of their FedRAMP authorizations and additional security controls required by the Cloud Computing SRG. (FedRAMP is a US program that enables secure cloud computing for the government.)

Impact Level 4 covers Controlled Unclassified Information — data requiring protection from unauthorized disclosure under Executive Order 13556 (November 2010) and other mission-critical data. It may include data designated as For Official Use Only, Law Enforcement Sensitive, or Sensitive Security Information. This authorization enables US federal government customers to deploy these types of highly sensitive data on in-

scope Microsoft government cloud services.

## Covered services for DoD Impact Level 2 Authorization

Based on FedRAMP authorizations, DISA Cloud Service Support granted a DoD Impact Level 2 PA to:

- Azure and Azure Government Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) were granted this authorization based on the Provisional Authority to Operate (P-ATO) from the FedRAMP Joint Authorization Board.
- Dynamics 365 U.S. Government Software as a Service (SaaS) was granted this authorization based on the Agency FedRAMP Authority to Operate (ATO) from the Department of Housing and Urban Development (HUD).
- Office 365 U.S. Government was granted this authorization based on the Agency FedRAMP ATO from the Department of Health and Human Services (DHHS).

Impact Level 2 covers Non-Controlled Unclassified Information — data that is authorized for public release. It also covers other unclassified information that, while not considered 'mission critical,' still requires a minimal level of access control. This authorization enables US federal government customers to deploy non-sensitive information and basic defense applications and websites on in-scope Microsoft cloud services.

## Microsoft in-scope cloud services

### Covered services for DoD Impact Level 5

- [Azure Government for DoD](#)
- [Office 365 U.S. Government Defense](#)

### Covered services for DoD Impact Level 4

- [Azure Government](#)
- [Dynamics 365 U.S. Government](#)
- [Office 365 U.S. Government Defense](#)

### Covered services for DoD Impact Level 2

- [Azure](#)
- [Dynamics 365 U.S. Government](#)
- [Office 365 U.S. Government](#)
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Audits, reports, and certificates

Once granted a DoD PA, Microsoft cloud services are monitored and assessed annually: [Microsoft FedRAMP authorizations](#)

## Fast track your deployment of DoD solutions on Azure

Get a head start on taking advantage of the benefits of the cloud in government with the Azure Security and Compliance Department of Defense Blueprint. This blueprint provides tools and guidance to get you started building DoD-compliant solutions today. [Start using the Azure DoD Blueprint.](#)

## Frequently asked questions

**Can I use Microsoft's compliance in my organization's certification process?**

Yes. All DoD agencies may rely on the certifications of Microsoft cloud services as the foundation for any

program or initiative that requires a DoD authorization. (This also applies to other organizations that support DoD and require cloud services.) However, you need to achieve your own authorizations for components outside these services.

### Does Microsoft's DoD certification meet NIST 800–171 requirements?

In October 2016, the Department of Defense (DoD) promulgated a final rule implementing Defense Federal Acquisition Regulation Supplement (DFARS) clauses that apply to all DoD contractors who process, store, or transmit 'covered defense information' through their information systems. The rule states that such systems must meet the security requirements set forth in NIST SP 800–171, [Protecting Controlled Unclassified Information in nonfederal information systems and organizations](#), or an 'alternative, but equally effective, security measure' that is approved by the DoD contracting officer. And where a DoD contractor uses an external cloud service provider to process, store, or transmit covered defense information, such provider must meet security requirements that are equivalent to the FedRAMP Moderate baseline.

The following Microsoft cloud services have received a FedRAMP moderate authorization: Azure, Azure Government, Dynamics 365 U.S. Government, Office 365 MT, Office 365 U.S. Government, and Office 365 U.S. Government Defense.

Also, Microsoft offerings outside the FedRAMP-certified boundary that could potentially be used by DoD contractors to process, store, or transmit 'covered defense information' are undergoing a review to meet a December 31, 2017, compliance deadline. Microsoft is working to document how these internal and customer-facing services comply with NIST SP 800–171 or an acceptable security equivalent, to meet the DFARS relevant clauses.

## Resources

- [DoD Cloud Computing Security Requirements Guide \(SRG\) and other documents](#)
- [DISA Cloud Service Support](#)
- [Protecting Controlled Unclassified Information in nonfederal information systems and organizations](#)
- [NIST Cybersecurity Framework](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Microsoft Government Cloud](#)
- [Compliance on the Microsoft Trust Center](#)



# US DoE 10 CFR Part 810

11/30/2020 • 2 minutes to read • [Edit Online](#)

## Microsoft and DoE 10 CFR Part 810

Microsoft Azure Government can help support customers subject to the export control requirements of US Department of Energy (DoE) 10 CFR Part 810 through two authorizations:

- The FedRAMP High Provisional Authorization to Operate (P-ATO) issued by the Joint Authorization Board (JAB)
- The Level 4 and 5 Provisional Authorizations from the Department of Defense (DoD) Defense Information Systems Agency

FedRAMP offers an appropriate baseline to provide assurances that Azure Government delivers core infrastructure and virtualization technologies and services such as compute, storage, and networking that are designed with stringent NIST controls. These help meet customer data separation requirements and help enable secure connections to customers' on-premises environments.

Furthermore, Azure Government is a US government community cloud that is physically separated from the Azure cloud. It provides additional assurances regarding specific background screening requirements by the US government, including specific controls that restrict access to information and systems to screened US citizens among Azure operations personnel.

## Microsoft in-scope cloud services

- [Azure Government](#)
- Intune

## How to implement

- [NERC CIP Standards & Cloud Computing](#): Guidance for electric utilities and Registered Entities deploying workloads on Azure or Azure Government.

## About DoE 10 CFR Part 810

The US Department of Energy (DoE) export control regulation [10 CFR Part 810](#) governs the export of unclassified nuclear technology and assistance. It helps ensure that nuclear technologies exported from the United States will be used only for peaceful purposes. The revised Part 810 (Final Rule) took effect in March 2015 and is administered by the [National Nuclear Security Administration](#). Section 810.6 states that specific DoE authorization is required for both provisions of assistance and transfers of sensitive nuclear technology that are "generally authorized," as well as those requiring specific authorization (such as for assistance involving sensitive nuclear technologies like enrichment and heavy water production).

## Frequently asked questions

**Do the 10 CFR Part 110 regulations of the US Nuclear Regulatory Commission apply to Azure Government?**

No. The [US Nuclear Regulatory Commission](#) (NRC) regulates the [export and import](#) of nuclear facilities and related equipment and materials under [10 CFR Part 110](#). The NRC does not regulate nuclear technology and assistance related to these items that fall under DoE jurisdiction. Therefore, NRC 10 CFR Part 110 regulations

would not apply to Azure Government.

### **How can I supply evidence that I am complying with DoE 10 CFR Part 810?**

If your organization is deploying data to Azure Government, you can rely on the Azure Government FedRAMP High P-ATO as evidence that you are handling data in an appropriately restricted manner. However, you are responsible for getting DoE authorization of your own systems, including the use of cloud services.

### **What are my responsibilities for classifying data deployed to Azure Government?**

Customers deploying data to Azure Government are responsible for their own security classification process. For customer data subject to DoE export controls, the classification system is augmented by the Unclassified Controlled Nuclear Information (UCNI) controls established by Section 148 of the [US Atomic Energy Act](#).

## Resources

- [Azure Cloud Services and US Export Controls](#)
- [Microsoft and FedRAMP](#)
- [Microsoft and DoD](#)
- [Microsoft Government Cloud](#)
- [Compliance on the Microsoft Trust Center](#)

# US Export Administration Regulations (EAR)

2/5/2021 • 5 minutes to read • [Edit Online](#)

## About the EAR

The US Department of Commerce enforces the Export Administration Regulations (EAR) through the [Bureau of Industry and Security \(BIS\)](#). The EAR broadly governs and imposes controls on the export and re-export of most commercial goods, software, and technology, including “dual-use” items that can be used both for commercial and military purposes and certain defense items.

BIS guidance holds that, when data or software is uploaded to the cloud or transferred between user nodes, the customer, not the cloud provider, is the “exporter” who has the responsibility to ensure that transfers of, storage of, and access to that data or software complies with the EAR.

According to the BIS, *export* refers to the transfer of protected technology or technical data to a foreign destination or its release to a foreign person in the United States (also referred to as a *deemed export*). The EAR broadly governs:

- Exports from the United States.
- Re-exports or retransfers of US-origin items and certain foreign-origin items with more than a *de minimis* portion of US-origin content.
- Transfers or disclosures to persons from other countries.

Items subject to the EAR can be found on the Commerce Control List (CCL) where each item is assigned a unique [Export Control Classification Number \(ECCN\)](#). Items not listed on the CCL are designated as EAR99 and most EAR99 commercial products will not require a license to be exported. However, depending on the destination, end user, or end use of the item, even an EAR99 item may require a BIS export license.

The [final rule](#), published in June 2016, clarified that EAR licensing requirements also would not apply to the transmission and storage of unclassified technical data and software if they were encrypted end-to-end using FIPS 140-2 validated cryptographic modules and were not intentionally stored in a military-embargoed country or in the Russian Federation.

## Microsoft and the EAR

Microsoft technologies, products, and services are subject to the US Export Administration Regulations (EAR). While there is no compliance certification for the EAR, Microsoft Azure, Microsoft Azure Government, and Microsoft Office 365 Government (GCCHigh and DoD environments) offer important features and tools to help eligible customers subject to the EAR manage export control risks and meet their compliance requirements.

The US Commerce Department, which enforces the EAR, has taken the position that customers, not cloud service providers such as Microsoft, are considered to be exporters of their own customer data. While most customer data is not considered “technology” or “technical data” subject to EAR export controls, Microsoft in-scope cloud services are structured to help customers manage and significantly mitigate the potential export control risks they face. Microsoft generally, but not exclusively, recommends the use of its government cloud services for eligible customers. With appropriate planning, customers can use the following tools and their own internal procedures to help ensure full compliance with US export controls.

- **Controls on data location.** Customers have visibility into where their data is stored and access to robust tools to restrict its storage. They may therefore ensure that their data is stored in the United States and minimize transfer of controlled technology or technical data outside the United States. Furthermore, customer data is not stored in a non-conforming location, consistent with EAR prohibitions on where data is

“intentionally stored”: no Azure datacenter is located in any of the 25 Group D:5 countries or the Russian Federation.

- **End-to-end encryption.** By taking advantage of the end-to-end encryption safe harbor for physical storage locations specified in the EAR, Microsoft in-scope cloud services deliver encryption features that can help protect against export control risks. They also offer customers a [wide range of options for encrypting data](#) in transit and at rest, and the flexibility to choose among encryption options.
- **Tools and protocols to prevent unauthorized deemed export.** The use of encryption also helps protect against a potential deemed export (or deemed re-export) under the EAR, because even if a non-US person has access to encrypted data, nothing is revealed if they cannot read or understand the data while it is encrypted; thus there is no “release” of controlled data.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- [Office 365 Government \(GCC-High and DoD\)](#)
- Intune

## How to implement

Overview of US export controls and guidance for customers assessing their obligations under the EAR.

- [Azure](#)
- [Office 365](#)

## Frequently asked questions

### What should I do to comply with export controls when using Microsoft cloud services?

Under the EAR, when data is uploaded to a cloud server such as the Microsoft cloud, the customer who owns the data — not the cloud services provider — is considered to be the exporter. For that reason, the owner of the data — that is, the Microsoft customer — must carefully assess how their use of the Microsoft cloud may implicate US export controls and determine whether any of the data they want to use or store there may be subject to EAR controls, and if so, what controls apply. Learn more about how [Azure](#) and [Office 365](#) cloud services can help customers ensure their full compliance with US export controls.

### Are Microsoft technologies, products, and services subject to the EAR?

Most Microsoft technologies, products, and services either:

- Are not subject to the EAR and thus are not on the Commerce Control List and have no ECCN;
- Or they are EAR99 or 5D992 Mass Market-eligible for self-classification by Microsoft and may be exported to non-embargoed countries without a license as No License Required (NLR).

That said, a few Microsoft products have been assigned an ECCN that may or may not require a license. Consult the EAR or legal counsel to determine the appropriate license type and eligible countries for export purposes.

### What's the difference between the EAR and International Traffic in Arms Regulations (ITAR)?

The primary US export controls with the broadest application are the EAR, administered by the US Department of Commerce. The EAR is applicable to dual-use items that have both commercial and military applications, and to items with purely commercial applications.

The United States also has separate and more specialized export control regulations, such as the ITAR, that governs the most sensitive items and technology. Administered by the US Department of State, they impose controls on the export, temporary import, re-export, and transfer of many military, defense, and intelligence items (also known as “defense articles”), including related technical data.

# Resources

- [Exporting Microsoft Products: Overview](#)
- [Exporting Microsoft Products: FAQ](#)
- [Exporting Microsoft Products: Product Lookup](#)
- [Export restrictions on cryptography](#)
- [Microsoft and FIPS 140-2](#)
- [Microsoft and ITAR](#)
- [Compliance on the Microsoft Trust Center](#)

# Federal Risk and Authorization Management Program (FedRAMP)

2/5/2021 • 6 minutes to read • [Edit Online](#)

## FedRAMP overview

The US Federal Risk and Authorization Management Program (FedRAMP) was established to provide a standardized approach for assessing, monitoring, and authorizing cloud computing products and services under the Federal Information Security Management Act (FISMA), and to accelerate the adoption of secure cloud solutions by federal agencies.

The Office of Management and Budget now requires all executive federal agencies to use FedRAMP to validate the security of cloud services. (Other agencies have also adopted it, so it is useful in other areas of the public sector as well.) The National Institute of Standards and Technology (NIST) SP 800-53 sets the mandatory standards, establish security categories of information systems—confidentiality, integrity, and availability—to assess the potential impact on an organization should its information and information systems be compromised. FedRAMP is the program that certifies that a cloud service provider (CSP) meets those standards.

CSPs desiring to sell services to a federal agency can take three paths to demonstrate FedRAMP compliance:

- Earn a Provisional Authority to Operate (P-ATO) from the Joint Authorization Board (JAB). The JAB is the primary governance and decision-making body for FedRAMP. Representatives from the Department of Defense, the Department of Homeland Security, and the General Services Administration serve on the board. The board grants a P-ATO to CSPs that have demonstrated FedRAMP compliance.
- Receive an Authority to Operate (ATO) from a federal agency.
- Or, work independently to develop a CSP Supplied Package that meets program requirements.

Each of these paths requires a stringent technical review by the FedRAMP Program Management Office (PMO) and an assessment by an independent third-party organization that is accredited by the program.

FedRAMP authorizations are granted at three impact levels based on NIST guidelines—low, medium, and high. These levels rank the impact that the loss of confidentiality, integrity, or availability could have on an organization—low (limited effect), medium (serious adverse effect), and high (severe or catastrophic effect).

## Microsoft and FedRAMP

Microsoft's government cloud services, including Azure Government, Dynamics 365 Government, and Office 365 U.S. Government meet the demanding requirements of the US Federal Risk and Authorization Management Program (FedRAMP), enabling U.S. federal agencies to benefit from the cost savings and rigorous security of the Microsoft Cloud.

Microsoft government cloud services offer public sector customers a rich array of services compliant with FedRAMP, and robust guidance and implementation tools, including the [FedRAMP High blueprint](#), which helps customers deploy a core set of policies for any Azure-deployed architecture that must implement FedRAMP High controls.

## Microsoft Azure P-ATOs

Azure and Azure Government have earned a P-ATO at the High Impact Level from the Joint Authorization Board, the highest bar for FedRAMP accreditation, which authorizes the use of Azure and Azure Government to process

highly sensitive data.

The FedRAMP audit of Azure and Azure Government included the information security management system that encompasses infrastructure, development, operations, management, and support of in-scope services. Once a P-ATO is granted, a CSP still requires an authorization (an ATO) from any government agency it works with. For Azure, a government agency can use the Azure P-ATO in its own security authorization process and rely on it as the basis for issuing an agency ATO that also meets FedRAMP requirements.

Azure continues to support more services at FedRAMP High Impact levels than any other cloud provider. And while FedRAMP High in the Azure public cloud will meet the needs of many US government customers, agencies with more stringent requirements will continue to rely on Azure Government, which provides additional safeguards such as the heightened screening of personnel. Microsoft lists all [Azure public services currently available](#) in Azure Government to the FedRAMP High boundary, as well as services planned for the current year.

## Microsoft Dynamics 365 U.S. Government ATO

Dynamics 365 U.S. Government was granted a FedRAMP Agency ATO at the High Impact Level by the US Department of Housing and Urban Development (HUD). Although the scope of the certification is limited to the Government Community Cloud, Dynamics 365 U.S. Government business and enterprise plans operate following the same set of stringent FedRAMP controls.

## Microsoft Office 365 and Office 365 U.S. Government ATOs

- Office 365 and Office 365 U.S. Government have an ATO from the US Department of Health and Human Services (DHHS).
- Office 365 U.S. Government Defense has a P-ATO from the US Defense Information Systems Agency (DISA). Any customer wishing to deploy Office 365 U.S. Government Defense may use the DISA PIATO to generate an agency ATO to document their acceptance of it.
- Office 365 (enterprise and business plans) and Office 365 U.S. Government have a FedRAMP Agency ATO at the Moderate Impact Level from the DHHS Office of the Inspector General. Office 365 U.S. Government was the first cloud-based email and collaboration service to obtain this authorization.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- [Dynamics 365 U.S. Government](#)
- Intune
- [Office 365 and Office 365 U.S. Governmen](#)
- Office 365 U.S. Government Defense
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- Microsoft Defender ATP

### NOTE

The use of Azure Active Directory within Azure Government requires the use of components that are deployed outside of Azure Government on the Azure public cloud.

## Audits, reports, and certificates

Microsoft is required to recertify its cloud services each year to maintain its P-ATOs and ATOs. To do so, Microsoft must monitor and assess its security controls continuously, and demonstrate that the security of its

services remains in compliance.

- [Microsoft cloud services FedRAMP authorizations](#)
- [Microsoft FedRAMP Audit Reports](#)

To receive other FedRAMP reports, send email to [Azure Federal Documentation](#).

## Quickly deploy your FedRAMP solutions on Azure Government

Let Microsoft guide you through the ATO process and quickly deploy your FedRAMP solutions using the FedRAMP High blueprint, which helps customers implement a core set of policies for any Azure-deployed architecture that must implement FedRAMP High controls.

[Start using the Azure FedRAMP High Blueprint](#)

## Frequently asked questions

### Do Microsoft cloud services comply with the Federal Information Security Management Act (FISMA)?

FISMA is the federal law that requires US federal agencies and their partners to procure information systems and services only from organizations that adhere to FISMA requirements. Most agencies and their vendors that indicate that they are FISMA-compliant are referring to how they meet the controls identified by the NIST in Special Publication 800-53 rev 4. The FISMA process (but not the underlying standards themselves) was replaced by FedRAMP in 2011.

### To whom does FedRAMP apply?

'FedRAMP is mandatory for federal agency cloud deployments and service models at the low and moderate risk impact levels.' Any federal agency that wants to engage a CSP may be required to meet FedRAMP specifications. In addition, companies that employ cloud technologies in products or services used by the federal government may be required to obtain an ATO.

### Where does my agency start its own compliance effort?

For an overview of the steps federal agencies must take to successfully navigate FedRAMP and meet its requirements, go to [Get Authorized: Agency Authorization](#).

### Can I use Microsoft compliance in my agency's authorization process?

Yes. You may use the certifications of Microsoft cloud services as the foundation for any program or initiative that requires an ATO from a federal government agency. However, you need to achieve your own authorizations for components outside these services.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Federal Risk and Authorization Management Program](#)
- [FedRAMP Security Assessment Framework](#)
- [Managing compliance in the cloud at Microsoft](#)
- [Microsoft Government Cloud](#)



- [Azure Compliance Offerings](#)

# Federal Information Processing Standard (FIPS) Publication 140-2

2/5/2021 • 4 minutes to read • [Edit Online](#)

## FIPS 140-2 standard overview

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products, as defined in Section 5131 of the Information Technology Management Reform Act of 1996.

The [Cryptographic Module Validation Program](#) (CMVP), a joint effort of the U.S. National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS), validates cryptographic modules to the *Security Requirements for Cryptographic Modules* standard (i.e., FIPS 140-2) and related FIPS cryptography standards. The FIPS 140-2 security requirements cover 11 areas related to the design and implementation of a cryptographic module. The NIST Information Technology Laboratory operates a related program that validates the FIPS approved cryptographic algorithms in the module.

## Microsoft's approach to FIPS 140-2 validation

Microsoft maintains an active commitment to meeting the 140-2 requirements, having validated cryptographic modules since the standard's inception in 2001. Microsoft validates its cryptographic modules under the National Institute of Standards and Technology (NIST) [Cryptographic Module Validation Program](#) (CMVP). Multiple Microsoft products, including many cloud services, use these cryptographic modules.

For technical information on Microsoft Windows cryptographic modules, the security policy for each module, and the catalog of CMVP certificate details, see the [Windows and Windows Server FIPS 140-2 content](#).

## Microsoft in-scope cloud services

While the current CMVP FIPS 140-2 implementation guidance precludes a FIPS 140-2 validation for a cloud service itself; cloud service providers can choose to obtain and operate FIPS 140 validated cryptographic modules for the computing elements that comprise their cloud service. Microsoft online services that include components, which have been FIPS 140-2 validated include, among others:

- [Azure and Azure Government](#)
- [Dynamics 365 and Dynamics 365 Government](#)
- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)

## Frequently asked questions

### What is the difference between "FIPS 140 Validated" and "FIPS 140 compliant"?

"FIPS 140 Validated" means that the cryptographic module, or a product that embeds the module has been validated ("certified") by the CMVP as meeting the FIPS 140-2 requirements. "FIPS 140 compliant" is an industry term for IT products that rely on FIPS 140 Validated products for cryptographic functionality.

### When does Microsoft undertake a FIPS 140 validation?

The cadence for starting a module validation aligns with the feature updates of Windows 10 and Windows Server. As the software industry evolved, operating systems are released more frequently, with monthly software updates. Microsoft undertakes validation for feature releases, but in between releases, seeks to

minimize the changes to the cryptographic modules.

### **Which computers are included in a FIPS 140 validation?**

Microsoft validates cryptographic modules on a representative sample of hardware configurations running Windows 10 and Windows Server. It is common industry practice to accept this FIPS 140-2 validation when an environment uses hardware, which is similar to the samples used for the validation process.

### **There are many modules listed on the NIST website. How do I know which one applies to my agency?**

If you are required to use cryptographic modules validated through FIPS 140-2, you need to verify that the version you use appears on the validation list. The CMVP and Microsoft maintain a list of validated cryptographic modules, organized by product release, along with instructions for identifying which modules are installed on a Windows system. For more information on configuring systems to be compliant, see the [Windows and Windows Server FIPS 140-2 content](#).

### **What does 'When operated in FIPS mode' mean on a certificate?**

This caveat informs the reader that required configuration and security rules must be followed to use the cryptographic module in a way that is consistent with its FIPS 140-2 security policy. Each module has its own security policy — a precise specification of the security rules under which it will operate — and employs approved cryptographic algorithms, cryptographic key management, and authentication techniques. The security rules are defined in the security policy for each module. For more information, including links to the security policy for each module validated through the CMVP, see the [Windows and Windows Server FIPS 140-2 content](#).

### **Does FedRAMP require FIPS 140-2 validation?**

Yes, the Federal Risk and Authorization Management Program (FedRAMP) relies on control baselines defined by the [NIST SP 800-53 Revision 4](#), including [SC-13 Cryptographic Protection](#) mandating the use of FIPS-validated cryptography or NSA-approved cryptography.

### **How does Microsoft Azure support FIPS 140-2?**

Azure is built with a combination of hardware, commercially available operating systems (Linux and Windows), and Azure-specific version of Windows. Through the Microsoft [Security Development Lifecycle](#) (SDL), all Azure services use FIPS 140-2 approved algorithms for data security because the operating system uses FIPS 140-2 approved algorithms while operating at a hyper scale cloud.

### **Can I use Microsoft's adherence to FIPS 140-2 in my agency's certification process?**

To comply with FIPS 140-2, your system must be configured to run in a FIPS approved mode of operation, which includes ensuring that a cryptographic module uses only FIPS-approved algorithms. For more information on configuring systems to be compliant, see the [Windows and Windows Server FIPS 140-2 content](#).

### **What is the relationship between FIPS 140-2 and Common Criteria?**

These are two separate security standards with different, but complementary, purposes. FIPS 140-2 is designed specifically for validating software and hardware cryptographic modules, while the Common Criteria is designed to evaluate security functions in IT software and hardware products. Common Criteria evaluations often rely on FIPS 140-2 validations to provide assurance that basic cryptographic functionality is implemented properly.

## **Resources**

- [FIPS Pub 140-2 Security Requirements for Cryptographic Modules](#)
- [NIST Cryptographic Module Validation Program](#)

- [Windows, Windows Server, and FIPS 140-2](#)
- [Compliance on the Microsoft Trust Center](#)

# US Internal Revenue Service Publication 1075

2/5/2021 • 4 minutes to read • [Edit Online](#)

## US Internal Revenue Service Publication 1075 overview

Internal Revenue Service Publication 1075 (IRS 1075) provides guidance for US government agencies and their agents that access federal tax information (FTI) to ensure that they use policies, practices, and controls to protect its confidentiality. IRS 1075 aims to minimize the risk of loss, breach, or misuse of FTI held by external government agencies. For example, a state Department of Revenue that processes FTI in tax returns for its residents, or health services agencies that access FTI, must have programs in place to safeguard that information.

To protect FTI, IRS 1075 prescribes security and privacy controls for application, platform, and datacenter services. For instance, it prioritizes the security of datacenter activities, such as the proper handling of FTI, and the oversight of datacenter contractors to limit entry. To ensure that government agencies receiving FTI apply those controls, the IRS established the Safeguards Program, which includes periodic reviews of these agencies and their contractors.

## Microsoft and US Internal Revenue Service Publication 1075

Microsoft Azure Government and [Microsoft Office 365 U.S. Government](#) cloud services provide a contractual commitment that they have the appropriate controls in place, and the security capabilities necessary for Microsoft agency customers to meet the substantive requirements of IRS 1075.

These Microsoft cloud services for government provide a platform on which customers can build and operate their solutions, but customers must determine for themselves whether those specific solutions are operated in accordance with IRS 1075 and are, therefore, subject to IRS audit.

To help government agencies in their compliance efforts, Microsoft:

- Offers detailed guidance to help agencies understand their responsibilities and how various IRS controls map to capabilities in Azure Government and Office 365 U.S. Government. The IRS 1075 Safeguard Security Report (SSR) thoroughly documents how Microsoft services implement the applicable IRS controls, and is based on the FedRAMP packages of Azure Government and Office 365 U.S. Government. Because both IRS 1075 and FedRAMP are based on NIST 800-53, the compliance boundary for IRS 1075 is the same as the FedRAMP authorization.
- The IRS must explicitly approve the release of any IRS Safeguards document, so only government customers under NDA can review the SSR.
- Makes available audit reports and monitoring information produced by independent assessors for its cloud services.
- Provides to the IRS Azure Government Compliance Considerations and Office 365 U.S. Government Compliance Considerations, which outline how an agency can use Microsoft Cloud for Government services in a way that complies with IRS 1075. Government customers under NDA can request these documents.
- Offers customers the opportunity (at their expense) to communicate with Microsoft subject matter experts or outside auditors if needed.

## Microsoft in-scope cloud services

FedRAMP authorizations are granted at three impact levels based on NIST guidelines — low, medium, and high. These rank the impact that the loss of confidentiality, integrity, or availability could have on an organization —

low (limited effect), medium (serious adverse effect), and high (severe or catastrophic effect).

- [Azure and Azure Government](#)
- Dynamics 365 U.S. Government
- [Office 365 and Office 365 U.S. Government](#)
- Office 365 U.S. Government Defense
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Audits, reports, and certificates

Compliance with the substantive requirements of IRS 1075 is covered under the FedRAMP audit every year.

- [FedRAMP authorizations](#)
- [Azure IRS 1075 safeguard security report](#)

## Frequently asked questions

**How does Microsoft address the requirements of IRS 1075?**

Microsoft regularly monitors its security, privacy, and operational controls and NIST 800-53 rev. 4 controls required by the FedRAMP baseline for Moderate Impact information systems. It provides quarterly access to this information through continuous monitoring reports. Azure Government and Office 365 U.S. Government customers can access this sensitive compliance information through the [Service Trust Portal](#).

In addition, Microsoft has committed to including IRS 1075 controls in its master control set for Azure Government and Office 365 U.S. Government, and to auditing against them annually.

**Can I review the FedRAMP packages or the System Security Plan?**

Yes, if your organization meets the eligibility requirements for Azure Government and Office 365 U.S. Government. Contact your Microsoft account representative directly to review these documents. You can also refer to the FedRAMP list of compliant cloud service providers.

**Can I use the Azure or Office 365 public cloud environments and still be compliant with IRS 1075?**

No. The only environments where FTI can be stored and processed are Azure Government or Office 365 U.S. Government. Government customers must meet the eligibility requirements to use these environments.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [IRS Publication 1075](#)
- [IRS Safeguards Program](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Microsoft Cloud for Government](#)
- [Compliance on the Microsoft Trust Center](#)

# International Traffic in Arms Regulations (ITAR)

11/30/2020 • 2 minutes to read • [Edit Online](#)

## ITAR overview

The US Department of State is responsible for managing the export and temporary import of defense articles (meaning any item or technical data designated under the US Munitions List, as described in Title 22 CFR 121.1) that are governed by the Arms Export Control Act (Title 22 USC 2778) and the International Traffic in Arms Regulations (ITAR) (Title 22 CFR 120–130). The Directorate for Defense Trade Controls (DDTC) is responsible for managing entities governed under these programs.

## Microsoft and ITAR

Microsoft provides certain cloud services or service features that can support customers with ITAR obligations. While there is no compliance certification for the ITAR, Microsoft operates and has designed in-scope services to be capable of supporting a customer's ITAR obligations and compliance program.

Microsoft Azure Government and Microsoft Office 365 U.S. Government for Defense provide support for customers with data subject to the ITAR through additional contractual commitments to customers regarding the location of stored data, and limitations on the ability to access such data to US persons. Microsoft provides these assurances for the infrastructure and operational components of these government cloud services, but customers are ultimately responsible for the protection and architecture of their applications within their environments.

Customers must sign additional agreements formally notifying Microsoft of their intention to store ITAR-controlled data, so that Microsoft may comply with responsibilities both to our customers and to the US government.

The ITAR has specific obligations to report violations, which can provide certain risk mitigation benefits. The Microsoft Enterprise Agreement Amendment enables Microsoft and the customer to work together in reporting such violations.

Customers seeking to host ITAR-regulated data should work with their Microsoft account and licensing teams to learn more, obtain proper agreements, and access relevant system architecture information.

## Microsoft in-scope cloud services

- [Azure Government](#)
- [Office 365 U.S. Government Defense](#)

## Frequently asked questions

**Where can I request compliance information?**

Contact your Microsoft account representative.

## Resources

- [DDTC ITAR](#)
- [ITAR Title 22 CFR 120–130](#)
- [Using Azure Government with ITAR controlled data](#)

- [Azure Government](#)
- [Office 365 U.S. Government](#)
- [Compliance on the Microsoft Trust Center](#)



# Microsoft 365 NIST 800-53 action plan — Top priorities for your first 30 days, 90 days, and beyond

2/5/2021 • 8 minutes to read • [Edit Online](#)

Microsoft 365 allows you to operate your enterprise with a cloud control framework, which aligns controls with multiple regulatory standards. Microsoft 365 includes Office 365, Windows 10, and Enterprise Mobility + Security. Microsoft's internal control system is based on the National Institute of Standards and Technology (NIST) special publication 800-53, and Office 365 has been accredited to latest NIST 800-53 standard.

Microsoft is recognized as an industry leader in cloud security. Using years of experience building enterprise software and running online services, our team is constantly learning and continuously updating our services and applications to deliver a secure cloud productivity service that meets rigorous industry standards for compliance. Microsoft's government cloud services, including Office 365 U.S. Government, meet the demanding requirements of the US Federal Risk and Authorization Management Program (FedRAMP), enabling U.S. federal agencies to benefit from the cost savings and rigorous security of the Microsoft Cloud.

This article includes a prioritized action plan you can follow as you work to meet the requirements of NIST 800-53. This action plan was developed in partnership with Protiviti, a Microsoft partner specializing in regulatory compliance.

## Action plan outcomes

These recommendations are provided across three phases in a logical order with the following outcomes:

PHASE	OUTCOMES
30 days	<ul style="list-style-type: none"><li>* Understand your NIST 800-53 requirements and consider engaging with a Microsoft Advisory Partner.</li><li>* Learn and understand the Microsoft 365 built-in defense-in-depth strategy.</li><li>* Protect user and administrator access to Office 365.</li><li>* Ensure all access to the system is auditable according to your organization's audit and accountability policies.</li></ul>
90 days	<ul style="list-style-type: none"><li>* Enhance your anti-malware, patching, and configuration management program.</li><li>* Use Microsoft 365 security capabilities to control access to the environment and to protect organizational information and assets.</li><li>* Utilize built in auditing capabilities to monitor sensitive or risky activities within Office 365.</li><li>* Deploy Advanced Threat Protection for both links and attachments in email and Office documents.</li></ul>

PHASE	OUTCOMES
Beyond 90 days	<ul style="list-style-type: none"> <li>* Use Microsoft 365 advanced tools and information protection to implement ongoing controls for devices and protection for corporate data.</li> <li>* Monitor ongoing compliance across Microsoft 365 and other Cloud applications.</li> <li>* Use enhanced threat detection and protection capabilities with advanced threat analytics to provide a robust and layered security strategy for the organization. Develop an incident response plan to mitigate the effects of compromised systems in your organization.</li> </ul>

## 30 days — Powerful Quick Wins

These tasks can be accomplished quickly and have low impact to users.

AREA	TASKS
Understand your NIST 800-53 requirements and consider engaging with a Microsoft Advisory Partner.	<ul style="list-style-type: none"> <li>• Work with your Microsoft Partner to perform a gap analysis of your NIST 800-53 compliance for the organization and to develop a roadmap that charts your journey to compliance.</li> <li>• Use guidance in <a href="#">Microsoft Compliance Manager</a> to define and document policies and procedures for both access control and information sharing which addresses purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance.</li> </ul>
Learn and understand the Microsoft 365 built-in defense-in-depth strategy.	<ul style="list-style-type: none"> <li>• Assess and manage your compliance risks by using <a href="#">Compliance Manager</a> to conduct an NIST 800-53 assessment of your organization. Align Microsoft 365 security controls for managing and mitigating risks to the assessment's outcomes.</li> <li>• Utilize <a href="#">Microsoft Secure Score</a> to track the organization's usage of Microsoft 365 security capabilities over time within both Office 365 and on Windows 10 desktops.</li> <li>• Learn about Microsoft's technologies and strategies used to provide <a href="#">Office 365 data encryption</a>, as well as strategies for <a href="#">protection against denial-of-service attacks</a> in the Microsoft Cloud.</li> </ul>
Protect user and administrator access to Office 365.	<ul style="list-style-type: none"> <li>• Establish <a href="#">strong credential management</a> to protect user account credentials.</li> <li>• Learn about <a href="#">recommended identity and device access policies</a> for Office 365 services.</li> <li>• Utilize the <a href="#">Office 365 administrative roles</a> to implement role-based access to administration capabilities and to enable separation of administration duties. Note: many administrator roles in Office 365 have a corresponding role in Exchange Online, SharePoint Online, and Skype for Business Online. Segment permissions to ensure that a single administrator does not have greater access than necessary.</li> </ul>
Ensure all access to the system is audited according to your organization's audit and accountability policies.	Enable <a href="#">audit logging</a> and <a href="#">mailbox auditing</a> (for all Exchange mailboxes) to monitor Office 365 for potentially malicious activity and to enable forensic analysis of data breaches.

## 90 days — Enhanced Protections

These tasks take a bit more time to plan and implement.

AREA	TASKS
Enhance your Anti-malware, patching, and configuration management program.	<ul style="list-style-type: none"><li>• Protect corporate assets and desktops by deploying and enabling <a href="#">Windows Defender Antivirus</a> to your organization and leveraging its tight integration with Windows 10.</li><li>• Keep track of quarantined infected systems and prevent further damage until remediation steps are taken.</li><li>• Confidently rely on Microsoft 365 rigorous standard change management process for trusted updates, hotfixes, and patches.</li></ul>
Use Microsoft 365 security capabilities to control access to the environment and to protect organizational information and assets.	<ul style="list-style-type: none"><li>• Implement <a href="#">recommended identity and device access policies</a> to protect user and administrative accounts.</li><li>• Implement <a href="#">Office 365 Message Encryption (OME)</a> capabilities to help users comply with your organization's policies when sending sensitive data via email.</li><li>• Deploy <a href="#">Windows Defender Advanced Threat Protection (ATP)</a> to all desktops for protection against malicious code, as well as data breach prevention and response.</li><li>• Configure, test and deploy policies to identify, monitor and <a href="#">automatically protect</a> over 80 common sensitive data types within documents and emails, including financial, medical, and personally identifiable information.</li><li>• Automatically inform email senders that they may be about to violate one of your policies — even before they send an offending message by configuring <a href="#">Policy Tips</a>. Policy Tips can be configured to display a brief note (in Outlook, Outlook on the web, and OWA for devices) that provides information about possible policy violations during message creation.</li><li>• Protect sensitive corporate data and meet your organization's information sharing policies by implementing controls for <a href="#">external sharing in SharePoint Online and OneDrive for Business</a>. Ensure only authenticated external users can access corporate data.</li></ul>
Utilize built in auditing capabilities to monitor sensitive or risky activities within Office 365.	<ul style="list-style-type: none"><li>• Enable <a href="#">Alert Policies</a> in the Microsoft 365 security or compliance center to raise automatic notifications when sensitive activities occur, such as when a user's account privileges are elevated or when sensitive data is accessed. All privileged functions should be audited and monitored.</li><li>• On a regular cadence, <a href="#">search your audit logs</a> in the security or compliance center to review changes that have been made to the tenant's configuration settings.</li><li>• For long-term storage of audit log data, use the Office 365 Management Activity API reference to integrate with a security information and event management (SIEM) tool.</li></ul>
Deploy Advanced Threat Protection for both links and attachments in email and Office documents.	Implement <a href="#">Office 365 Advanced Threat Protection (ATP)</a> to help prevent the most common attack vectors including phishing emails and Office documents containing malicious links and attachments.

## Beyond 90 Days: Ongoing Security, Data Governance, and Reporting

These actions take longer and build on previous work.

AREA	TASKS
<p>Use Microsoft 365 advanced tools and information protection to implement ongoing controls for devices and protection for corporate data.</p>	<ul style="list-style-type: none"> <li>* Use <a href="#">Microsoft Intune</a> to protect sensitive data stored and accessed on mobile devices and to ensure compliant corporate devices are used to access cloud services.</li> </ul>
<p>Monitor ongoing compliance across Microsoft 365 and other Cloud applications.</p>	<ul style="list-style-type: none"> <li>* To evaluate performance against the organization's defined policies and procedures, use <a href="#">Compliance Manager</a> on an ongoing basis to perform regular assessments of the organization's enforcement of information security policies.</li> <li>* Use <a href="#">Azure AD Privileged Identity Management</a> to control and perform regular reviews of all users and groups with high levels of permissions (i.e. privileged or administrative users).</li> <li>* Deploy and configure <a href="#">Privileged Access Management</a> to provide granular access control over privileged admin tasks in Office 365. Once enabled, users will need to request just-in-time access to complete elevated and privileged tasks through an approval workflow that is highly scoped and time-bound.</li> <li>* Audit <a href="#">non-owner mailbox access</a> to identify potential leaks of information and to proactively review non-owner access on all Exchange Online mailboxes.</li> <li>* Use <a href="#">Office 365 Alert Policies, data loss prevention reports, and Microsoft Cloud App Security</a> to monitor your organization's usage of cloud applications and to implement advanced alerting policies based on heuristics and user activity.</li> <li>* Use <a href="#">Microsoft Cloud App Security</a> to automatically track risky activities, to identify potentially malicious administrators, to investigate data breaches, or to verify that compliance requirements are being met.</li> </ul>
<p>Leverage enhanced threat detection and protection capabilities with advanced threat analytics to provide a robust and layered security strategy for the organization. Develop an incident response plan to mitigate the effects of compromised systems in your organization.</p>	<ul style="list-style-type: none"> <li>* Deploy and configure <a href="#">Windows Advanced Threat Analytics</a> to leverage rich analytics and reporting to gain critical insights into which users are being targeted in your organization and the cyber-attack methodologies being exploited.</li> <li>* Leverage <a href="#">Office 365 Advanced Threat Protection reports and analytics</a> to analyze threats through insights into malicious content and malicious emails automatically detected within your organization. Utilize built-in reports and message trace capabilities to investigate email messages that have been blocked due to an unknown virus or malware.</li> <li>* Use <a href="#">Office 365 Threat Intelligence</a> to aggregate insights and information from various sources to get a holistic view of your cloud security landscape.</li> <li>* <a href="#">Integrate Office 365 Threat Intelligence and Windows Defender Advanced Threat Protection</a> to quickly understand if users' devices are at risk when investigating threats in Office 365.</li> <li>* Simulate common attack methods within your Office 365 environment using the <a href="#">Office 365 Attack Simulator</a>. Review results from attack simulations to identify training opportunities for users and to validate your organization's incident response procedures.</li> <li>* Configure <a href="#">permissions within the security or compliance center</a> to ensure access to monitoring and audit data is restricted to approved users and integrated with the organization's incident response measures.</li> </ul>

AREA	TASKS

## Learn more

Learn more about [Microsoft and the NIST Cyber Security Framework \(CSF\)](#), including NIST 800-53.

# NIST SP 800-171

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About NIST SP 800-171

The US National Institute of Standards and Technology (NIST) promotes and maintains measurement standards and guidelines to help protect the information and information systems of federal agencies. In response to Executive Order 13556 on managing controlled unclassified information (CUI), it published [NIST SP 800-171](#), *Protecting Controlled Unclassified Information In Nonfederal Information Systems and Organizations*. CUI is defined as information, both digital and physical, created by a government (or an entity on its behalf) that, while not classified, is still sensitive and requires protection.

NIST SP 800-171 was originally published in June 2015 and has been updated several times since then in response to evolving cyberthreats. It provides guidelines on how CUI should be securely accessed, transmitted, and stored in nonfederal information systems and organizations; its requirements fall into four main categories:

- Controls and processes for managing and protecting
- Monitoring and management of IT systems
- Clear practices and procedures for end users
- Implementation of technological and physical security measures

## Microsoft and NIST SP 800-171

Accredited third-party assessment organizations, Kratos Secureinfo and Coalfire, partnered with Microsoft to attest that its in-scope cloud services meet the criteria in NIST SP 800-171, *Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations*, when they process CUI. The [Microsoft implementation of FedRAMP](#) requirements help ensure Microsoft in-scope cloud services meet or exceed the requirements of NIST SP 800-171 using the systems and practices already in place.

NIST SP 800-171 requirements are a subset of NIST SP 800-53, the standard that FedRAMP uses. Appendix D of NIST SP 800-171 provides a direct mapping of its CUI security requirements to the relevant security controls in NIST SP 800-53, for which the in-scope cloud services have already been assessed and authorized under the FedRAMP program.

Any entity that processes or stores US government CUI — research institutions, consulting companies, manufacturing contractors, must comply with the stringent requirements of NIST SP 800-171. This attestation means Microsoft in-scope cloud services can accommodate customers looking to deploy CUI workloads with the assurance that Microsoft is in full compliance. For example, all DoD contractors who process, store, or transmit 'covered defense information' using in-scope Microsoft cloud services in their information systems meet the US Department of Defense DFARS clauses that require compliance with the security requirements of NIST SP 800-171.

## Microsoft in-scope cloud services

- [Azure Government](#)
- [Azure Commercial](#)
- [Dynamics 365 U.S. Government](#)
- Intune
- [Office 365 U.S. Government Community Cloud \(GCC\), Office 365 GCC High, and DoD](#)

## Audits, reports, and certificates

- [Azure Government Attestation of Compliance with NIST SP 800-171](#)

## How to implement

- [Azure Blueprint samples](#): Get support for implementing workloads that comply with NIST-based controls.

## Frequently asked questions

### Can I use Microsoft compliance with NIST SP 800-171 for my organization?

Yes. Microsoft customers may use the audited controls described in the reports from independent third-party assessment organizations (3PAO) on FedRAMP standards as part of their own FedRAMP and NIST risk analysis and qualification efforts. These reports attest to the effectiveness of the controls Microsoft has implemented in its in-scope cloud services. Customers are responsible for ensuring that their CUI workloads comply with NIST SP 800-171 guidelines.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Microsoft DoD Certification Meets NIST 800-171 Requirements](#)
- [NIST 800-171 Compliance Starts with Cybersecurity Documentation](#)
- [Microsoft Cloud Services FedRAMP Authorizations](#)
- [NIST 800-171 3.3 Audit and Accountability with Office 365 GCC High](#)
- [Microsoft and the NIST Cybersecurity Framework](#)
- [Microsoft Government Cloud](#)
- [Compliance on the Microsoft Trust Center](#)

# National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

2/5/2021 • 5 minutes to read • [Edit Online](#)

## NIST CSF overview

The National Institute of Standards and Technology (NIST) promotes and maintains measurement standards and guidance to help organizations assess risk. In response to Executive Order 13636 on strengthening the cybersecurity of federal networks and critical infrastructure, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (FICIC) in February 2014.

The main priorities of the FICIC were to establish a set of standards and practices to help organizations manage cybersecurity risk, while enabling business efficiency. The NIST Framework addresses cybersecurity risk without imposing additional regulatory requirements for both government and private sector organizations.

The FICIC references globally recognized standards including NIST SP 800-53 found in Appendix A of the NIST's [Framework for Improving Critical Infrastructure Cybersecurity](#). Each control within the FICIC framework is mapped to corresponding NIST 800-53 controls within the FedRAMP Moderate Baseline.

## Microsoft and the NIST CSF

NIST Cybersecurity Framework (CSF) is a voluntary Framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks. Microsoft Cloud services have undergone independent, third-party FedRAMP Moderate and High Baseline audits and are certified according to the FedRAMP standards. Also, through a validated assessment performed by HITRUST, a leading security and privacy standards development and accreditation organization, Office 365 is certified to the objectives specified in the NIST CSF.

Learn how to accelerate your NIST Cybersecurity Framework deployment with Compliance Score and our Azure Security and Compliance Blueprint:

- [Overview of the NIST SP 800-53 R4 blueprint sample](#)
- [Learn more about the NIST CSF assessment for Office 365 in Compliance Score](#)

## Microsoft in-scope cloud services

- [Azure Government](#)
- [Dynamics 365 for Government](#)
- [Office 365 and Office 365 U.S. Government](#)

## Audit cycle and certification

The NIST CSF certification of Office 365 is valid for two years.

- [Office 365 NIST CSF Letter of Certification](#)

## Quickly build NIST CSF solutions on Azure

The NIST Cybersecurity Framework (CSF) standard can be challenging in the cloud. Fortunately, with Azure you'll have a head start the Azure Security and Compliance NIST CSF Blueprint. This blueprint provides tools and guidance to get you started building NIST CSF-compliant solutions today.



- [Start using the Azure NIST CSF Blueprint](#)

## Perform risk assessment on Office 365 using NIST CSF in Compliance Score

Cybersecurity remains a critical management issue in the era of digital transforming. To help you implement and verify security controls for your Office 365 tenant, Microsoft provides recommended customer actions in the NIST CSF Assessment in Compliance Score.

- [Start using Compliance Score](#)

## Frequently asked questions

### **Has an independent assessor validated that Azure Government, Dynamics 365, and Office 365 support NIST CSF requirements?**

Yes, a third-party assessment organization has attested that the Azure Government cloud service offering conforms to the NIST Cybersecurity Framework (CSF) risk management practices, as defined in the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, dated February 12, 2014. The NIST CSF is mapped to FedRAMP Moderate controls framework and an independent assessor has assessed Dynamics 365 against the FedRAMP Moderate baseline. Also, Office 365 obtained [the NIST CSF letter of certification](#) from HITRUST in June 2018.

### **How do Microsoft Cloud Services demonstrate compliance with the framework?**

Using the formal audit reports prepared by third parties for the FedRAMP accreditation, Microsoft can show how relevant controls noted within these reports demonstrate compliance with the NIST Framework for Improving Critical Infrastructure Cybersecurity. Audited controls implemented by Microsoft serve to ensure the confidentiality, integrity, and availability of data stored, processed, and transmitted by Azure, Office 365, and Dynamics 365 that have been identified as the responsibility of Microsoft.

### **What are Microsoft's responsibilities for maintaining compliance with this initiative?**

Participation in the FICIC is voluntary. However, Microsoft ensures that Azure, Office 365, and Dynamics 365 meet the terms defined within the governing Online Services Terms and applicable service level agreements. These define Microsoft's responsibility for implementing and maintaining controls adequate to secure the Azure platform and monitor the system.

### **Can I use Microsoft's compliance for my organization?**

Yes. The independent third-party compliance reports to the FedRAMP standards attest to the effectiveness of the controls Microsoft has implemented to maintain the security and privacy of the Microsoft Cloud Services. Microsoft customers may use the audited controls described in these related reports as part of their own FedRAMP and NIST FICIC's risk analysis and qualification efforts.

### **Which organizations are deemed by the United States Government to be critical infrastructure?**

According to the [Department of Homeland Security](#), these include organizations in the following sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear (Reactors Materials and Waste), Transportation Systems and Water (and Wastewater).

### **What are the in-scope services for Office 365?**

The in-scope services of NIST CSF certification are Exchange Online Archiving, Exchange Online Protection, Exchange Online, Skype for Business, Admin Center, SharePoint Online, Project Online, OneDrive for Business,

Office Online, MyAnalytics, Microsoft Teams, Microsoft 365 Apps for enterprise in Office 365 Multi-tenant cloud and Office 365 GCC.

#### NOTE

Microsoft 365 Apps for enterprise enables access to various cloud services, such as Roaming Settings, Licensing, and OneDrive consumer cloud storage, and may enable access to additional cloud services in the future. Roaming Settings and Licensing support the standards for HITRUST. OneDrive consumer cloud storage does not, and other cloud services that are accessible through Microsoft 365 Apps for enterprise and that Microsoft may offer in the future also may not, support these standards.\*

#### Why are some Office 365 services not in the scope of this certification?

Microsoft provides the most comprehensive offerings compared to other cloud service providers. To keep up with our broad compliance offerings across regions and industries, we include services in the scope of our assurance efforts based on the market demand, customer feedback, and product lifecycle. If a service is not included in the current scope of a specific compliance offering, your organization has the responsibility to assess the risks based on your compliance obligations and determine the way you process data in that service. We continuously collect feedback from customers and work with regulators and auditors to expand our compliance coverage to meet your security and compliance needs.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Microsoft Cloud Services Authorizations](#)
- [Mapping Microsoft Cyber Offerings to: NIST Cybersecurity Framework \(CSF\), CIS Controls, ISO27001:2013 and HITRUST CSF](#)
- [Framework for Improving Critical Infrastructure Cybersecurity](#)
- [Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure](#)
- [Microsoft Government Cloud](#)
- [Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

# U.S. Section 508

11/30/2020 • 2 minutes to read • [Edit Online](#)

## About U.S. Section 508

The United States Congress amended the Rehabilitation Act in 1998 and 2000 to require federal agencies to make their electronic and information technology (EIT) products, such as software, hardware, electronic content, and support documentation, accessible to people with disabilities. Section 508 of the United States Workforce Rehabilitation Act of 1973 (29 US Code §794d), as amended, mandates that federal agencies procure, maintain, and use EIT in a manner that ensures federal employees with disabilities have comparable access to, and use of, data and EIT relative to other federal employees.

Microsoft is a major software and cloud-services provider to U.S. federal and state governments. To assist government customers in making procurement decisions, Microsoft publishes Accessibility Conformance Reports describing the extent to which our products and services support the criteria of Section 508. This information can help Microsoft customers determine whether a particular product or service will meet their specific needs.

## Microsoft and U.S. Section 508

Microsoft's consideration of U.S. Section 508 in the development of products and services points to its commitment to making technology and data accessible for all customers.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Azure DevOps Services
- Dynamics 365 and Dynamics 365 U.S. Government
- Intune
- [Office 365 and Office 365 U.S. Government](#)
- [Office 365 U.S. Government Defense](#)
- Windows Server 2016

## Microsoft accessibility conformance reports

Find [conformance reports](#) for all our products and services.

## Resources

- [Microsoft accessibility page](#): Explore the ways in which Microsoft innovates so everyone has the ability to achieve more.
- [Office 365 Accessibility Center](#): Office 365 resources for people with disabilities.
- [Enterprise Disability Answer Desk](#): Dedicated support for enterprise customers with accessibility questions about our products and services or compliance.
- [DHS Trusted Tester Program](#): Get information about the U.S. Department of Homeland Security (DHS) Trusted Tester Program, in which Microsoft participates.
- [Compliance on the Microsoft Trust Center](#)

# Family Educational Rights and Privacy Act (FERPA)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## FERPA overview

The Family Educational Rights and Privacy Act (FERPA) is a US federal law that protects the privacy of students' education records, including personally identifiable and directory information. FERPA was enacted to ensure that parents and students age 18 and older can access those records, request changes to them, and control the disclosure of information, except in specific and limited cases where FERPA allows for disclosure without consent.

The law applies to schools, school districts, and any other institution that receives funding from the US Department of Education — that is, virtually all public K–12 schools and school districts, as well as most post-secondary institutions, both public and private.

Security is central to compliance with FERPA, which requires the protection of student information from unauthorized disclosures. Educational institutions that use cloud computing need contractual reassurances that a technology vendor manages sensitive student data appropriately.

## Microsoft and (FERPA)

FERPA does not require or recognize audits or other certifications, so any academic institution that is subject to FERPA must assess for itself whether and how its use of a cloud service affects its ability to comply with FERPA requirements. However, Microsoft has made the following contractual commitments that attest to its compliance:

- In its [Online Services Terms](#), Microsoft agrees to be designated as a “school official” with “legitimate educational interests” in customer data as defined under FERPA. (Customer data would include any student records provided through a school’s use of Microsoft cloud services.) When handling student education records, Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) just as school officials do.
- Furthermore, Microsoft commits to using customer data only to provide organizations with its cloud services and compatible purposes (such as improving malware detection), and does not mine customer data for advertising.
- Microsoft also contractually commits not to disclose customer data except as the educational institution directs, as described in the contract, or as required by law. Schools that provide education records to Microsoft through their use of a Microsoft cloud service can thus be assured that those records are subject to stringent contractual restrictions regarding their use and disclosure.

As a result of these contractual commitments, customers that are subject to FERPA — both educational institutions and third parties to whom they give access to sensitive student data — can confidently use in-scope Microsoft business cloud services to process, store, and transmit that data.

## Microsoft in-scope cloud services

Services for which Microsoft agrees to be designated as a 'school official' with 'legitimate educational interests' in customer data include:

- [Azure](#)
- [Dynamics 365](#)
- [Intune](#)

- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)
- Power BI, PowerApps, and Power Automate (formerly Microsoft Flow) either as a standalone service or as included in an Office 365 branded plan or suite
- Azure DevOps Services
- Windows Defender ATP

## Audits, reports, and certificates

FERPA does not require or recognize audits or certifications.

## Frequently asked questions

### Why is FERPA important?

This US federal law mandates the protection of the privacy of students' education records. It also gives parents and eligible students access to those records and the ability to correct them, as well as certain rights related to the release of records to third parties.

### Where can I find more information on FERPA?

- [Federal Register: FERPA Final Rule](#) (December 2011)
- [FERPA general guidance for parents](#)

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Family Educational Rights and Privacy Act](#)
- [Electronic Code of Federal Regulations: FERPA](#)
- [Federal Register: FERPA Final Rule](#)
- [FERPA implementation guide for Microsoft Azure](#)
- [Azure FERPA compliance framework mapping](#)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

# North American Electric Reliability Corporation (NERC)

2/5/2021 • 6 minutes to read • [Edit Online](#)

## About the NERC

The [North American Electric Reliability Corporation](#) (NERC) is a nonprofit regulatory authority whose mission is to ensure the reliability of the North American bulk power system. NERC is subject to oversight by the US Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. In 2006, FERC granted the Electric Reliability Organization (ERO) designation to NERC in accordance with the Energy Policy Act of 2005 (US Public Law 109-58). NERC develops and enforces reliability standards known as NERC [Critical Infrastructure Protection \(CIP\) standards](#).

## Microsoft and the NERC CIP standard

The North American Electric Reliability Corporation (NERC) is a nonprofit regulatory authority whose mission is to ensure the reliability of the North American bulk power system. NERC is subject to oversight by the US Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. In 2006, FERC granted the Electric Reliability Organization (ERO) designation to NERC in accordance with the Energy Policy Act of 2005 (US Public Law 109-58). NERC develops and enforces reliability standards known as NERC [Critical Infrastructure Protection \(CIP\) standards](#).

All bulk power system owners, operators, and users must [comply with NERC CIP standards](#). These entities are required to register with NERC. Cloud Service Providers and third-party vendors are not subject to NERC CIP standards; however, the CIP standards include goals that should be considered when [Registered Entities](#) use vendors in the operation of the Bulk Electric System (BES). Microsoft customers operating Bulk Electric Systems are wholly responsible for ensuring their own compliance with NERC CIP standards. Neither Microsoft Azure nor Microsoft Azure Government constitutes a BES or BES Cyber Asset.

As stated by NERC in the current set of [CIP standards](#) and the NERC [Glossary of Terms](#), BES Cyber Assets perform real-time functions of monitoring or controlling the BES, and would affect the reliable operation of the BES within 15 minutes of being impaired. To properly accommodate BES Cyber Assets and Protected Cyber Assets in cloud computing, existing definitions in NERC CIP standards would [need to be revised](#). However, there are many workloads that deal with CIP sensitive data and do not fall under the 15-minute rule, including the broad category of BES Cyber System Information (BCSI).

Azure and Azure Government are suitable for Registered Entities deploying certain workloads subject to NERC CIP standards, including BCSI workloads. Microsoft makes the following documents available to Registered Entities interested in deploying data and workloads subject to NERC CIP compliance obligations in Azure or Azure Government:

- [NERC CIP Standards and Cloud Computing](#) is a white paper that discusses compliance considerations for NERC CIP requirements based on established third-party audits that are applicable to cloud service providers such as FedRAMP. It covers background screening for cloud operations personnel and answers common question about logical isolation and multitenancy that are of interest to Registered Entities. It also addresses security considerations for on-premises vs. cloud deployment.
- [Cloud Implementation Guide for NERC Audits](#) is a guidance document that provides control mapping between the current set of NERC CIP standards requirements and the [NIST SP 800-53 Rev 4](#) control set that forms the basis for FedRAMP. It is designed as technical how-to guidance to help Registered Entities address NERC CIP compliance requirements for assets deployed in the cloud. The document contains pre-filled

[Reliability Standard Audit Worksheets \(RSAWs\)](#) narratives that help explain how Azure controls address NERC CIP requirements, and guidance for Registered Entities on how to use Azure services to implement controls that they own.

The NERC ERO Enterprise [released](#) a Compliance Monitoring and Enforcement Program (CMEP) [practice guide](#) to provide guidance to ERO Enterprise CMEP staff when assessing a Registered Entity's process to authorize access to designated BCSI storage locations and any access controls the Registered Entity implemented. Moreover, NERC reviewed Azure control implementation details and FedRAMP audit evidence related to NERC CIP-004-6 and CIP-011-2 standards that are applicable to BCSI. Based on the ERO-issued practice guide and reviewed FedRAMP controls to ensure that Registered Entities encrypt their data, no additional guidance or clarification is needed for Registered Entities to deploy BCSI and associated workloads in the cloud. However, Registered Entities are ultimately responsible for compliance with NERC CIP standards according to their own facts and circumstances. Registered Entities should review the [Cloud Implementation Guide for NERC Audits](#) for help with documenting their processes and evidence used to authorize electronic access to BCSI storage locations, including encryption key management used for BCSI encryption in Azure and Azure Government.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)

## Audits, reports, and certificates

Microsoft is required to recertify its cloud services each year to maintain its P-ATOs and ATOs. To do so, Microsoft must monitor and assess its security controls continuously, and demonstrate that it remains in compliance.

- [Microsoft cloud services authorizations](#)
- [Microsoft FedRAMP Audit Reports](#)

## How to implement

### **NERC CIP Standards and Cloud Computing**

Addresses compliance for Registered Entities considering cloud adoption for workloads subject to NERC CIP standards.

[Learn more](#)

### **Cloud Implementation Guide for NERC Audits**

Technical guidance helps Registered Entities with NERC audits of assets deployed in Azure or Azure Government.

[Learn more](#)

## Frequently asked questions

### **Who is responsible for compliance with NERC CIP standards?**

All bulk power system owners, operators, and users must [comply with NERC CIP standards](#). These entities are required to register with NERC. Cloud Service Providers and third-party vendors are not subject to NERC CIP standards; however, the CIP standards include goals that should be considered when [Registered Entities](#) use vendors in the operation of the Bulk Electric System (BES). Microsoft customers operating Bulk Electric Systems are wholly responsible for ensuring their own compliance with NERC CIP standards. Neither Azure nor Azure Government constitutes a BES or BES Cyber Asset.

To assess the suitability of Azure and Azure Government for data and workloads subject to NERC CIP standards, Registered Entities should consult with their own compliance officers and NERC auditors. They should review

the [Cloud Implementation Guide for NERC Audits](#) for help with documenting their processes and evidence for assets deployed in the cloud.

### What workloads can Registered Entities deploy on Azure and Azure Government?

The NERC [CIP standards](#) and [Glossary of Terms](#) state that BES Cyber Assets perform real-time functions of monitoring or controlling the BES, and that if impaired would, within 15 minutes, affect the reliable operation of the BES. To properly accommodate BES Cyber Assets and Protected Cyber Assets in cloud computing, existing definitions in NERC CIP standards would [need to be revised](#). However, there are many workloads that deal with CIP sensitive data and do not fall under the 15-minute rule, including the broad category of BES Cyber System Information (BCSI).

The NERC ERO Enterprise [released](#) a Compliance Monitoring and Enforcement Program (CMEP) [practice guide](#) to provide guidance to ERO Enterprise CMEP staff when assessing a Registered Entity's process to authorize access to designated BCSI storage locations and any access controls the Registered Entity implemented. Moreover, NERC reviewed Azure control implementation details and FedRAMP audit evidence related to NERC CIP-004-6 and CIP-011-2 standards that are applicable to BCSI. Based on the ERO issued practice guide and reviewed FedRAMP controls to ensure that Registered Entities encrypt their data, no additional guidance or clarification is needed for Registered Entities to deploy BCSI and associated workloads in the cloud. However, Registered Entities are ultimately responsible for compliance with NERC CIP standards according to their own facts and circumstances.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [NERC Compliance Guidance](#)
- [NERC Cyber Security - Supply Chain Risk Management](#)
- [NERC Compliance and Enforcement](#)
- [NERC Organization and Certification](#)
- [Microsoft and FedRAMP](#)
- [Microsoft and CSA STAR Attestation and Certification](#)
- [Microsoft and SOC 2 Reports](#)
- [Compliance on the Microsoft Trust Center](#)



# Title 23 NYCRR Part 500

2/5/2021 • 4 minutes to read • [Edit Online](#)

## Title 23 NYCRR Part 500 overview

In response to the significant and ever-increasing threats to the cybersecurity of information and financial systems, in 2017, the State of New York Department of Financial Services imposed a new set of cybersecurity requirements on financial institutions that are licensed or authorized to do business in the state. This regulation — Title 23 New York Codes, Rules, and Regulation Part 500: Cybersecurity Requirements for Financial Services Companies — is designed to protect customer data and the information technology systems of financial institutions such as state-chartered, private, and international banks, mortgage brokers, and insurance companies.

## Microsoft and Title 23 NYCRR Part 500

Microsoft provides a comprehensive guide, [Microsoft Cloud Services: Supporting Compliance with NYDFS Cybersecurity Requirements](#), for financial services regulated under Title 23 NYCRR Part 500. It explains in depth how Azure, Office 365, and Power BI cloud services support compliance with the requirements. Financial institutions that seek to operate in the global financial center of New York must meet them, so compliance is critical for many institutions.

Follow this guidance to accelerate your compliance with Title 23 NYCRR Part 500: [Microsoft Cloud Services: Supporting Compliance with NYDFS Cybersecurity Requirements](#)

The New York regulations require each financial institution to:

- **Develop and maintain a robust cybersecurity program** starting with an assessment of the institution's specific risk profile and then designing a program that addresses them. The [Microsoft Cloud Financial Services Compliance Program](#) was created to help financial services assess the risks of using Microsoft cloud services. It includes direct engagement with our engineers and corporate risk officers and access to our compliance and security experts.
- **Implement a comprehensive cybersecurity policy** that addresses information security, data governance and classification, access controls, business continuity, and the like. Microsoft offers guidance for developing this policy with in-depth information about our certifications and risk assessments; business continuity and disaster recovery metrics; and diagnostics for logging and auditing.
- **Designate a chief information security officer (CISO)** to manage the cybersecurity program and enforce policy. To help your CISO, Microsoft provides in-depth cybersecurity information about Microsoft cloud deployments through [Azure Security Center](#), [Office 365 Advanced Threat Analytics](#), and [Power BI Security](#).
- **Monitor and test the effectiveness of its cybersecurity program:** Microsoft provides information from audits of its cybersecurity practices that include continuous monitoring, periodic penetration testing, and vulnerability assessments. Customers can conduct their own tests without advance permission from Microsoft.
- **Maintain an audit trail.** Built-in audit functionalities of Azure, Office 365, and Power BI customers generate information that can be used to reconstruct financial transactions and develop audit trail information.
- **Limit access to information systems that contain nonpublic information:** Measures that Azure, Office 365, and Power BI offer a role-based access control (RBAC) process native to each service, strict security and access requirements for every Microsoft administrator, and audits of every request for elevated access privileges.

- **Institute procedures to assess and test the security of externally developed applications:** For developers using Visual Studio, [Security Rules](#) for managed code can help ensure that application cybersecurity threats are detected and mitigated before the code is deployed.
- **Use periodic risk assessments to design and enhance cybersecurity programs:** For customers, Microsoft aggregates information about security threats, provides roadmaps of change management, and regularly updates information about subcontractors. Microsoft also regularly conducts risk assessments of its own services, the results of which are available to customers.
- **Use qualified personnel to manage cybersecurity risks and oversee cybersecurity functions:** Microsoft employs stringent procedures for our employee access to your customer data. If we hire subcontractors, we remain responsible for service delivery, and ensure that subcontractors fully comply with Microsoft privacy and security commitments, including requirements for handling sensitive data, background checks, and non-disclosure agreements.
- **Implement policies and procedures to ensure the security of information held by third-party service providers:** Azure, Office 365, and Power BI make multi-factor authentication available for all inbound connections to company networks; implement controls, including encryption, to protect nonpublic information in transit over external networks and at rest; and offer [Microsoft Online Services Terms](#) that provide for customer notification, incident investigation, and risk mitigation for security incidents.
- **Implement data retention and deletion policies and procedures:** You can always access and extract your customer data stored in Azure, Office 365, and Power BI.
- **Monitor the activity of authorized users, detect unauthorized access, and offer regular cybersecurity awareness training to employees:** Azure, Office 365, and Power BI include outside-in monitoring to raise alerts about incidents, and extensive diagnostics for logging and auditing. [Microsoft Virtual Academy](#) offers online training that covers the cybersecurity of Microsoft cloud services.
- **Develop plans to respond to and recover from cybersecurity incidents:** Microsoft helps you prepare for cybersecurity incidents using a defensive strategy to detect, predict, and prevent security breaches before they occur. When developing your own plans, you can draw on our incident management plan for responding to cybersecurity breaches.

## Microsoft in-scope cloud services

- [Azure](#)
- Intune
- [Office 365](#)
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Frequently asked questions

### What institutions are covered under this regulation?

Consult the New York Department of Financial Services [Who We Supervise](#) to determine whether your institution is governed by this regulation.

## Resources

- [Featured resources](#)
- [New York State Department of Financial Services 23 NYCRR 500: Cybersecurity Requirements For Financial Services Companies](#)
- [FAQs: 23 NYCRR Part 500–Cybersecurity](#)
- [Microsoft Cloud Services: Supporting Compliance with NYDFS Cybersecurity Requirements](#)
- [Compliance on the Microsoft Trust Center](#)

## Other Microsoft resources for financial services

- [Microsoft business cloud services and financial services](#)
- [Microsoft Cloud Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Shared responsibilities for cloud computing-](#)

# Dutch Authority for the Financial Markets and the Central Bank of the Netherlands

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the AFM and DNB

The primary financial regulators in the Netherlands are the [Dutch Authority for the Financial Markets \(Autoriteit Financiële Markten, AFM\)](#) and the [Central Bank of the Netherlands \(De Nederlandsche Bank, DNB\)](#). The AFM, whose role is comparable to the SEC in the United States, is the independent supervisory authority for the savings, lending, investment, and insurance markets.” The DNB, within the European System of Central Banks, determines, and implements monetary policy and exercises prudential supervision of financial organizations for the Netherlands.

Both of these institutions act in concert with the European Banking Authority (EBA), “an independent EU authority that works to ensure effective and consistent prudential regulation and supervision across the European banking sector.” To that end, the EBA has outlined a comprehensive approach to the use of cloud computing by financial institutions in the EU, [Recommendations on outsourcing to cloud services providers](#).

In general, the laws and guidelines support the point of view that cloud computing involving third-party services qualifies as a form of outsourcing, and financial institutions in the Netherlands must address the associated risks before moving business activities to the cloud. These include:

- The Financial Supervision Act (FSA) ([Dutch](#) and [English](#)), issued by the Dutch legislature in 2018, attaches conditions for financial institutions to control the risks associated with outsourcing and ensure that it doesn’t impede regulatory supervision.
- The Circulaire Cloud Computing ([Dutch](#) and [English](#)), issued by the DNB, requires that before supervised Dutch institutions engage in cloud computing, they must inform the DNB of their prospective outsourcing arrangements to ensure that operational processes and risks are under control.

Using a template that the DNB provides, they must submit a mandatory risk analysis that includes:

- An assessment regarding: compliance with current legislation, mutual understanding between the parties regarding the services offered, the stability and reliability of the service provider, where the services are to be provided, and the importance of and degree of reliance on the outsourced services.
- Explicit attention to addressing risks associated with data integrity, confidentiality, and availability.

The [Commission Delegated Regulation EU 2017/565](#) describes at great length the requirements for an outsourcing agreement between investment firms and cloud service providers.

## Microsoft and the AFM and DNB

To help guide financial institutions in the Netherlands considering outsourcing business functions to the cloud, Microsoft has published [a compliance checklist for financial institutions in the Netherlands](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When financial institutions in the Netherlands outsource business activities to the cloud, they must comply with the rules and guidelines of the Dutch Authority for Financial Markets (AFM) and the Central Bank of the Netherlands (DNB) within the broad policy framework of the European Banking Authority (EBA).

The Microsoft checklist helps financial firms in the Netherlands conducting due-diligence assessments of

Microsoft business cloud services and includes:

- An overview of the regulatory landscape for context.
- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Compliance checklist: Netherlands](#): Financial firms can get help when conducting risk assessments of Microsoft business cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Case overviews, tutorials, and other resources to build Azure solutions for financial services.

## Frequently asked questions

### Is regulatory approval required?

No. However, the Circulaire Cloud Computing states that the DNB expects supervised Dutch institutions to submit a risk analysis concerning prospective outsourcing arrangements before engaging in cloud computing.

### Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. The provisions and arrangements to be included in cloud contracts depend on the type of financial institution. Requirements, such as those described in Art. 31 of the Commission Delegated Regulation (EU) 2017/565, are set out in Part 2 of the checklist.

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Compliance on the Microsoft Trust Center](#)

# Australian Prudential Regulation Authority (APRA)

2/5/2021 • 5 minutes to read • [Edit Online](#)

## APRA overview

The [Australian Prudential Regulation Authority](#) (APRA) oversees banks, credit unions, insurance companies, and other financial services institutions in Australia. Recognizing the momentum towards cloud computing, APRA has called on regulated entities to implement a thoughtful cloud-adoption strategy with effective governance, thorough risk assessment, and regular assurance processes. Regulated institutions must comply with the [APRA Prudential Standard CPS 231 Outsourcing](#) when outsourcing a material business activity — any activity that has the potential, if disrupted, to have a significant impact on the financial institution's business operations or ability to manage its risks effectively. Based on its review of outsourcing arrangements involving cloud computing services submitted to APRA, APRA published specific, detailed guidance in its information paper, [Outsourcing involving cloud computing services](#) to help regulated entities assess cloud providers and services more effectively and guide them through the regulatory issues of outsourcing to the cloud. When outsourcing, including to a cloud service, regulated institutions must also review and consider their ongoing compliance with [APRA Prudential Standard CPS 234 Information Security](#).

## Microsoft and APRA

For financial institutions in Australia that are assessing cloud providers and their services, Microsoft has published:

- [Microsoft response to the APRA Information Paper on Cloud](#)
- [Microsoft cloud services: a compliance checklist for financial institutions in Australia](#)
- [Microsoft cloud services: compliance with APRA Prudential Standard CPS 234](#)

Together they demonstrate how financial firms can move data and workloads to Microsoft Azure with the confidence that they are complying with Australian Prudential Regulation Authority (APRA) regulations and guidance.

To learn about the benefits of APRA-compliant financial services on Azure, read the [Regtech meets Fintech: Perpetual and Microsoft transform the finance sector](#) article.

## Microsoft response to the APRA Information Paper on Cloud

This Microsoft paper provides detailed guidance for financial services with a detailed response to each issue raised in the APRA Information Paper [Outsourcing involving cloud computing services](#). The APRA guidelines identify three risk categories into which cloud usage typically falls — low, heightened, and extreme inherent risk — and highlight key issues that regulated entities must consider as part of their risk assessment.

The Microsoft response focuses on the two highest risk categories. While cloud services are not prohibited by any risk category, APRA expects you to undertake a commensurately higher level of diligence, and you should expect an increasing level of APRA scrutiny, as you move up the risk categories. APRA lists a range of factors that typically indicate high or extreme inherent risk for cloud outsourcing. Microsoft addresses each of these factors in depth, providing information and tools to help you assess and manage the risk of moving your data and workloads to Azure.

Microsoft also addresses each APRA risk management consideration: strategy, governance, solution selection process, APRA access and ability to act, transition approach, risk assessments and security, ongoing oversight, business disruption, and audit and assurance. Point by point, we give advice and offer tools to help you respond

to each issue when deploying Azure.

Get practical support for moving data and workloads to Azure in compliance with APRA regulations: [Download the Microsoft response to the APRA Information Paper on Cloud](#).

## Microsoft response to the APRA CPS 234 on Information Security

APRA [Prudential Standard CPS 234 Information Security](#) requires regulated institutions to:

- clearly define information-security related roles and responsibilities;
- maintain an information security capability commensurate with the size and extent of threats to their information assets;
- implement controls to protect information assets and undertake regular testing and assurance of the effectiveness of controls; and
- promptly notify APRA of material information security incidents.

CPS 234 closely mirrors the core Microsoft security framework: protect, detect, and respond.

[Microsoft cloud services: compliance with APRA Prudential Standard CPS 234 Information Security](#) sets out each of the relevant CPS 234 regulatory obligations, and maps against it the Microsoft cloud service controls, capabilities, functions, contract commitments, and supporting information to help your APRA-regulated entity comply with its regulatory obligations under CPS 234.

## Navigating your way to the cloud: A compliance checklist for financial institutions in Australia

This Microsoft checklist introduces APRA regulatory requirements that financial firms must address when moving to the cloud. It maps Azure against not only the [Prudential Standard CPS 231 Outsourcing](#), but other relevant APRA standards, such as for business continuity and risk management. Completing this checklist helps your financial service institutions adopt Azure with the confidence that it meets the relevant APRA requirements.

By relying on our comprehensive approach to risk assurance in the cloud, we are confident that Australian financial services organizations can move to Microsoft cloud services in a manner that is not only consistent with APRA guidance, but can provide customers with a more advanced security risk management profile than on-premises or other hosted solutions.

Get practical support for moving data and workloads to Azure in compliance with APRA regulations: [Download Microsoft cloud services: a compliance checklist for financial institutions in Australia](#).

## Microsoft in-scope cloud services

- [Azure](#)
- [Office 365](#)
- [Dynamics 365](#)

## Frequently asked questions

**Do financial institutions need APRA approval before outsourcing material business activities?**

No. However, most regulated financial organizations must notify APRA after entering into agreements to outsource material business activities within Australia or consult with APRA before outsourcing those activities outside of Australia.

In addition, if the cloud services are deemed to carry 'heightened or extreme inherent risk' as described in the APRA [Information Paper on Clouds](#), the financial institution is encouraged (but not required) to consult with

APRA, regardless of whether the service is provided within or outside of Australia.

### Are transfers of data outside of Australia permitted?

Yes. General privacy legislation (which applies across all sectors, not just to financial institutions) permits transfers outside of Australia under certain conditions. Microsoft agrees to contractual terms in line with Australian Privacy Principles so that transfers of data outside of Australia are permitted when you use Microsoft cloud services. However, many of our Australian financial services customers take advantage of the cloud services available from our Australian datacenters, for which we make specific contractual commitments to store categories of data at rest in the Australian geography. These commitments are outlined further in the [compliance checklist](#).

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Australian Prudential Regulation Authority](#)
- [APRA Information Paper Outsourcing involving cloud computing services](#)
- [Prudential Standard CPS 231 Outsourcing](#)
- [Prudential Standard CPS 234 Information Security](#)
- [Microsoft response to the APRA Information Paper on the Cloud](#)
- [Microsoft cloud services: a compliance checklist for financial institutions in Australia](#)
- [Microsoft cloud services: compliance with APRA Prudential Standard CPS 234](#)
- [Microsoft Australia: Cloud in Financial Services](#)
- [Microsoft Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)
- [Compliance on the Microsoft Trust Center](#)



# Financial Authority (AMF) and Prudential Authority (ACPR) France

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the AMF and ACPR

The [Financial Authority \(Autorité des Marchés Financiers, AMF\)](#) and the [Prudential Authority \(Autorité de Contrôle Prudentiel et de Résolution, ACPR\)](#) are the primary financial regulators in France. In its capacity as the stock market regulator, the AMF is responsible for the supervision of financial markets and investment firms. The ACPR, an independent administrative authority under the central bank, the [Banque de France](#), supervises the banking and insurance sectors.

The AMF and ACPR act in concert with the European Banking Authority (EBA), “an independent EU authority, which works to ensure effective and consistent prudential regulation and supervision across the European banking sector.” To that end, the EBA has outlined a comprehensive approach to the use of cloud computing by financial institutions in the EU, [Recommendations on outsourcing to cloud services providers](#).

There are several requirements and guidelines that financial institutions in France should be aware of when moving operational functions to the cloud:

- The AMF General Regulation ([French](#) and [English](#)) sets rules and procedures to enforce financial legislation. In particular, Article 313-75 sets forth conditions that must be reflected in contracts that financial institutions enter into with cloud service providers.
- ACPR published [The risks associated with cloud computing \(French and English\)](#), which encourages organizations under ACPR supervision to take suitable measures to manage risk when they outsource business functions to the cloud. In addition, [Article 239 in the ACPR Order of 3 November 2014 on the internal control of companies \(French\)](#) under ACPR supervision also specifies mandatory terms to be included in contracts with cloud service providers.
- In certain cases, regulated institutions must notify the AMF and ACPR regarding material outsourcing arrangements, particularly if they have the potential to significantly impact their business operations.
- In its role as the data protection authority for France, the [CNIL](#) (Commission Nationale de l’Informatique et des Libertés) has issued many cloud computing guidelines, including [Recommendations for companies planning to use cloud computing services \(French and English\)](#).

## Microsoft and the AMF and ACPR

To help guide financial institutions in France considering outsourcing business functions to the cloud, Microsoft has published [Navigating your way to the cloud: a checklist for financial institutions in France](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When financial institutions in France outsource business activities to the cloud, they must comply with the requirements of the Financial Authority (AMF) and Prudential Authority (ACPR) of France within the broad policy framework of the European Banking Authority (EBA). In particular, they must be aware of Article 313-75 of the AMF General Regulation, and the ACPR guidelines on cloud computing risks and its mandatory requirements for contracts with cloud service providers.

The Microsoft checklist helps French financial firms conducting due-diligence assessments of Microsoft business cloud services and includes:

- An overview of the regulatory landscape for context.
- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Compliance checklist: France](#): Financial firms can get help conducting risk assessments of Microsoft business cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Use-case overviews, tutorials, and other resources to build Azure solutions for financial services.

## Frequently asked questions

### Is regulatory approval required?

The EBA publication, [Recommendations on outsourcing to cloud services providers] (<https://eba.europa.eu/sites/default/documents/files/documents/10180/1848359/c1005743-567e-40fc-a995-d05fb93df5d1/Draft%20Recommendation%20on%20outsourcing%20to%20Cloud%20Service%20%20%28EBA-CP-2017-06%29.pdf> /5fa5cdde-3219-4e95-946d-0c0d05494362), outlines a comprehensive approach to material outsourcing by financial institutions in the EU. Also, in certain instances, financial firms must notify the AMF or ACPR of their outsourcing arrangements, as described on pages 8 and 9 of the [checklist](#). While it is unlikely these circumstances would apply to the use of Microsoft cloud services, financial services should verify their applicability by reviewing the checklist.

### Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. Article 239 of the [ACPR Order of 3 November 2014](#) and Article 313-75 of the [AMF General Regulation](#) set forth conditions that must be reflected in contracts that financial institutions enter into with cloud service providers. Part 2 of the Microsoft [checklist](#) (page 62) maps these against the sections in Microsoft contractual documents where they are addressed.

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Compliance on the Microsoft Trust Center](#)

# Commodity Futures Trading Commission (CFTC)

## Rule 1.31(c-d) United States

2/5/2021 • 3 minutes to read • [Edit Online](#)

### About CFTC Rule 1.3(c-d)

The [Commodity Futures Trading Commission](#) (CFTC), an independent US federal agency, regulates the commodity futures and options markets and, more recently, the swaps market.

The long-standing CFTC Rule 1.31 defines records retention requirements established by SEC Rule 17a-4(f). In addition, it specifies that electronic records must be maintained for five years and that the originals be kept "readily accessible" during the first two years and made available for inspection by the Commission or the US Department of Justice during the entire retention period.

In 2017, the [CFTC revised its rule](#), amending and modernizing its recordkeeping regulation to adopt less prescriptive, principles-based standards that provide greater flexibility in how records can be maintained. This revision makes the rule more technology neutral, enabling regulated entities to choose the technology most appropriate for their business while maintaining the safeguards that "ensure the reliability of the recordkeeping process." The revised rule removes the requirement that organizations maintain the original records for two years, but retains the five-year maintenance period, which harmonizes practices for firms regulated by both the CFTC and the SEC.

### Microsoft and CFTC Rule 1.31(c-d)

Financial services customers, representing one of the most heavily regulated industries in the world, are subject to complex provisions like the retention of financial transactions and related communication in a non-erasable and non-modifiable state. One of the most prescriptive is Rule 1.31 of the US Commodity Futures Trading Commission (CFTC) that stipulates stringent requirements for regulated entities that elect to retain books and records on electronic storage media. Records stored must be tamper-proof with no ability to alter or delete them until after the designated retention period. Microsoft Azure Immutable Blob Storage with Policy Lock and Microsoft Office 365 with Preservation Lock can help financial institutions meet the storage requirements of CFTC Rule 1.31(c-d).

#### **Microsoft Azure**

To evaluate Azure compliance with CFTC Rule 1.31(c-d), Microsoft retained an independent assessment firm that specializes in records management and information governance, Cohasset Associates. In the resulting report, [CFTC 1.31 \(c\)-\(d\) Compliance Assessment: Microsoft Azure Storage](#), Cohasset validated that [Azure Immutable Blob Storage](#) with the Policy Lock option, when used to retain time-based Blobs in a non-erasable and non-rewritable (WORM) format, meets the principles-based requirements of the CFTC rule. Each Blob (record) is protected from being modified, overwritten, or deleted until the required retention period has expired and any associated legal holds have been released. Software providers and partners with sensitive workloads can now rely on Azure Immutable Blob Storage as a one-stop shop cloud solution for records retention. Financial institutions can now build their own applications taking advantage of these features while remaining compliant.

#### **Microsoft 365**

For [CFTC 1.31\(c-d\)](#) requirements, Cohasset validated that Microsoft 365 includes archiving features that enable regulated customers, including broker-dealers, to store data in a manner that helps them comply with SEC requirements for records retention. Retention features in Microsoft 365 help preserve a wide range of data, including email, voicemail, shared documents, instant messages, and third-party data. In particular, archiving in

Microsoft 365 enables customers to set global or granular messaging retention policies to store data for a defined period and beyond in a non-rewriteable, non-erasable format.

## Microsoft in-scope cloud services

- [Azure](#)
- [Office 365](#)

## Audits, reports, and certificates

[Azure & CFTC Rule 1.31: SEC 17a-4(f) & CFTC 1.31(c-d) Compliance Assessment of Azure Storage

[Office 365 & CFTC Rule 1.31: Archiving in Office 365, data retention, and SEC Rule 17a-4 compliance

## How to implement

- [Financial services regulation](#): Compliance map of key US regulatory principles for cloud computing and Microsoft online services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Use case overviews, tutorials, and other resources to build Azure solutions for financial services.

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Microsoft Office 365 Retention Policies](#)
- [Microsoft Financial Services Blog](#)
- [Compliance on the Microsoft Trust Center](#)

# European Banking Authority (EBA)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the EBA

The [European Banking Authority \(EBA\)](#) is 'an independent authority that works to ensure effective and consistent prudential regulation and supervision across the EU banking sector'. In December 2017, the EBA issued its [Final Report: Recommendations on outsourcing to cloud services providers](#), which outlined a comprehensive approach to the outsourcing of cloud computing by financial institutions in the EU. The recommendations clarify when outsourcing to the cloud is permitted, apply a principles-based approach towards measuring risk from a technology-neutral perspective, and strive towards greater harmonization within Europe and beyond.

The EBA recommendations took effect in July 2018, and they build on and add clarity to the general outsourcing guidelines published in 2006 by the Committee of European Banking Supervisors. In fact, the issuance of these recommendations comes after a consultation period during which Microsoft provided substantive feedback. Many of the final recommendations account for comments Microsoft provided to the EBA.

## Microsoft and the EBA

To help financial institutions in the EU follow the European Banking Authority (EBA) recommendations for cloud adoption, Microsoft published [European Banking Authority Guidance Addresses Cloud Computing for the First Time](#). This document addresses key requirements and explains how Microsoft Azure and Microsoft 365 can be used to satisfy them. The guidance can help financial institutions adopt Azure and Microsoft with the confidence that they can meet their obligations under the EBA framework.

The Microsoft guidance addresses, point by point, each of the EBA recommendations:

- **Audit rights.** Microsoft provides contractual audit rights for customers and rights of examination for regulators in its industry-leading Financial Services Amendment.
- **Notification regarding outsourcing.** Microsoft can assist customers with notifying regulators of material activities to be outsourced.
- **Data residency.** With 36 regions, including six in Europe, Microsoft offers the largest number of datacenters worldwide of any cloud service provider. Organizations can deploy workloads in one region without being required to host data in Europe.
- **Notification regarding subcontractors.** Microsoft leads the industry with a contractual commitment to provide customers with 180-day notice of new subcontractors, and a right to terminate if the customer does not approve of the appointment of a new subcontractor.
- **Business continuity.** Microsoft provides business continuity and resolution provisions in our Financial Services Amendment, including the willingness to provide transition assistance through Microsoft Consulting Services.
- **Risk assessment and security monitoring.** Microsoft enables customers to conduct their own risk assessments and provides tools and dashboards so they can supervise and monitor our cloud services.

For financial institutions in the EU, Microsoft has also published [Risk Assessment and Compliance Guide for Financial Institutions in the Microsoft Cloud](#), a checklist modeled after EBA guidance. It explains how to establish a governance model optimized to meet regulatory requirements, and efficiently evaluate the risks of using Microsoft cloud services, followed by submission for regulatory approval. Our guide includes a list of questions to be answered in a regulatory submission that are drawn from, and responsive to, EBA guidance on outsourcing to cloud service providers.

# Microsoft in-scope cloud services

- [Azure](#)
- [Microsoft 365](#)

## How to implement

- [Response to EBA guidance](#): Microsoft guidance helps EU financial institutions follow EBA recommendations for cloud adoption.
- [Financial use cases](#): Use-case overviews, tutorials, and other resources to build Azure solutions for financial services.
- [Financial Compliance Program](#): Financial institutions can get help with assessing the risks of using Microsoft cloud services.

## Frequently asked questions

### What information should be included in a submission to regulators?

The Microsoft publication, [Risk Assessment and Compliance Guide for Financial Institutions in the Microsoft Cloud](#), offers a checklist of questions that the EBA guidance recommends answering in a regulatory submission, and provides suggestions on how to answer those questions.

## Resources

- [Microsoft Service Trust Portal](#)
- [Microsoft Cloud Checklist for Financial Institutions in Europe](#)
- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Microsoft Financial Services Blog](#)
- [Compliance on the Microsoft Trust Center](#)

# United Kingdom Financial Conduct Authority (FCA)

12/14/2020 • 3 minutes to read • [Edit Online](#)

## FCA (UK) overview

The [Financial Conduct Authority](#) (FCA), an independent public body that is accountable to the Treasury, regulates 58,000 financial firms and markets in the UK and serves as the prudential regulator for over 18,000 of those organizations. [Prudential Regulation Authority](#) (PRA), which also serves as the prudential regulator for the Bank of England and regulates 1,500 of the larger financial services institutions such as banks, building societies, credit unions, insurers, and investment firms. (The FCA picks up prudential regulation for firms that do not fall under the PRA remit.)

The FCA had received feedback that financial institutions and cloud service providers were unclear about how to apply its rules for outsourcing to the cloud, a potential barrier to cloud use. Given that the FCA mandate includes promoting effective competition (for which innovation can be a driver), the FCA wanted to support the use of cloud services, stating “We see no fundamental reason why cloud services (including public cloud services) cannot be implemented, with appropriate consideration, in a manner that complies with our rules.” So the FCA clarified its requirements for outsourcing to the cloud, publishing final guidance in November 2016 in the [Guidance for firms outsourcing to the cloud and other third-party IT services](#) intended to help financial firms and cloud service providers understand FCA expectations when firms outsource to the cloud (or plan to do so). Although this guidance is not binding, the FCA expects firms to use it where appropriate. (Note that the PRA has different statutory objectives, so firms it regulates must confirm their approach with the PRA.) This is a detailed document and offers specific guidance for the use, evaluation, and ongoing monitoring of third parties in the delivery of IT services. It divides considerations into 13 areas of interest, ranging from legal, and regulatory considerations and risk management to continuity planning and plans for exiting outsourcing arrangements

## Microsoft and FCA (UK)

Microsoft has published a comprehensive guide, [Enabling compliance: The Microsoft approach to FCA finalized cloud guidance](#), detailing how Azure can help financial services customers that are authorized and regulated by the UK Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) when moving IT operations to the cloud.

The Microsoft guide describes in great detail our compliance with numerous recognized international standards, our transparency around how your customer data is handled to give you control over it, and the contractual provisions that address-specific financial regulatory requirements.

Sections in the Microsoft guide map in depth to each area of interest in the FCA guidance. For example, a key aspect of the regulatory outsourcing requirements is that financial services firms must identify and manage any risks which outsourcing may introduce into their business. Microsoft discusses its approach in carrying out a risk assessment, documenting it, identifying current best practices, and so on. We help you assess the relevant risks and make available a wide range of resources to facilitate your due diligence.

Learn how Azure is enabling FCA compliance in UK banks: [Read Microsoft collaborates with ClearBank: Launch of first new UK clearing bank in over 250 years](#)

## Accelerate your deployment on Azure

[Download Microsoft approach to FCA finalized cloud guidance](#)

## Microsoft in-scope cloud services

- [Azure](#)
- Intune
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Frequently asked questions

**Can I use Microsoft responses to this framework in my organization's compliance process?**

Yes. However, although Microsoft responses to this framework are confirmed compliant by third parties, customers are responsible for validating the compliance of solutions they have implemented on Azure or Power BI.

## Resources

- [Microsoft Cloud Checklist for Financial Institutions in the UK](#)
- [FG 16/5 — Guidance for firms outsourcing to the cloud and other third-party IT services](#)
- [Enabling compliance: The Microsoft approach to FCA finalized cloud guidance](#)
- [Microsoft Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)
- [Compliance on the Microsoft Trust Center](#)



# Federal Financial Institutions Examination Council (FFIEC)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## FFIEC overview

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body comprising five banking regulators that are responsible for US federal government examinations of financial institutions in the United States. The FFIEC Examiner Education Office publishes IT Examination Handbooks intended for field examiners from FFIEC member agencies.

The [FFIEC Audit IT Examination Handbook](#) contains guidance for these examiners to assess the quality and effectiveness of IT audit programs of both financial institutions and TSPs. Specifically, it includes mention of SOC 1, SOC 2, and SOC 3 attestation reports of the American Institute of Certified Public Accountants (AICPA) as examples of independent audit reports. However, the FFIEC recommends that financial institutions not rely solely on the information contained in these reports, but also use verification and monitoring procedures discussed in detail in the [FFIEC Outsourcing Technology Services IT Examination Handbook](#).

## Microsoft and FFIEC

Microsoft Azure, Microsoft Power BI, and Microsoft Office 365 are built to meet the stringent requirements of Providing cloud services for financial services institutions. As part of our support, we offer guidance to help you comply with FFIEC audit requirements for information technology and the ability to use Azure SOC attestations when pursuing your FFIEC compliance obligations.

To help financial institution clients meet their FFIEC compliance requirements with Azure, Microsoft has developed the [Azure Security and Compliance Blueprint for FFIEC Regulated Services Workloads](#). It offers guidance on the use of Azure cloud services and considerations for customer compliance with FFIEC requirements and risk assessment guidelines.

To further help you comply with FFIEC requirements, Microsoft cloud services provide [SOC attestation reports](#) produced by an independent CPA firm. For example, the SOC 1 Type 2 attestation is based on the AICPA SSAE 18 standard (see AT-C Section 105) that replaced SAS 70, and is appropriate for reporting on certain controls for financial reporting. The SOC reports include the auditor's opinion on the effectiveness of Microsoft controls in achieving the related control objectives during the specified monitoring period. Financial institutions can use this formal audit when pursuing FFIEC-specific compliance obligations for assets deployed on Azure, Power BI, and Office 365.

## Microsoft in-scope cloud services

- [Azure](#)
- Intune
- [Office 365](#)
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Audits, reports, and certificates

Azure and Office 365 SOC attestation reports.

## Frequently asked questions

Can I use Microsoft compliance with SOC standards to meet the FFIEC compliance obligations for my institution?

To help you meet these obligations, Microsoft supplies the specifics about our compliance with SOC standards as described above. However, ultimately, it is up to you to determine whether our services comply with the specific laws and regulations applicable to your institution. The FFIEC also advises that 'users of audit reports or reviews should not rely solely on the information contained in the report to verify the internal control environment of the TSP. They should use other verification and monitoring procedures as discussed more fully in the [Outsourcing Technology Booklet](#) of the FFIEC IT Examination Handbook.'

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Federal Financial Institutions Examination Council \(FFIEC\)](#)
- [Compliance Map of Cloud Computing and Regulatory Principles in the US](#)
- [FFIEC Audit IT Examination Handbook](#)
- [FFIEC Outsourcing Technology Services IT Examination Handbook](#)
- [Azure Security and Compliance FFIEC Financial Services Blueprint](#)

## Other Microsoft resources for financial services

- [Microsoft Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)
- [Shared responsibilities for cloud computing](#)
- [Compliance on the Microsoft Trust Center](#)

# Financial Market Supervisory Authority (FINMA) Switzerland

2/5/2021 • 2 minutes to read • [Edit Online](#)

## About FINMA

The [Financial Market Supervisory Authority](#) (Eidgenössische Finanzmarktaufsicht, FINMA) is the regulator of independent financial markets in Switzerland and is responsible for ensuring that Swiss financial markets function effectively. It has prudential supervision over banks, insurance companies, exchanges, securities dealers, and other financial institutions.

The FINMA published [Circular 2018/3 Outsourcing—banks and insurers](#) to define the requirements that banks, securities dealers, and insurance companies must abide by when they outsource to a service provider any functions that are significant to the company's business activities. Any company that outsources its business activities is accountable to the FINMA just as it would be if it carried out the outsourced functions itself.

## Microsoft and FINMA

To help guide financial institutions in Switzerland considering outsourcing business functions to the cloud, Microsoft has published [A compliance checklist for financial institutions in Switzerland](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When Swiss financial institutions outsource business activities, they must comply with the requirements of the Swiss Financial Market Supervisory Authority (FINMA) and be cognizant of other requirements and guidelines that include those of the Swiss Bank Act, the Swiss Bank Ordinance, and the Swiss Insurance Supervision Act.

The Microsoft checklist helps Swiss financial firms conducting due-diligence assessments of Microsoft business cloud services and includes:

- An overview of the regulatory landscape for context.
- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Compliance checklist: Switzerland](#): Financial firms can get help in conducting risk assessments of Microsoft business cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Use case overviews, tutorials, and other resources to build Azure solutions for financial services.

# Frequently asked questions

## Is regulatory approval required?

No. The use of public cloud computing is permitted without an approval by the FINMA, subject always to compliance with the requirements set out in the regulations and guidelines listed above.

## Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. In Part 2 of the Compliance Checklist, we have mapped these terms against the sections in the Microsoft contractual documents where you find them addressed. In addition, the Swiss Federal Data Protection and Information Commissioner (FDPIC) supplies a sample contract for transborder outsourcing of data processing. This is the same as the Standard Contractual Clauses (also known as [EU Model Clauses](#)) under the [Microsoft Online Services Terms](#).

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Compliance on the Microsoft Trust Center](#)

# Financial Industry Regulatory Authority (FINRA) Rule 4511(c) United States

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About FINRA Rule 4511

The [Financial Industry Regulatory Authority \(FINRA\)](#) is the largest independent body regulating securities firms with oversight of more than 4,500 brokerage firms in the United States. It was authorized by the US Congress “to protect America’s investors by making sure that the broker-dealer industry operates fairly and honestly.”

In 2011, the US Security and Exchange Commission (SEC) approved the FINRA adoption of SEC rules governing the retention of books and records on electronic storage media. [FINRA Rule 4511\(c\)](#) specifies that “all books and records required to be made pursuant to the FINRA rules shall be preserved in a format and media that complies with SEA (Securities Exchange Act) Rule 17a-4.”

Also, FINRA Rule 4511(c) requires firms to preserve for a period of at least six years those books and records for which there is no specified retention period under applicable FINRA or SEA rules. Effectively, if the books and records pertain to an account, the retention period is mandated to be six years following account closure. Otherwise, the retention period is for six years after such books and records are created.

## Microsoft and FINRA Rule 4511(c)

Financial services customers, representing one of the most heavily regulated industries in the world, are subject to complex provisions like the retention of financial transactions and related communication in a non-erasable and non-modifiable state. Among them is Rule 4511 of the Financial Industry Regulatory Authority (FINRA) that stipulates stringent requirements for regulated entities that elect to retain books and records on electronic storage media. Records stored must be tamper-proof with no ability to alter or delete them until after the designated retention period.

Microsoft Azure Immutable Blob Storage with Policy Lock and Microsoft Office 365 with Preservation Lock can help financial institutions meet the immutable storage requirements of FINRA Rule 4511(c).

## Microsoft Azure

To evaluate Azure compliance with FINRA Rule 4511(c), Microsoft retained an independent assessment firm that specializes in records management and information governance, Cohasset Associates. The resulting report, [SEC 17a-4\(f\) & CFTC 1.31 \(c-d\) Compliance Assessment: Microsoft Azure Storage](#), encompasses Azure compliance with FINRA Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f).

Cohasset validated that [Azure Immutable Blob Storage](#) with the Policy Lock option, when used to retain time-based Blobs in a non-erasable and non-rewritable (WORM) format, meets relevant FINRA storage requirements. Each Blob (record) is protected from being modified, overwritten, or deleted until the required retention period has expired and any associated legal holds have been released.

Software providers and partners with sensitive workloads can now rely on Azure Immutable Blob Storage as a one-stop shop cloud solution for records retention and immutable storage. Financial institutions can now build their own applications taking advantage of these features while remaining compliant.

## Microsoft 365

For [FINRA Rule 4511\(c\)](#) requirements, Cohasset validated that Microsoft 365 includes archiving features that

enable regulated customers, including broker-dealers, to store data in a manner that helps them comply with SEC requirements for records retention. Retention features in Microsoft 365 help preserve a wide range of data, including email, voicemail, shared documents, instant messages, and third-party data. In particular, archiving in Microsoft 365 enables customers to set global or granular messaging retention policies to store data for a defined period and beyond in a non-rewriteable, non-erasable format.

## Microsoft in-scope cloud services

- [Azure](#)
- [Office 365](#)

## Audits, reports, and certificates

### **Azure & FINRA Rule 4511(c)**

[SEC 17a-4\(f\) & CFTC 1.31 \(c-d\) Compliance Assessment of Azure Storage](#)

### **Office 365 & FINRA Rule 4511(c)**

[Archiving in Office 365, data retention, and SEC Rule 17a-4 compliance](#)

## How to implement

- **Financial services regulation:** Compliance map of key US regulatory principles for cloud computing and Microsoft online services. [Learn more](#)
- **Risk Assessment & Compliance Guide:** Create a governance model for risk assessment of Microsoft cloud services, and regulator notification. [Learn more](#)
- **Financial use cases:** Use case overviews, tutorials, and other resources to build Azure solutions for financial services. [Learn more](#)

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Microsoft Office 365 Retention Policies](#)
- [Microsoft Financial Services Blog](#)
- [Compliance on the Microsoft Trust Center](#)

# Center for Financial Industry Information Systems (FISC)

11/30/2020 • 2 minutes to read • [Edit Online](#)

## FISC overview

The Center for Financial Industry Information Systems (FISC) is a not-for-profit organization established by the Japanese Ministry of Finance in 1984 to promote security in banking computer systems in Japan. Some 700 corporations in Japan are supporting members, including major financial institutions, insurance and credit companies, securities firms, computer manufacturers, and telecommunications enterprises.

In collaboration with its member institutions, the Bank of Japan, and the Financial Services Agency (a government organization responsible for overseeing banking, securities and exchange, and insurance in Japan), the FISC created guidelines for the security of banking information systems. These include basic auditing standards for computer system controls, contingency planning in the event of a disaster, and the development of security policies and standards encompassed in more than 300 controls.

Although the application of these guidelines in a cloud computing environment is not required by regulation, most financial institutions in Japan that implement cloud services have built information systems that satisfy these security standards, and it can be difficult to justify diverging from them. (The latest guidelines, Version 8 Supplemental Revised, issued in 2015, added two revisions relating to the use of cloud services by financial institutions and countermeasures against cyberattack.)

Conformance with this framework is not required by regulation, and not audited or otherwise validated by the FISC.

## Microsoft and FISC

Microsoft engaged outside assessors to validate that Microsoft Azure, Dynamics 365, and Microsoft Office 365 meet requirements of the FISC Security Guidelines on Computer Systems for Financial Institutions 9th Edition Revised. Microsoft provided evidence of compliance in each of the following areas:

- Datacenter guidelines for buildings and computer rooms, power, air conditioning, datacenter, and facilities monitoring.
- Operational guidelines for organizations, training, access control, system development, and auditing.
- Technical guidelines for measures to improve the reliability of hardware and software, and for countermeasures against security risks including data protection, prevention against unauthorized use, threat detection, and disaster recovery.

Financial institutions can rely on this evaluation of the compliance of these three areas for the in-scope infrastructure and platform services of Azure, Dynamics 365, Office 365, and Microsoft Cloud App Security.

[Learn more about validation of external assessors and links to assessor's sites \(Japanese Only\).](#)

## Microsoft in-scope cloud services

- [Azure](#)
- [Microsoft Cloud App Security](#)
- [Intune](#)
- [Office 365](#)

- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Frequently asked questions

### To whom do the FISC guidelines apply?

Banks and other financial institutions in Japan that want to validate their approach to system security, reliability, and auditing, and align with established best practices in Japan, follow the FISC guidelines.

### Where can I get more information on Version 8 of the FISC requirements?

The FISC has published two reports from its Council of Experts:

- [Usage of Cloud Computing by Financial Institutions](#)
- [Countermeasures Against Cyber Attacks on Financial Institutions](#)

### Where can I get the details of Microsoft's responses to the FISC framework?

You can also see security references ([in Japanese](#)) from third parties who have evaluated the FISC compliance of Microsoft cloud services.

### Can I use Microsoft's responses to this framework in my organization's qualification process?

Yes. However, although Microsoft responses to this framework are confirmed compliant by third parties, customers are responsible for validating the compliance of solutions they have implemented on Azure or Office 365.

## Resources

- [Microsoft Online Services Terms](#)
- [FISC Security Guidelines/Safety Standards](#)
- [FISC Report on Usage of Cloud Computing](#)
- [Compliance on the Microsoft Trust Center](#)

## Resources in Japanese

- [FISC](#)



# Financial Supervisory Authority (FSA) Denmark

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the FSA

The [Financial Supervisory Authority \(Finanstilsynet\)](#), under the Ministry of Industry, Business, and Financial Affairs, is the financial regulatory authority of the Danish government. Its principal role is to prepare regulatory guidelines for financial institutions in Denmark and monitor their compliance, as well as cooperate with regional and international authorities and regulators.

The FSA acts in concert with the European Banking Authority (EBA), “an independent EU authority, which works to ensure effective and consistent prudential regulation and supervision across the European banking sector.” To that end, the EBA has outlined a comprehensive approach to the use of cloud computing by financial institutions in the EU, [Recommendations on outsourcing to cloud services providers](#).

There are several guidelines that financial institutions in Denmark should be aware of when moving business functions to the cloud. In general, they prescribe contractual requirements for both financial institutions and cloud service providers to help ensure that financial organizations can adequately monitor and audit the outsourced functions. These include guidelines issued by the Ministry of Industry, Business, and Financial Affairs:

- The Danish Act on Financial Institutions ([Danish](#))
- The Executive Order 1304 on outsourcing of significant areas of activity ([Danish](#) and [English](#)) and the accompanying Guideline (Danish)
- Guidance on the use of cloud services as part of IT-outsourcing ([Danish](#)) issued by the FSA.

## Microsoft and the FSA

To help guide financial institutions in Denmark considering outsourcing business functions to the cloud, Microsoft has published [a compliance checklist for financial institutions in Denmark](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When Danish financial institutions outsource business activities they must comply with the requirements of the Financial Supervisory Authority (FSA), and work within the broad policy framework of the European Banking Authority (EBA). Specifically, those requirements focus on how contractual agreements between financial services and cloud providers can ensure adequate control of outsourced activities.

The Microsoft checklist helps Danish financial firms conducting due-diligence assessments of Microsoft business cloud services and includes:

- An overview of the regulatory landscape for context.
- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Compliance checklist: Denmark](#): Financial firms can get help in conducting risk assessments of Microsoft business cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Use case overviews, tutorials, and other resources to build Azure solutions for financial services.

## Frequently asked questions

### Is regulatory approval required?

No. The FSA does not approve outsourcing and the outsourcer (or cloud service provider) is, therefore, not required to obtain advance approval from the FSA. However, the FSA does specify that the outsourcer must notify it no later than eight business days after entering into an outsourcing agreement. The notification must be made in writing using a form specified by the FSA.

### Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. The Executive Order on Outsourcing of Significant Areas of Activity (and the accompanying Guideline) stipulates some specific points that financial institutions must incorporate in their cloud services contracts. Part 2 of the Microsoft [checklist](#) (page 48) maps these points against the sections in the Microsoft contractual documents where they are addressed.

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Compliance on the Microsoft Trust Center](#)

# Gramm-Leach-Bliley Act (GLBA)

2/5/2021 • 2 minutes to read • [Edit Online](#)

## GLBA overview

The Gramm-Leach-Bliley Act (GLBA) is a US law that reformed the financial services industry, allowing commercial and investment banks, securities firms, and insurance companies to consolidate, and addressed concerns about protecting consumer privacy. It required the Federal Trade Commission (FTC) and other financial services regulators to implement regulations to address such privacy provisions as the Financial Privacy Rule and the Safeguards Rule. GLBA requirements to safeguard sensitive consumer data apply to financial institutions that offer financial products and services to consumers, such as loans, investment advice, and insurance. The FTC is charged with enforcing compliance.

## Microsoft and GLBA

Microsoft Azure, Microsoft Office 365, Dynamics 365, and Microsoft Power BI can help meet the stringent requirements of providing cloud services for financial services institutions. As part of our support, we offer guidance to help you comply with the requirements of the GLBA by providing technical and organizational safeguards to help maintain security and prevent unauthorized usage.

Microsoft has developed risk assessment tools for both [Azure](#) and [Office 365](#) to help you more efficiently conduct a risk assessment of Azure and Office 365 services. The tool (an Excel spreadsheet) features 19 information security domains (such as security policy and risk management) that track the requirements of financial services regulations and other relevant standards, including GLBA (in Column R in the Azure spreadsheet and Column Q in the Office 365 spreadsheet). The tools explain how Azure and Office 365 comply with each requirement applicable to cloud service providers and can help you meet GLBA security requirements.

## Promote your GLBA compliance

- [Download the Azure Financial Services Cloud Risk Assessment Tool](#)
- [Download the Office 365 Cloud Risk Assessment Tool](#)

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- Intune
- [Office 365](#)
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Frequently asked questions

**How do I know if my financial institution must comply with the GLB Act?**

The FTC answers this in detail on its GLB Act page, [Who is covered by the privacy rule?](#)

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium

template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Gramm-Leach-Bliley Act](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Office 365 Cloud Risk Assessment Tool](#)
- [Compliance on the Microsoft Trust Center](#)

## Other Microsoft resources for financial services

- [Microsoft Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)
- [Shared responsibilities for cloud computing](#)

# Financial Supervision Authority (KNF) Poland

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the KNF

The [Polish Financial Supervision Authority](#) ([Komisja Nadzoru Finansowego](#), KNF) is the financial regulatory authority in Poland, responsible for supervision of the financial market, which includes oversight over banking, capital markets, insurance, pension schemes, and electronic money institutions.

The KNF acts in concert with the [European Banking Authority](#) (EBA), “an independent EU authority, which works to ensure effective and consistent prudential regulation and supervision across the European banking sector.” To that end, the EBA has outlined a comprehensive approach to the use of cloud computing by financial institutions in the EU, [Recommendations on outsourcing to cloud services providers](#).

There are several requirements and guidelines that financial institutions in Poland should be aware of when moving business functions and data to the cloud:

- The Banking Act of 1997 ([Polish](#) and [English](#)) does not regulate cloud services directly but instead sets out legal requirements for outsourcing banking operations including how personal information can be processed. Cloud services could be subject to Banking Act provisions if the outsourced services are of key significance for the bank, or if outsourcing involves giving the service provider access to sensitive data that is subject to banking secrecy requirements.
- The Announcement, issued by the KNF Office in 2017, provides a detailed checklist and action plan for regulated institutions that intend to move business functions to the cloud.
- [Recommendation D](#): Management of Information Technology and ICT Environment Security at Banks defines KNF expectations for prudent IT security management by banks, particularly as to how they manage risk. The KNF makes 22 recommendations for best security practices and has issued comparable guidelines for [insurance companies](#), [investment firms](#), and [general pension companies](#).

In addition, the use of cloud services by financial institutions must comply with Poland’s Personal Data Protection Act of 1997, which is fundamental to the processing of personal data. To align with the GDPR, it was amended in late 2018 by the Act on Facilitation of Performance of Business Activity ([Polish](#)) and will take effect 1 January 2019.

## Microsoft and the KNF

To help guide financial institutions in Poland considering outsourcing business functions to the cloud, Microsoft has published [Navigating your way to the cloud: A compliance checklist for financial institutions in Poland](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When financial institutions in Poland outsource business activities to the cloud, they must address requirements of the Banking Act of 1997 and the 2017 KNF Announcement regarding the use of data processing services in the cloud, both of which fall within the broad policy framework of the European Banking Authority. In addition, financial firms using cloud services must comply with the GDPR-aligned 2018 amendment to the Personal Data Protection Act of 1997, now updated to align with the GDPR.

The Microsoft checklist helps Polish financial firms conducting due-diligence assessments of Microsoft business cloud services and includes:

- An overview of the regulatory landscape for context.

- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Compliance checklist: Poland](#): Financial firms can get help in conducting risk assessments of Microsoft business cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Use case overviews, tutorials, and other resources to build Azure solutions for financial services.
- [Privacy in Microsoft Cloud](#): Get details on Microsoft privacy principles and standards and on privacy laws specific to Poland.

## Frequently asked questions

### Is regulatory approval required?

No. However, under the Banking Act of 1997, if the service provider is based outside the European Economic Area (EEA) or if outsourced operations are to be implemented outside the EEA, banks must obtain KNF approval before entering into contracts.

### Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. Part 2 of the [Microsoft checklist](#) (page 77) contains a comprehensive list of the requirements that should be included in contracts with cloud service providers.

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Compliance on the Microsoft Trust Center](#)

# Monetary Authority of Singapore (MAS) and Association of Banks in Singapore (ABS)

11/30/2020 • 5 minutes to read • [Edit Online](#)

## MAS and ABS Overview

### Monetary Authority of Singapore (MAS)

In July 2016, the MAS, the sole bank regulator in Singapore and its central bank, issued its [Guidelines on Outsourcing Risk Management](#). In the guidelines, the MAS set out its expectations for outsourcing cloud services by financial institutions in Singapore, including banks, insurance companies, and trust companies. This was the result of an industry-wide consultation that began in October 2014 that included Microsoft participation.

The MAS Guidelines substantially streamline the process for technology adoption, provide clarity on the regulator's expectations, and address many of the misconceptions that had previously slowed the financial industry's adoption of cloud solutions.

Furthermore, the guidelines are unequivocal in their support of the use of cloud services — including a public cloud — by financial institutions and that they stand to benefit from doing so. They have eliminated the expectation that financial institutions would notify the MAS before any significant material outsourcing commitments. Instead, MAS-regulated institutions are expected to refine their risk-based approach when assessing material outsourcing and conduct a self-assessment of all outsourcing arrangements against these guidelines. (For now, these guidelines are not legally binding, but the MAS has indicated that it will issue a statutory notice in the future.)

### Association of Banks in Singapore (ABS)

Shortly after the release of the MAS Guidelines on Outsourcing Risk Management, the ABS, a non-profit organization representing the interests of local and foreign banks operating in Singapore (but not other financial institutions), introduced a non-binding practical guide, [Cloud Computing Implementation Guide](#). It is designed to help banks implement outsourcing arrangements following MAS Guidelines.

## Microsoft MAS and ABS

With the endorsement of cloud computing — including the use of public clouds — by the Monetary Authority of Singapore (MAS) and support from the Association of Banks in Singapore (ABS), Microsoft published the [Microsoft response to MAS outsourcing guidelines and ABS guidance](#) and a [Compliance Checklist for financial institutions in Singapore](#). Together they demonstrate how financial firms can move data and workloads to the Microsoft Cloud with the confidence that they are complying with MAS guidelines and complete a self-assessment of their outsourcing arrangements against the new guidelines.

The [Microsoft response to MAS guidelines and ABS guidance](#) gives financial firms an overview of the key issues raised by the MAS Guidelines and the ABS Guide as they apply to cloud services, Microsoft interpretations of and responses to each of the key issues, and details on how Microsoft can help facilitate compliance with MAS guidelines. It addresses MAS and ABS guidance separately.

The [Microsoft response to the MAS Guidelines](#) focuses on MAS recommendations for prudent risk management practices for outsourcing. It describes point by point how Microsoft has the right policies, processes, and tools to help you evaluate the risks, provides checklists to help you assess our business cloud services, and describes the processes for governance and internal controls.

The Microsoft response to the ABS Guide centers on Sections 3 and 4.

- Section 3 builds on the due diligence and vendor management requirements of the MAS Guidelines by addressing in more detail such matters as contractual considerations. We give detailed information about Microsoft vendor management tools and the assistance we can offer during the due-diligence assessment.
- Section 4 recommends a set of key baseline controls — from encryption to penetration and vulnerability management — that cloud service providers should have in place when working with banks. We describe how our controls address the security concerns of each of the specified controls.

Get practical support for moving data and workloads to the Microsoft Cloud in compliance with MAS Guidelines

[Download the Navigating your way to the cloud: Microsoft's response to MAS outsourcing guidelines and ABS guidance](#)

Compliance Checklist for Financial Institutions in Singapore

This document includes an overview of the regulatory landscape, which introduces the relevant requirements in Singapore, and a compliance checklist, which lists the regulatory issues that need to be addressed and maps Microsoft's cloud services against those issues. By reviewing and completing the checklist point by point, financial institutions can adopt Microsoft cloud services with confidence that they are complying with the relevant requirements in Singapore.

By relying on our comprehensive approach to risk assurance in the cloud, we are confident that financial institutions in Singapore can move to the Microsoft Cloud in a manner that is consistent with MAS Guidelines and the ABS Guide, while also providing a more advanced security risk management profile than many on-premises solutions.

Get practical support for moving data and workloads to the Microsoft Cloud in compliance with MAS Guidelines

[Download the Compliance Checklist for Financial Institutions in Singapore](#)

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- Intune
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- [Office 365](#)

## Frequently asked questions

### Is regulatory approval required?

No, there is no requirement for prior notification, consultation, or approval of outsourcing arrangements. However, the MAS expects financial institutions to be ready to demonstrate how they comply, and to notify the MAS as soon as possible of adverse developments arising from a financial institution's outsourcing arrangements — for example, a data breach incident.

### What is a "material" outsourcing arrangement and why is the definition important?

An outsourcing arrangement is "material" if a service failure or breach has the potential to materially affect a financial firm's business operations or ability to manage risk and comply with applicable laws and regulations; or if it involves customer information and, in the event of any unauthorized access or disclosure, loss, or theft of customer information, has a material impact on a firm's customers. The definition of "customer information" expressly excludes securely encrypted information.

This definition is important since certain provisions of MAS Outsourcing Guidelines apply only to "material



outsourcing arrangements.” These include an obligation to perform annual reviews, mandatory contractual clauses addressing audit rights, and ensuring that outsourcing outside of Singapore does not affect MAS supervisory efforts.

## Resources

- [MAS Guidelines on Outsourcing Risk Management](#)
- [Frequently Asked Questions on MAS Guidelines on Outsourcing](#)
- [ABS Cloud Computing Implementation Guide 1.1](#)
- [Navigating your way to the cloud: the Microsoft response to MAS Outsourcing Guidelines and the ABS Cloud Implementation Guide\\*\\*](#)
- [Microsoft compliance checklist](#)

## Other Microsoft resources for financial services

- [Microsoft Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)
- [Shared responsibilities for cloud computing](#)
- [Compliance on the Microsoft Trust Center](#)

# National Bank of Belgium (NBB) and the Financial Services and Markets Authority (FSMA)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the NBB and FSMA

The primary financial services regulators in Belgium are the [National Bank of Belgium](#) (NBB) and the [Financial Services and Markets Authority](#) (FSMA).

The NBB is responsible for prudential supervision of credit institutions, insurers, stockbrokers, and other financial organizations. As the central bank of Belgium, the NBB conducts monetary policy for Belgium and contributes to the stability of its financial system. Alongside the NBB, the FSMA supervises Belgian financial markets, financial service providers including investment firms, and supplemental pensions. Its tasks include oversight of the financial information that companies disseminate and the products they offer to consumers and their compliance with the rules of business conduct.

The NBB and FSMA act in concert with the European Banking Authority (EBA), 'an independent EU authority that works to ensure effective and consistent prudential regulation and supervision across the European banking sector.' To that end, the EBA has outlined a comprehensive approach to the use of cloud computing by financial institutions in the EU, [Recommendations on outsourcing to cloud services providers](#).

There are several requirements and guidelines that financial institutions in Belgium should be aware of when moving business functions to the cloud, including:

- NBB Circular PPB 2004/5, Sound management practices in outsourcing by credit institutions and investment firms ([Dutch](#) and [French](#)), and the broadly equivalent provisions of the [FSMA Circular 05-06.2007](#) (French and Dutch) on organizational requirements for firms providing investment services.
- Circular NBB 2009-17, Financial services via the Internet: Prudential requirements ([English](#)), examines outsourcing risks and sets out the requirements for internal control and management of those risks. It also discusses compliance with the financial rules of conduct and the potential impact of cross-border transactions in the cloud.
- Circular NBB 2015-32, Additional prudential expectations regarding operational business continuity, and security of systemically important financial institutions ([Dutch](#) and [English](#)), sets out management and security processes for institutions that play a critical role in the financial system, and whose disruption could jeopardize its proper functioning.

## Microsoft and the NBB and FSMA

To help guide financial institutions in Belgium considering outsourcing business functions to the cloud, Microsoft has published [A compliance checklist for financial institutions in Belgium](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When financial organizations in Belgium outsource business functions to the cloud, they must comply with the rules and guidelines of the National Bank of Belgium (NBB) and the Financial Services and Markets Authority (FSMA) within the broad policy framework of the European Banking Authority (EBA).

The Microsoft checklist helps financial firms in Belgium that are conducting due-diligence assessments of Microsoft business cloud services. It includes:

- An overview of the regulatory landscape for context.

- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Office 365](#)

## How to implement

- [Compliance checklist: Belgium](#): Financial institutions can get help in conducting risk assessments of Microsoft cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Use case overviews, tutorials, and other resources to build Azure solutions for financial services.

## Frequently asked questions

### Is regulatory approval required?

No. However, financial institutions must notify the NBB and FSMA in the event of a disruption in an outsourcing arrangement that has the potential to materially impact the institution's business operations, reputation, or profitability, or its ability to manage risk and comply with applicable laws and regulations.

### Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. There are specific points that financial institutions must be sure to incorporate in their cloud services contracts. Part 2 of the [Microsoft checklist](#) (page 49) maps these against the sections in the Microsoft contractual documents where they are addressed.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Compliance on the Microsoft Trust Center](#)

# Office of the Superintendent of Financial Institutions (OSFI) Canada

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the OSFI

The [Office of the Superintendent of Financial Institutions](#) (OSFI) is an independent agency of the Government of Canada responsible for the prudential regulation and supervision of federally regulated financial institutions and pension plans in Canada.

In its oversight role, OSFI published the B-10 Guidelines for [Outsourcing of Business Activities, Functions, and Processes](#). They established 'prudent practices, procedures, or standards' for federally regulated financial institutions to evaluate and manage the risk associated with outsourcing their business to a service provider. A subsequent OSFI memorandum, [New technology-based outsourcing requirements](#), reminded these institutions that the B-10 Guidelines remain current and that they must meet OSFI expectations for material outsourcing arrangements.

In addition, the use of cloud services by financial institutions must comply with the [Personal Information Protection and Electronic Documents Act](#) (PIPEDA), and in some instances, provincial data privacy laws.

## Microsoft and OSFI

To help guide financial institutions in Canada considering outsourcing business functions to the cloud, Microsoft has published [Navigating your way to the cloud: A compliance checklist for financial institutions in Canada](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When Canadian financial institutions outsource business activities, they must comply with the B-10 Guidelines for [Outsourcing of Business Activities, Functions, and Processes](#) published by the Office of the Superintendent of Financial Institutions (OSFI), as well as Canadian privacy laws, including the [Personal Information Protection and Electronic Documents Act](#) (PIPEDA).

The Microsoft checklist helps Canadian financial firms conducting due-diligence assessments of Microsoft business cloud services and includes:

- An overview of the regulatory landscape for context.
- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Compliance checklist: Canada](#): Financial firms can get help in conducting risk assessments of Microsoft

business cloud services.

- [Privacy in Microsoft Cloud](#): Get details on Microsoft privacy principles and standards and on privacy laws specific to Canada.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Industry use cases for Azure](#): Use case overviews, tutorials, and other resources to build Azure solutions for financial services.

## Frequently asked questions

### Is regulatory approval required?

No. There is no requirement for prior notification, consultation, or approval. The use of public cloud computing is permitted, subject always to compliance with OSFI requirements.

The [OSFI B-10 Guidelines](#) indicate that OSFI expects a financial institution to design a risk management program that applies to all of its outsourcing arrangements, with risk mitigation commensurate with the associated risks. However, only material outsourcing arrangements need to be documented by a written contract that addresses safeguards identified in the guidelines. Part 2 of the Microsoft [checklist](#) (page 53) maps these against the sections in Microsoft contractual documents where they are addressed.

### Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes, but only if the outsourcing arrangement is a material outsourcing or if it involves any transfer of personal information to the cloud service provider.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Compliance on the Microsoft Trust Center](#)

# Payment Card Industry (PCI) Data Security Standard (DSS)

2/5/2021 • 5 minutes to read • [Edit Online](#)

## PCI DSS overview

The Payment Card Industry (PCI) Data Security Standards (DSS) is a global information security standard designed to prevent fraud through increased control of credit card data. Organizations of all sizes must follow PCI DSS standards if they accept payment cards from the five major credit card brands, Visa, MasterCard, American Express, Discover, and the Japan Credit Bureau (JCB). Compliance with PCI DSS is required for any organization that stores, processes, or transmits payment and cardholder data.

## Microsoft and PCI DSS

Microsoft completed an annual PCI DSS assessment using an approved Qualified Security Assessor (QSA). The auditors reviewed Microsoft Azure, Microsoft OneDrive for Business, and Microsoft SharePoint Online environments, which include validating the infrastructure, development, operations, management, support, and in-scope services. The PCI DSS designates four levels of compliance based on transaction volume. Azure, OneDrive for Business, and SharePoint Online are certified as compliant under PCI DSS version 3.2 at Service Provider Level 1 (the highest volume of transactions, more than 6 million a year).

The assessment results in an Attestation of Compliance (AoC), which is available to customers and Report on Compliance (RoC) issued by the QSA. The effective period for compliance begins upon passing the audit and receiving the AoC from the assessor and ends one year from the date the AoC is signed.

Customers who want to develop a cardholder environment or card processing service can use these validations in many of the underlying portions, thereby reducing the associated effort and costs of getting their own PCI DSS certification.

It is important to understand that PCI DSS compliance status for Azure, OneDrive for Business, and SharePoint Online not automatically translate to PCI DSS certification for the services that customers build or host on these platforms. Customers are responsible for ensuring that they achieve compliance with PCI DSS requirements.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Microsoft Cloud App Security
- Flow cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Microsoft Graph
- Intune
- [Microsoft Defender Advanced Threat Protection](#)
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- OneDrive for Business and SharePoint Online (United States only)

## Audit, reports, and certificates

- [Azure PCI DSS Attestation of Compliance \(AoC\)](#)
- [OneDrive for Business and SharePoint Online PCI DSS Attestation of Compliance \(AoC\)](#)

## Get your PCI DSS solution running on Azure

Build and deploy your PCI DSS solution in the cloud even faster with the Azure Security and Compliance PCI DSS Blueprint. Get reference architectures, deployment guidance, control implementation mappings, automated scripts and more. [Start using the Azure PCI DSS Blueprint.](#)

## Frequently asked questions

### **Why does the Attestation of Compliance (AoC) cover page say 'June 2018'?**

The June 2018 date on the cover page is when the AoC template was published. Refer to Section 2 for the date of the assessment.

### **Why are there multiple Azure Attestations of Compliance (AoCs)?**

The Azure AoC package has AoCs corresponding to Azure Public, Germany, and Government cloud. Customers should use the AoC that corresponds with their Azure environment.

### **What is the relationship between the PA DSS and PCI DSS?**

The Payment Application Data Security Standard (PA DSS) is a set of requirements that comply with the PCI DSS, and replaces Visa's Payment Application Best Practices, and consolidates the compliance requirements of the other primary card issuers. The PA DSS helps software vendors develop third-party applications that store, process, or transmit cardholder payment data as part of a card authorization or settlement process. Retailers must use PA DSS certified applications to efficiently achieve their PCI DSS compliance. The PA DSS does not apply to Azure.

### **What is an acquirer and does Azure use one?**

An acquirer is a bank or other entity that processes payment card transactions. Azure does not offer payment card processing as a service and thus does not use an acquirer.

### **To what organizations and merchants does the PCI DSS apply?**

PCI DSS applies to any company, no matter the size, or number of transactions, that accepts, transmits, or stores cardholder data. That is, if any customer ever pays a company using a credit or debit card, then the PCI DSS requirements apply. Companies are validated at one of four levels based on the total transaction volume over a 12-month period. Level 1 is for companies that process over 6 million transactions a year; Level 2 for 1 million to 6 million transactions; Level 3 is for 20,000 to 1 million transactions; and Level 4 is for fewer than 20,000 transactions.

### **Where do I begin my organization's PCI DSS compliance efforts for a solution deployed on Azure?**

The information that the PCI Security Standards Council makes available is a good place to learn about specific compliance requirements. The council publishes the [PCI DSS Quick Reference Guide](#) for merchants and others involved in payment card processing. The guide explains how the PCI DSS can help protect a payment card transaction environment and how to apply it.

Compliance involves several factors, including assessing the systems and processes not hosted on Azure. Individual requirements vary based on which Azure services are used and how they are employed within the solution.

### **Are there plans for OneDrive for Business and SharePoint Online to be PCI DSS-compliant outside of the United States?**

Currently OneDrive for Business and SharePoint Online is PCI-DSS compliant only in the United States (US). Microsoft will evaluate the requirements and timelines for regions outside of US and provide updates when and if other regions are added to the roadmap.

### What is in-scope for OneDrive for Business and SharePoint Online?

Currently, only files and documents uploaded to OneDrive for Business and SharePoint Online will be compliant with PCI DSS.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [PCI Security Standards Council](#)
- [PCI Data Security Standard](#)
- [Azure PCI DSS 3.2.1 Blueprint](#)
- [PCI DSS Quick Reference Guide](#)
- [Compliance on the Microsoft Trust Center](#)



# Reserve Bank of India (RBI) and Insurance Regulatory and Development Authority of India (IRDAI)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About RBI and IRDAI

The [Reserve Bank of India](#) (RBI), India's central banking institution, the [Insurance Regulatory and Development Authority of India](#) (IRDAI), and the [Ministry of Electronics and Information Technology](#) (MeitY) comprise three of the key financial industry regulators overseeing banks, insurance organizations, and market infrastructure institutions. Their directives include outsourcing and risk management guidelines and requirements for compliance with privacy rules governing sensitive data.

Outsourcing and risk management guidance includes:

- [Guidelines on Managing Risk and Code of Conduct in Outsourcing of Financial Services by Banks](#) (RBI) address the risks that regulated banks would be exposed to while outsourcing financial services and help ensure that outsourcing does not impede the supervisory role of the RBI. The RBI does not require prior approval for banks seeking to outsource financial services; however, core banking functions, such as internal audit and compliance functions, should not be outsourced.
- [Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds](#) (RBI). Financial institutions must report outsourcing arrangements where the scale and nature of the activities are significant or require extensive data sharing with service providers outside of India. This guidance applies particularly if operational data is stored or processed outside India.
- [Outsourcing of Activities by Indian Insurers Regulation](#) (IRDAI). Every year, insurance organizations are required to report outsourcing to IRDAI of certain support functions of core activities within 45 days of the close of the financial year. (Page 7 in the Microsoft [checklist](#) describes what constitutes 'support functions of core activities.'

Financial firms using cloud services must also comply with privacy rules, including the [Information Technology \(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information\) Rules, 2011](#) (MeitY). Developed to strengthen India's data protection laws, these rules govern the protection and handling of sensitive personal data.

## Microsoft, RBI, and IRDAI

To help guide financial institutions in India considering outsourcing business functions to the cloud, Microsoft has published a compliance checklist for financial institutions in India. By reviewing and completing the [checklist](#), financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When Indian financial institutions outsource business activities to the cloud, they must follow the guidelines of the Reserve Bank of India for managing risk and addressing the issues that arise from the use of information technology. They must also comply with the data security and privacy requirements established by the Ministry of Electronics and Information Technology (MeitY). In addition, insurance organizations must follow outsourcing guidelines published by the Insurance Regulatory and Development Authority of India (IRDAI).

The Microsoft checklist helps financial firms in India that are conducting due-diligence assessments of Microsoft business cloud services and includes:

- An overview of the regulatory landscape for context.
- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft Office 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Compliance checklist for India](#): Financial firms can get help conducting risk assessments of Microsoft business cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases for Azure](#): Use case overviews, tutorials, and other resources to build Azure solutions for financial services.

## Frequently asked questions

### Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. The guidelines referenced above stipulate some specific points that financial institutions must incorporate into their cloud services contracts. Part 2 of the [checklist](#) (page 70) maps these against the sections in the Microsoft contractual documents where they are addressed.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Microsoft and MeitY](#)
- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Compliance on the Microsoft Trust Center](#)

# Securities and Exchange Commission (SEC) Rule 17a-4(f) United States

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About SEC Rule 17a-4(f)

The [US Securities and Exchange Commission \(SEC\)](#) is an independent agency of the US federal government and the primary overseer and regulator of US securities markets. It wields enforcement authority over federal securities laws, proposes new securities rules, and oversees market regulation of the securities industry.

The SEC defines rigorous and explicit requirements for regulated entities that elect to retain books and records on electronic storage media. It established [17 CFR 240.17a-3](#) and [17 CFR 240.17a-4](#) to regulate recordkeeping, including retention periods, for securities broker-dealers. Later, the SEC [amended](#) 17 CFR 240.17a-4 paragraph (f), issuing two interpretive releases expressly to allow books and records to be retained on electronic storage media as long as certain conditions were met.

An electronic storage system meets those conditions if it prevents the alteration or erasure of records for the required retention period. Retention periods vary from three to six years based on record types, with immediate accessibility mandated for the first two years. Moreover, one of the interpretive releases requires that the storage system be capable of retaining records beyond the SEC-established retention period to comply with subpoenas, legal hold, or other such requirements.

## Microsoft and SEC Rule 17a-4(f)

Financial services customers, representing one of the most heavily regulated industries in the world, are subject to complex provisions like the retention of financial transactions and related communication in a non-erasable and non-modifiable state. Among the most prescriptive is Rule 17a-4(f) of the US Security and Exchange Commission (SEC) that stipulates stringent requirements for regulated entities that elect to retain books and records on electronic storage media. Records stored must be tamper-proof with no ability to alter or delete them until after the designated retention period.

Microsoft Azure Immutable Blob Storage with Policy Lock and Microsoft Office 365 with Preservation Lock can help financial institutions meet the immutable storage requirements of SEC Rule 17a-4(f).

To evaluate Azure and Office 365 compliance with SEC Rule 17a-4(f), Microsoft retained an independent assessment firm that specializes in records management and information governance, Cohasset Associates. In the resulting report for:

- **Azure:** [SEC 17a-4\(f\) Compliance Assessment: Microsoft Azure Storage](#), Cohasset validated that [Azure Immutable Blob Storage](#) with the Policy Lock option, when used to retain time-based Blobs in a non-erasable and non-rewritable (WORM) format, meets the immutable storage requirements of the SEC rule. Each Blob (record) is protected from being modified, overwritten, or deleted until the required retention period has expired and any associated legal holds have been released. Software providers and partners with sensitive workloads can now rely on Azure Immutable Blob Storage as a onestop-shop cloud solution for records retention and immutable storage. Financial institutions can now build their own applications taking advantage of these features while remaining compliant.
- **Microsoft 365:** For [SEC 17a-4\(f\)](#) requirements, Cohasset validated that Microsoft 365 includes archiving features that enable regulated customers, including broker-dealers, to store data in a manner that helps them comply with SEC requirements for records retention. Retention features in Microsoft 365 help preserve a wide range of data, including email, voicemail, shared documents, instant messages, and third-party data. In

particular, archiving in Microsoft 365 enables customers to set global or granular messaging retention policies to store data for a defined period and beyond in a non-rewriteable, non-erasable format.

## Microsoft in-scope cloud services

- [Azure](#)
- [Office 365](#)

## Audits, reports, and certificates

### **Azure & SEC Rule 17**

[SEC 17a-4\(f\) & CFTC 1.31 \(c-d\) Compliance Assessment of Azure Storage](#)

### **Office 365 & SEC Rule 17**

[SEC 17a-4\(f\) Compliance Assessment: Microsoft Security & Compliance Center with SharePoint, OneDrive, Teams, Exchange, and Skype for Business](#)

## How to implement

### **Financial services regulation**

Compliance map of key US regulatory principles for cloud computing and Microsoft online services. [Learn more](#)

### **Risk Assessment & Compliance Guide**

Create a governance model for risk assessment of Microsoft cloud services, and regulator notification. [Learn more](#)

### **Financial use cases**

Use case overviews, tutorials, and other resources to build Azure solutions for financial services. [Learn more](#)

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Archiving in Microsoft Office 365, Data Retention, and Rule 17a-4](#)
- [Compliance Microsoft Financial Services](#)
- [Compliance Program Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Microsoft Office 365 Retention Policies](#)
- [Microsoft Financial Services Community](#)
- [Compliance on the Microsoft Trust Center](#)

# Securities and Exchange Commission: Regulation Systems Compliance and Integrity (SCI)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About Regulation SCI

The US Securities and Exchange Commission (SEC) is an independent agency of the US federal government and the primary overseer and regulator of US securities markets. It wields enforcement authority over federal securities laws, proposes new securities rules, and oversees market regulation of the securities industry.

In November 2014, the SEC adopted [Regulation Systems Compliance and Integrity \(SCI\)](#) (and Form SCI for reporting SCI events) to bolster the technology infrastructure in the US securities markets. The regulation is designed to reduce the frequency of system outages, improve resiliency when such incidents do occur, and increase SEC oversight of securities market technology and enforcement of its regulations.

The SCI rules apply to SCI entities, which include such self-regulatory organizations (SROs) as stock and options exchanges, registered clearing agencies, and alternative trading systems (ATs). The rules primarily regulate the systems that directly support key securities market functions: trading, clearance and settlement, order routing, market data, market regulation, and market surveillance.

## Microsoft and SEC Regulation SCI

The US Securities and Exchange Commission (SEC) adopted Regulation SCI to strengthen the technology infrastructure of the financial organizations that operate and support the US securities markets. Under SEC oversight, its requirements are designed to ensure that these systems have high availability, strong resiliency, and low latency (high volume of messages with little delay).

To help guide US financial services customers who must comply with this regulation, Microsoft has published the [Microsoft Azure SEC Regulation Systems Compliance and Integrity Cloud Implementation Guide](#). The guidance within this document:

- Provides an overview of overall Azure capabilities that support strong resiliency, high availability, and low latency.
- Makes clear which control areas and regulatory aspects Azure addresses. This point-by-point mapping of Azure features and services to SCI requirements measures Azure compliance against the regulatory framework. It also helps customers understand where they can shift security responsibilities to Azure that they had fully owned when they operated on premises. These capabilities are backed by the promises Microsoft makes in Azure SLAs.
- Specifies each Regulation SCI requirement that is the customer's responsibility to address, and offers Azure documentation and services to help them address these responsibilities.

This document provides a thorough checklist of critical Regulation SCI focus areas. This checklist helps financial organizations understand how they can adopt Azure to help assure their regulators, customers, and leadership that they can comply with the applicable regulatory requirements.

## Microsoft in-scope cloud services

- [Azure](#)

## How to implement

- [Regulation SCI Implementation Guide](#): Maps Azure capabilities against the regulation and details the shared responsibility for compliance.
- [Designing reliable Azure applications](#): A brief overview of how to build reliability into each step of Azure application design.
- [Designing highly available applications](#): How developers can help ensure that their Azure Storage applications are highly available.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.

## Frequently asked questions

### What does shared responsibility mean when using cloud technology?

As computing environments move from datacenters on-premises to those in the cloud, the responsibility of security also shifts—the cloud services provider (CSP) and customer now share that responsibility. For every application and solution, how much of that responsibility falls on the customer and how much on the CSP depends on the Azure model that a customer deploys—IaaS, SaaS, or PaaS. It is the customer's duty to understand to what degree they are accountable for implementing the required security controls. However, Microsoft provides guidance to help customers navigate this complex dynamic. For more information, read [Shared Responsibilities for Cloud Computing](#).

### Which financial institutions can take advantage of Azure to help meet Regulation SCI requirements?

Financial organizations, or SCI entities, that are subject to this regulation can deploy Azure. The SEC says its regulation applies to 'self-regulatory organizations (SROs), including stock and options exchanges, registered clearing agencies, FINRA, and the MSRB, alternative trading systems (ATSs), that trade NMS and non-NMS stocks exceeding specified volume thresholds, disseminators of consolidated market data (plan processors), and certain exempt clearing agencies.'

## Resources

- [SEC Responses to Frequently Asked Questions Concerning Regulation SCI](#)
- [Business continuity and disaster recovery \(BCDR\): Azure Paired Regions](#)
- [Compliance Map of Cloud Computing Regulatory Principles and Microsoft Online Services](#)
- [Microsoft Cloud Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft Financial Services](#)
- [Microsoft and SEC Rule 17a-4](#)
- [Compliance on the Microsoft Trust Center](#)

# Service Organization Controls (SOC)

2/17/2021 • 5 minutes to read • [Edit Online](#)

## SOC 1, 2, and 3 Reports overview

Increasingly, businesses outsource basic functions such as data storage and access to applications to cloud service providers (CSPs) and other service organizations. In response, the American Institute of Certified Public Accountants (AICPA) has developed the Service Organization Controls (SOC) framework, a standard for controls that safeguard the confidentiality and privacy of information stored and processed in the cloud. This aligns with the International Standard on Assurance Engagements (ISAE), the reporting standard for international service organizations.

Service audits based on the SOC framework fall into two categories — SOC 1 and SOC 2 — that apply to in-scope Microsoft cloud services.

A SOC 1 audit, intended for CPA firms that audit financial statements, evaluates the effectiveness of a CSP's internal controls that affect the financial reports of a customer using the provider's cloud services. The Statement on Standards for Attestation Engagements (SSAE 18) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) are the standards under which the audit is performed, and is the basis of the SOC 1 report.

A SOC 2 audit gauges the effectiveness of a CSP's system based on the AICPA Trust Service Principles and Criteria. An Attest Engagement under Attestation Standards (AT) Section 101 is the basis of SOC 2 and SOC 3 reports.

At the conclusion of a SOC 1 or SOC 2 audit, the service auditor renders an opinion in a SOC 1 Type 2 or SOC 2 Type 2 report, which describes the CSP's system and assesses the fairness of the CSP's description of its controls. It also evaluates whether the CSP's controls are designed appropriately, were in operation on a specified date, and were operating effectively over a specified time period.

Auditors can also create a SOC 3 report — an abbreviated version of the SOC 2 Type 2 audit report — for users who want assurance about the CSP's controls but don't need a full SOC 2 report. A SOC 3 report can be conferred only if the CSP has an unqualified audit opinion for SOC 2.

## Microsoft and SOC 1, 2, and 3 Reports

Microsoft covered cloud services are audited at least annually against the SOC reporting framework by independent third-party auditors. The audit for Microsoft cloud services covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.

Microsoft has achieved SOC 1 Type 2, SOC 2 Type 2, and SOC 3 reports. In general, the availability of SOC 1 and SOC 2 reports is restricted to customers who have signed nondisclosure agreements with Microsoft; the SOC 3 report is publicly available.

## Microsoft in-scope cloud services

### Covered services for SOC 1 and SOC 2

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- [Dynamics 365 and Dynamics 365 U.S. Government](#)
- Microsoft Graph

- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- Microsoft Stream
- Azure DevOps Services

### **Covered services for SOC 3**

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- Microsoft Graph
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)
- Power BI
- Microsoft Stream

## Audits, reports, and certificates

### **Audit cycle**

Microsoft cloud services are audited at least annually against SOC 1 (SSAE18, ISAE 3402), SOC 2 (AT Section 101), and SOC 3 standards.

### **Azure, Dynamics 365, Microsoft Cloud App Security, Flow, Microsoft Graph, Intune, Power BI, PowerApps, Microsoft Stream, and Microsoft Datacenters**

- [Azure + Dynamics 365 and Azure + Dynamics 365 Government SOC 1 Type 2 Report](#)
- [Azure + Dynamics 365 and Azure + Dynamics 365 Government SOC 2 Type 2 Report](#)
- [Azure + Dynamics 365 and Azure + Dynamics 365 Government SOC 3 Report](#)

### **Office 365**

- [Office 365 Core - SSAE 18 SOC 1 Report](#)
- [Office 365 Core - SSAE 18 SOC 2 Report](#)
- [Office 365 Core - SSAE 18 SOC 3 Report](#)
- [Office 365 Microservices T1-SSAE 18 SOC2 Type I Report](#)
- [Customer Lockbox SOC 1 SSAE 16 Audit Report](#)
- [Yammer SOC 2 AT 101 Type I Audit Report](#)
- [Yammer SOC 2 Type II Report](#)
- [See bridge letters and additional audit reports](#)

## Frequently asked questions

How can I get copies of the SOC reports?



With the reports, your auditors can compare Microsoft business cloud services results with your own legal and regulatory requirements.

- You can see all SOC reports through the [Service Trust Platform](#).
- Azure DevOps Service customers that can't access [Service Trust Platform](#) can email [Azure DevOps](#) for its SOC 1 and SOC 2 reports. This email is to request Azure DevOps SOC reports only.

#### How often are Azure SOC reports issued?

SOC reports for Azure, Microsoft Cloud App Security, Flow, Microsoft Graph, Intune, Power BI, PowerApps, Microsoft Stream, and Microsoft Datacenters are based on a rolling 12-month run window (audit period) with new reports issued semi-annually (period ends are March 31 and September 30). Bridge letters are issued each quarter to cover the prior three month period. For example, the January letter covers 10/1-12/31, the April letter covers 1/1-3/31, the July letter covers 4/1-6/30, and the October letter covers 7/1-9/30. Customers can [download](#) the latest reports from the Service Trust Portal.

#### Do I need to conduct my own audit of Microsoft datacenters?

No. Microsoft shares the independent audit reports and certifications with customers so that they can verify Microsoft compliance with its security commitments.

#### Can I use Microsoft's compliance in my organization's certification process?

Yes. When you migrate your applications and data to covered Microsoft cloud services, you can build on the audits and certifications that Microsoft holds. The independent reports attest to the effectiveness of controls that Microsoft has implemented to help maintain the security and privacy of your data.

#### Where do I start with my organization's own compliance effort?

The [SOC Toolkit for Service Organizations](#) is a helpful resource for understanding SOC reporting processes and promoting your organization's use of them.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Better protect your data by using Microsoft cloud services](#)
- [Service Organization Control \(SOC\) Reports](#)
- [SSAE 16 Overview](#)
- [ISAE 3402 Overview](#)
- [Microsoft Online Services Terms](#)
- [Microsoft Government Cloud](#)
- [Compliance on the Microsoft Trust Center](#)

# Sarbanes-Oxley Act of 2002 (SOX)

11/30/2020 • 3 minutes to read • [Edit Online](#)

## SOX overview

The Sarbanes-Oxley Act of 2002 is a US federal law administered by the Securities and Exchange Commission (SEC). Among other directives, SOX requires publicly traded companies to have proper internal control structures in place to validate that their financial statements accurately reflect their financial results.

The SEC does not define or impose a SOX certification process. Instead, it provides broad guidelines for the companies it regulates to determine how to comply with SOX reporting requirements.

## Microsoft and SOX

Microsoft cloud services customers subject to compliance with the Sarbanes-Oxley Act (SOX) can use the SOC 1 Type 2 attestation that Microsoft received from an independent auditing firm when addressing their own SOX compliance obligations. This attestation is appropriate for reporting on internal controls over financial reporting.

Even though there is no SOX certification or validation for cloud service providers, Microsoft can help customers meet their SOX obligations. For example, SOX requires internal controls for the preparation and review of financial statements, especially controls that affect the accuracy, completeness, effectiveness, and public disclosure of material changes related to financial reporting. To help companies, Microsoft maintains a SOC 1 Type 2 attestation appropriate for reporting on such controls across a broad portfolio of services that can be used to build a wide range of applications. It is based on the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements 18 (SSAE 18) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402). (This attestation replaced SAS 70.)

The audit report, produced by a third-party auditing firm, attests that Microsoft controls were designed appropriately, in operation on a specified date, and operating effectively over a specified time period. Customers can review the reports to learn about Microsoft control objectives and the effectiveness of its controls, and get access to complementary controls.

To further help Azure clients address their SOX obligations, Microsoft has published [Azure Guidance for Sarbanes-Oxley](#). This paper provides migration best practices, including the implications of complying with SOX, and draws on internal experience migrating SOX-relevant applications — Microsoft Treasury and Microsoft Finance — to Azure.

At Microsoft, we share the responsibility of compliance with our customers. We supply the specifics about our compliance programs, which you can verify by requesting detailed audit results from the certifying third parties. Ultimately, however, it is up to you to determine whether our services comply with the specific laws and regulations applicable to your business. For example, there are SOX-related security controls, such as user access to cloud resources, that are your responsibility: your organization must develop appropriate auditing of these controls as part of your SOX compliance.

Learn more about how to use Microsoft Azure compliance reports when addressing your SOX compliance obligations: [Download the Azure Guidance for Sarbanes-Oxley](#)

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)

- Intune
- [Office 365](#)
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Audits, reports, and certificates

[SOC 1 Type 2](#) reports for:

- Azure and Power BI
- Dynamics 365
- Office 365

## Frequently asked questions

**How can I use Microsoft SOX compliance to facilitate my organization's compliance process?**

When you migrate your applications and data to covered Microsoft cloud services, you can build on the attestations and certifications that Microsoft holds. Independent auditor reports attest to the effectiveness of controls that Microsoft has implemented to help maintain the security and privacy of your data. However, you are wholly responsible for ensuring your organization's compliance with all applicable laws and regulations.

## Resources

- [Azure Guidance for Sarbanes-Oxley](#)
- [Microsoft Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)
- [Shared responsibilities for cloud computing](#)
- [Compliance on the Microsoft Trust Center](#)

## About TruSight

TruSight was founded by a consortium of leading financial services companies, including American Express, Bank of America, Bank of New York Mellon, JPMorgan Chase, and Wells Fargo. Their goal was to harness their collective financial expertise and combine their best practices into a consistent assessment methodology that elevates standards and simplifies the process of managing third-party relationships and the associated risk.

## Microsoft and TruSight

TruSight is a third-party risk-assessment utility created by leading US banks for the collective benefit of financial institutions, their suppliers, partners, and other third parties. TruSight simplifies assessments by executing best-practice, standardized evaluations once and making them available to many — enabling financial institutions to gain greater visibility into potential risks and manage third-party relationships more efficiently and effectively.

The foundation of TruSight's methodology is the robust, standardized Best Practices Questionnaire (BPQ) created by TruSight's founding banks and updated in partnership with their customers and industry experts. Its 27 diversified control domains are designed to meet the industry's evaluation needs across the categories of information and cyber security, privacy, business resiliency, and other operational risk domains.

For Microsoft, TruSight conducted a rigorous and comprehensive onsite assessment of Microsoft Azure, Microsoft Dynamics 365, Microsoft Power Platform, and Microsoft 365 to validate the design and implementation of controls according to BPQ requirements. The comprehensive validation procedures included structured inquiries, policy and procedure inspections, reviews with supporting evidence, and onsite dynamic control observations.

In September 2018, TruSight issued its first risk assessment of Microsoft cloud services, *Comprehensive Assessment of Microsoft Cloud*. Microsoft now undergoes annual TruSight reviews to ensure that the assessment remains current and reflects new regulatory requirements and technology updates in Microsoft services. TruSight has issued its latest report in October 2020.

As a result of this rigorous TruSight evaluation, financial services customers now have access on demand to a high-quality assessment of Microsoft cloud services based on standardized, industry-backed methodology without having to expend the considerable resources they would need to conduct it themselves.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365 \(version 9 and subsequent versions\)](#)
- [Microsoft 365](#)

## Audits, reports, and certificates

To purchase the *Comprehensive Assessment of Microsoft Cloud* report, contact [info@trusightsolutions.com](mailto:info@trusightsolutions.com). TruSight updates its assessment annually of our cloud services to ensure alignment with the latest regulatory requirements and advancements in Microsoft technology.

## How to implement

- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Use case overviews, tutorials, and other resources to build Azure solutions for financial services.
- [US financial services regulation](#): How Microsoft online services align with key regulatory expectations for US financial institutions.

## Frequently asked questions

**What are the benefits of relying on the TruSight assessment of Microsoft enterprise cloud services?**

- **Cost reallocation**: The TruSight report eliminates the need for financial institutions to conduct their own costly, time-consuming assessments, enabling them to focus their resources on managing — rather than assessing — risk.
- **Improved quality**: The TruSight methodology has established a consistent set of standards, which improves the quality and accuracy of information available from third parties.

## Resources

- [Microsoft Cloud Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)
- [Shared responsibilities for cloud computing](#)
- [Compliance on the Microsoft Trust Center](#)

# Health Data Hosting (HDS) France

11/30/2020 • 3 minutes to read • [Edit Online](#)

## About HDS

The Hébergeurs de Données de Santé (HDS) certification is required for entities such as cloud service providers that host the personal health data governed by French laws and collected for delivering preventive, diagnostic, and other health services. The HDS regulation was issued by [ASIP SANTÉ](#) which, under the French Ministry of Health, is responsible for promoting electronically based healthcare solutions in France.

Hosting of health data is regulated under French law by the French Public Health Code (Article L.1111-8), which stipulates that any healthcare organization—hospitals, pharmaceutical companies, laboratories—that handles personal medical data must use a service provider that is HDS-certified. In April 2018, new Articles R1111-8-8 to R1111-11 of the Public Health Code took effect, changing the accreditation procedure from an authorization by the French Ministry of Health to certification by an authorized body such as BSI.

HDS certification requires that service providers implement measures that keep personal health data secure, confidential, and accessible by patients. These measures include strong authentication and authorization procedures, robust backup systems, and powerful encryption methods. HDS also specifies mandatory provisions that must be included in contracts with the cloud service provider. These requirements apply no matter where the data is stored.

## Microsoft and HDS

Microsoft Azure, Microsoft Dynamics 365, and Microsoft Office 365 have been granted the Health Data Hosting (Hébergeurs de Données de Santé, HDS) certification, which is required for all entities hosting personal health data governed by French law. This made Microsoft the first major cloud service provider to meet the strict French standards for storing and processing health data. This certification, required by the revision to the 2018 French Public Health Code, imposes advanced security and privacy requirements on hosting services and cloud providers to ensure that the confidentiality and integrity of sensitive data is adequately protected.

Microsoft compliance with the HDS requirements has been audited and certified by the [BSI Group](#), an independent certifying body accredited by French authorities to conduct HDS audits.

The HDS certification enables healthcare providers in France to use Microsoft cloud services to save costs by improving clinical and operational efficiency, and it opens the door to the development of innovative, cutting-edge healthcare solutions. Providers are able to develop smart applications or use third-party applications hosted on Azure to implement predictive analytics to personalize healthcare, evaluate and treat patients at a distance (tele-medicine), and sharpen therapeutic drug monitoring.

The rigorous audit covered the measures Microsoft has taken to secure personal health data and protect its confidentiality, including the:

- [ISO/IEC 27001:2013 Information Security Management](#) certification of Microsoft cloud services, which are audited annually for compliance.
- High level of privacy based on compliance with the GDPR and the [ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud](#).

## Microsoft in-scope cloud services

- [Azure](#). The HDS certificate applies to Azure services listed as compliant with the ISO/IEC 27001 standard in

Azure Compliance offerings and provisioned from the France Central, France South, Europe West, and Europe North Azure regions.

- Dynamics 365. The HDS certificate applies to Dynamics 365 [Core Online Services](#) provisioned from France and European Union geographies.
- Intune
- Microsoft 365. The HDS certificate applies to Office 365 [Core Online Services](#) provisioned from France and European Union geographies.
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

The HDS certificate does not apply to Microsoft online services in preview or pre-release.

## Audits, reports, and certificates

The HDS certification is valid for three years.

- HDS: 2018: [ASIP SANTÉ](#)
- [BSI Group](#)

## How to implement

- **Contractual terms:** French Public Health code requires the execution of specific contractual terms between the health data hosting service or cloud service provider and its customers. Eligible customers must reach out to their Microsoft licensing point of contact to enter into these specific contractual terms before hosting health personal data on Microsoft online services.
- **Health and life sciences:** Case overviews, solution guides, tutorials, and other resources to help build Azure solutions.

## Resources

- [Microsoft Online Services Terms](#)
- [Microsoft HDS certification blog](#)
- [Azure France](#)
- [Azure for health](#)
- [Security at Microsoft](#)
- [Compliance on the Microsoft Trust Center](#)

# Health Insurance Portability and Accountability (HIPAA) & HITECH Acts

2/17/2021 • 6 minutes to read • [Edit Online](#)

## HIPAA and the HITECH Act overview

The Health Insurance Portability and Accountability Act (HIPAA) is a US healthcare law that establishes requirements for the use, disclosure, and safeguarding of individually identifiable health information. It applies to covered entities, doctors' offices, hospitals, health insurers, and other healthcare companies, with access to patients' protected health information (PHI), as well as to business associates, such as cloud service and IT providers, that process PHI on their behalf. (Most covered entities do not carry out functions such as claims or data processing on their own; they rely on business associates to do so.)

The law regulates the use and dissemination of PHI in four general areas:

- Privacy, which covers patient confidentiality.
- Security, which deals with the protection of information, including physical, technological, and administrative safeguards.
- Identifiers, which are the types of information that cannot be released if collected for research purposes.
- Codes for electronic transmission of data in healthcare-related transactions, including eligibility and insurance claims and payments.

The scope of HIPAA was extended with the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Together, HIPAA and HITECH Act rules include:

- The HIPAA Privacy Rule, which focuses on the right of individuals to control the use of their personal information, and covers the confidentiality of PHI, limiting its use and disclosure.
- The HIPAA Security Rule, which sets the standards for administrative, technical, and physical safeguards to protect electronic PHI from unauthorized access, use, and disclosure. It also includes such organizational requirements as Business Associate Agreements (BAAs).

The HITECH Breach Notification Final Rule, which requires giving notice to individuals and the government when a breach of unsecured PHI occurs.

## Microsoft and HIPAA and the HITECH Act

HIPAA regulations require that covered entities and their business associates, in this case, Microsoft when it provides services, including cloud services, to covered entities, enter into contracts to ensure that those business associates will adequately protect PHI. These contracts, or BAAs, clarify and limit how the business associate can handle PHI, and set forth each party's adherence to the security and privacy provisions set forth in HIPAA and the HITECH Act. Once a BAA is in place, Microsoft customers (covered entities) can use its services to process and store PHI.

Currently there is no official certification for HIPAA or HITECH Act compliance. However, those Microsoft services covered under the BAA have undergone audits conducted by accredited independent auditors for the Microsoft ISO/IEC 27001 certification.

Microsoft enterprise cloud services are also covered by FedRAMP assessments. Microsoft Azure and Microsoft Azure Government received a Provisional Authority to Operate from the FedRAMP Joint Authorization Board; Microsoft Dynamics 365 U.S. Government received an Agency Authority to Operate from the US Department of



Housing and Urban Development, as did Microsoft Office 365 U.S. Government from the US Department of Health and Human Services.

To learn how the Microsoft Cloud helps customers support HIPAA and the HITECH requirements, visit [Microsoft Customer Stories](#).

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Microsoft Cloud App Security
- [Microsoft Cloud for Healthcare](#)
- Microsoft Healthcare Bot Service
- [Microsoft Managed Desktop](#)
- Microsoft Stream
- Microsoft Professional Services: Premier and On Premises for Azure, Dynamics 365, Intune, and for medium business and enterprise customers of Microsoft 365 for business
- [Dynamics 365 and Dynamics 365 U.S. Government](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Intune
- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Azure DevOps Services

## Accelerate your deployment of HIPAA/HITRUST solutions on Azure

Get a head start on taking advantage of the benefits of the cloud for health data solutions with the [Azure Security and Compliance Blueprint: HIPAA/HITRUST Health Data and AI](#). This blueprint provides tools and guidance to get you started building HIPAA/HITRUST solutions today.

## Frequently asked questions

### Can my organization enter into a BAA with Microsoft?

Microsoft offers qualified companies or their suppliers a BAA that covers in-scope Microsoft services.

For Microsoft cloud services: The [HIPAA Business Associate Agreement](#) is available via the Online Services Terms by default to all customers who are covered entities or business associates under HIPAA. See 'Microsoft in-scope cloud services' on this webpage for the list of cloud services covered by this BAA.

For Microsoft Professional Services services: The HIPAA Business Associate Amendment is available for in-scope Microsoft Professional Services upon request to your Microsoft services representative.

### Does having a BAA with Microsoft ensure my organization's compliance with HIPAA and the HITECH Act?

No. By offering a BAA, Microsoft helps support your HIPAA compliance, but using Microsoft services does not on its own achieve it. Your organization is responsible for ensuring that you have an adequate compliance program and internal processes in place, and that your particular use of Microsoft services aligns with HIPAA and the HITECH Act.

## Can Microsoft modify my organization's BAA?

Microsoft cannot modify the HIPAA BAA, because Microsoft services are consistent for all customers and so must follow the same procedures for everyone. However, to create the BAA for Microsoft's HIPAA-regulated customers and its services, Microsoft collaborated with some of the leading US medical schools and their HIPAA privacy counsel, as well as other public- and private-sector HIPAA-covered entities.

## How can I get copies of the auditor's reports?

The [Service Trust Portal](#) provides independently audited compliance reports. You can use the portal to request audit reports so that your auditors can compare Microsoft's cloud services results with your own legal and regulatory requirements.

## How can I learn more about complying with HIPAA and the HITECH Act?

To assist customers with this task, Microsoft has published these guides:

- *HIPAA/HITECH Act implementation guidance* for [Azure](#) and for [Dynamics 365 and Office 365](#). Written for privacy, security, and compliance officers and others responsible for HIPAA and HITECH Act implementation, they describe concrete steps your organization can take to maintain compliance.
- [Practical guide to designing secure health solutions using Microsoft Azure](#) helps you better understand what it takes to successfully adopt a cloud service in a secure manner.
- [Addressing HIPAA security and privacy requirements in the Microsoft Cloud](#) offers a brief overview of regulation requirements. It also provides a detailed analysis of how Microsoft's cloud services were built with methodologies that map to those requirements, and guidance on how to build compliance-ready solutions.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [HIPAA Omnibus Rule](#) (The final regulations-modifying HIPAA rules)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Microsoft Online Services Terms](#)
- [Microsoft Government Cloud](#)
- [Understanding HIPAA Compliance with Azure](#)(May 19, 2016)
- [Azure HIPAA HITRUST blueprint sample](#)
- [Compliance on the Microsoft Trust Center](#)

# Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)

2/17/2021 • 6 minutes to read • [Edit Online](#)

## HITRUST — CSF overview

The Health Information Trust Alliance (HITRUST) is an organization governed by representatives from the healthcare industry. HITRUST created and maintains the Common Security Framework (CSF), a certifiable framework to help healthcare organizations and their providers demonstrate their security and compliance in a consistent and streamlined manner.

The CSF builds on HIPAA and the HITECH Act, which are US healthcare laws that have established requirements for the use, disclosure, and safeguarding of individually identifiable health information, and that enforce noncompliance. HITRUST provides a benchmark — a standardized compliance framework, assessment, and certification process — against which cloud service providers and covered health entities can measure compliance. The CSF also incorporates healthcare-specific security, privacy, and other regulatory requirements from such existing frameworks as the Payment Card Industry Data Security Standard ([PCI-DSS](#)), [ISO/IEC 27001](#) information security management standards, and Minimum Acceptable Risk Standards for Exchanges ([MARS-E](#)).

The CSF is divided into 19 different domains, including endpoint protection, mobile device security, and access control. HITRUST certifies IT offerings against these controls. HITRUST also adapts requirements for certification to the risks of an organization based on organizational, system, and regulatory factors.

Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)

HITRUST offers three degrees of assurance, or levels of assessment: self-assessment, CSF validated, and CSF-certified. Each level builds with increasing rigor on the one below it. An organization with the highest level, CSF-certified, meets all the certification requirements of the CSF. Microsoft Azure and Office 365 are the first hyperscale cloud services to receive certification for the HITRUST CSF. Coalfire, a HITRUST assessor firm, performed the assessments based on how Azure and Office 365 implement security, privacy, and regulatory requirements to protect sensitive information. Microsoft supports the HITRUST Shared Responsibility Program.

Learn how to accelerate your HITRUST deployment with our Azure Security and Compliance Blueprint.

[Download the Microsoft Azure HITRUST Customer Responsibility Matrix \(CRM\) blueprint v9.0d](#)

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Intune
- [Microsoft Managed Desktop](#)
- [Office 365 and Office 365 U.S. Government](#)

## Audits, reports, and certificates

The HITRUST CSF certification of Azure and Office 365 is valid for two years.

- [Azure HITRUST Letter of Certification](#)
- [Office 365 HITRUST Letter of Certification](#)

# Accelerate your deployment of HIPAA/HITRUST solutions on Azure

Get a head start on taking advantage of the benefits of the cloud for health data solutions with the Azure Security and Compliance Blueprint — HIPAA/HITRUST Health Data and AI. This blueprint provides tools and guidance to get you started building HIPAA/HITRUST solutions today.

[Start using the Azure HIPAA/HITRUST Blueprint](#)

## Accelerate your HIPAA/HITRUST compliance when using Office 365

Use Office 365 to manage health information in a secure and compliant way with Compliance Score, which enables you to perform risk assessments against health regulations like HIPAA and security control frameworks like NIST CSF and NIST 800-53. You can follow step-by-step guidance to know how to implement and maintain data protection controls that help you meet healthcare compliance obligations.

[Start using Compliance Score](#)

## Collaborate with Microsoft in the HITRUST Shared Responsibility Program

Accelerate achieving HITRUST compliance for your solution hosted on Microsoft Azure by pre-populating your assessment with fully inherited or shared responsibility controls for Azure in the HITRUST MyCSF tool, and collaborating with Microsoft on your assessment.

[Learn more](#)

## Frequently asked questions

### Can I use the Azure HITRUST compliance to build on my organization's certification process?

Yes. If your business requires a HITRUST certification for implementations deployed on Microsoft services, you can build on Azure HITRUST compliance when you conduct your compliance assessment. However, you are responsible for evaluating the HITRUST requirements and controls within your own organization.

### How can I get a copy of the HITRUST certification?

You can download a copy of letter of certification for [Azure](#) and [Office 365](#).

### What are the in-scope services for Office 365?

The in-scope services of HITRUST CSF certification are Exchange Online Archiving, Exchange Online Protection, Exchange Online, Skype for Business, Admin Center, SharePoint Online, Project Online, OneDrive for Business, Office Online, MyAnalytics, Microsoft Teams, Microsoft 365 Apps for enterprise in Office 365 Multi-tenant cloud and Office 365 GCC.

#### **NOTE**

Microsoft 365 Apps for enterprise enables access to various cloud services, such as Roaming Settings, Licensing, and OneDrive consumer cloud storage, and may enable access to additional cloud services in the future. Roaming Settings and Licensing support the standards for HITRUST. OneDrive consumer cloud storage does not, and other cloud services that are accessible through Microsoft 365 Apps for enterprise and that Microsoft may offer in the future also may not, support these standards.\*

### Why are some Office 365 services not in the scope of this certification?

Microsoft provides the most comprehensive offerings compared to other cloud service providers. To keep up

with our broad compliance offerings across regions and industries, we include services in the scope of our assurance efforts based on the market demand, customer feedback, and product lifecycle. If a service is not included in the current scope of a specific compliance offering, your organization has the responsibility to assess the risks based on your compliance obligations and determine the way you process the data in that service. We continuously collect feedback from customers and work with regulators and auditors to expand our compliance coverage to meet your security and compliance needs.

### **Does Microsoft certification mean that if my organization uses Azure or Office 365, it is compliant with HITRUST CSF?**

When you store your data in a SaaS like Office 365, it's a shared responsibility between Microsoft and your organization to achieve compliance. Microsoft manages majority of the infrastructure controls including physical security, network controls, application level controls, etc., and your organization has the responsibility to manage access controls and protect your sensitive data. The Office 365 HITRUST certification demonstrates the compliance of Microsoft's control framework. Building on that, your organization needs to implement and maintain your own data protection controls to meet HITRUST CSF requirements.

### **Does Microsoft provide guidance for my organization to implement appropriate controls when using Office 365?**

Yes, you can find recommended customer actions in Compliance Score, cross-Microsoft Cloud solutions that help your organization meet complex compliance obligations when using cloud services. Specifically, for HITRUST CSF, we recommend that you perform risk assessments using the NIST 800-53 and NIST CSF assessments in Compliance Score. In the assessments, we provide you with step-by-step guidance and the Microsoft solutions you can use to implement your data protection controls. You can learn more about Compliance Score in [Microsoft Compliance Score](#).

### **How do I engage with Microsoft?**

Log in to the HITRUST MyCSF<sup>®</sup> tool and pre-populate your assessment for your solution hosted on Microsoft Azure with either fully inherited or shared responsibility controls for Azure. A Microsoft HITRUST Administrator will then complete their part of the assessment using their account on the MyCSF<sup>®</sup> tool.

## **Use Microsoft Compliance Manager to assess your risk**

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## **Resources**

- [HITRUST Alliance](#)
- [HITRUST CSF 9.3](#)
- [Understanding and Leveraging the CSF](#)
- [Find out more about the HITRUST Shared Responsibility Program](#)
- [Compliance on the Microsoft Trust Center](#)

# Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0 Framework

11/30/2020 • 3 minutes to read • [Edit Online](#)

## MARS-E 2.0 Framework overview

In 2012, the Center for Medicare and Medicaid Services (CMS) published the Minimum Acceptable Risk Standards for Exchanges (MARS-E) in accordance with CMS information security and privacy programs. The suite of documents, including guidance, requirements, and templates, was designed to address mandates of the Patient Protection and Affordable Care Act (ACA) and regulations of the Department of Health and Human Services that apply to the ACA. The National Institute of Standards and Technology (NIST) Special Publication 800-53 serves as the parent framework that establishes the security and compliance requirements for all systems, interfaces, and connections between ACA-mandated health exchanges and marketplaces.

Following the release of MARS-E, NIST released an update, Special Publication 800-53r4, to address growing challenges to online security, including application security; insider and advanced persistent threats; supply chain risks; and the trustworthiness, assurance, and resilience of systems of mobile and cloud computing. CMS then revised the MARS-E framework to align with the updated controls and parameters in NIST 800.53r4, publishing MARS-E 2.0 in 2015.

These updates address the confidentiality, integrity, and availability in health exchanges of protected data, which includes personally identifiable information, protected health information, and federal tax information. The MARS-E 2.0 framework aims to secure this protected data and applies to all ACA administering entities, including exchanges or marketplaces, federal, state, state Medicaid, or Children's Health Insurance Program (CHIP) agencies, and supporting contractors.

## Microsoft and MARS-E 2.0 framework

Currently, there is no formal authorization and accreditation process for MARS-E. However, Microsoft Azure platform services have undergone independent FedRAMP audits at the Moderate Impact Level and Azure Government at the High Impact Level, and are authorized according to FedRAMP standards. Although these standards do not specifically focus on MARS-E, the MARS-E control requirements and objectives are closely aligned and serve to protect the confidentiality, integrity, and availability of data on Azure.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Intune

## Audits, reports, and certificates

Microsoft business cloud services are monitored and assessed each year for the FedRAMP authorization process.

## Frequently asked questions

### To whom does the standard apply?

MARS-E applies to all Affordable Care Act administering entities, including exchanges or marketplaces, federal, state, Medicaid, and CHIP agencies administering the Basic Health Program, as well as all their contractors and

subcontractors.

### **How does Microsoft demonstrate Azure and Azure Government compliance with this standard?**

Using the formal audit reports prepared by third parties for FedRAMP authorizations, Microsoft is able to show how relevant controls noted that within these reports demonstrate Azure capabilities in meeting MARS-E security and privacy control requirements. Audited controls implemented by Microsoft serve to protect the confidentiality, integrity, and availability of data stored on the Azure platform, and correspond to the applicable regulatory requirements defined in MARS-E that have been identified as the responsibility of Microsoft.

### **What are Microsoft's responsibilities for maintaining compliance with this standard?**

Microsoft ensures that the Azure platform meets the terms defined within the governing [Online Services Terms](#) and applicable service level agreements (SLAs). These agreements define our responsibility for implementing and maintaining controls adequate to secure the Azure platform and monitor the system.

### **Can I use Microsoft's compliance in the MARS-E qualification efforts for my organization?**

Yes. Third-party audit reports to the FedRAMP standards attest to the effectiveness of the controls Microsoft has implemented to maintain the security and privacy of the Azure platform. Azure and Azure Government customers may use the audited controls described in these related reports as part of their own FedRAMP and MARS-E risk analysis and qualification efforts.

## **Resources**

- MARS-E regulatory guidance, MARS-E Document Suite, Version 2.0
  - [Volume II: Minimum acceptable risk standards for exchanges](#)
  - [Volume III: Catalog of minimum acceptable risk security and privacy controls for exchanges](#)
- [Microsoft compliance framework for online services white paper](#)
- [Microsoft cloud services terms](#)
- [Compliance on the Microsoft Trust Center](#)

# NEN 7510

1/26/2021 • 3 minutes to read • [Edit Online](#)

## NEN 7510 overview

Organizations in the Netherlands that process patient health information must demonstrate control over that data and their organization consistent with the requirements set out in the NEN 7510 standard. Microsoft is not itself subject to NEN 7510, but its cloud customers in the healthcare sector need to establish that they comply with NEN 7510 regarding solutions built on the Microsoft Cloud. Microsoft cloud services undergo various periodic certifications and audits, some of which include elements closely related to requirements specified in NEN 7510.

## Microsoft and NEN 7510:2011

Microsoft has analyzed our current certifications and assurance statements and created a [NEN 7510 coverage report](#) (available on the Service Trust Platform), which maps those certifications and assurance statements against the NEN 7510 controls for which Microsoft is responsible as a cloud service provider. This document can help customers determine which other controls they must implement to ensure that their use of Microsoft cloud services for the storage or processing of patient health information complies with NEN 7510.

Learn how to accelerate your NEN 7510 deployment with our Azure Security and Compliance Blueprints: [Download the Microsoft Cloud: Azure and Office 365 NEN7510-2011 Standard Coverage User Guide](#)

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Intune
- [Office 365](#)

## Audits, reports, and certificates

- [Azure and Office 365 NEN 7510:2011 Standard Coverage](#)

## Frequently asked questions

### Is a customer that uses Microsoft cloud services compliant with NEN 7510?

Demonstrating NEN compliance is the responsibility of the healthcare organization (the 'customer'). When using a cloud services vendor, customers typically demand assurances from the vendor, and add their own (other) technology and organizational decisions, choices, and processes. This effort results in an overall assessment by the customer on its NEN 7510 compliance, which can be submitted for review or certification to a third-party auditor. The NEN 7510 coverage report provides insight into which NEN 7510 controls are covered by Microsoft cloud services, but, as such, does not cover end-to-end compliance.

### Is Microsoft compliant with NEN 7510?

The responsibility for NEN 7510 compliance is applicable to Dutch Healthcare organizations. It requires the organization to implement an information security management system and to address risk with appropriate technical and organizational measures. For Microsoft in its role as cloud service provider, NEN 7510 compliance is not the objective, nor is it technically feasible. When a customer implements or uses Microsoft cloud services, those services may be in scope of a NEN 7510 evaluation. However, the organization must add its own (other)



controls, choices, and processes that are part of the overall NEN 7510 evaluation. The objective of the report is to demonstrate that a Healthcare entity can adopt the Microsoft cloud services in a manner that is compliant with NEN 7510.

### **The report does not show 100% coverage. Is NEN 7510 compliance not feasible?**

Microsoft cloud services provide many controls that help organizations within Dutch Healthcare with their NEN 7510 compliance needs. However, an organization needs to complement those vendor assurances with their own implementation choices, other technology controls, and administrative processes. The report shows already over 94% direct coverage of the full list of applicable controls. For the remaining controls, Microsoft provides guidance in the report on how compliance with those controls can be demonstrated.

#### **NOTE**

Implementing the full list of controls is not the primary purpose of NEN 7510 (although the large coverage of Microsoft Online Services does help). NEN 7510 mandates the implementation of a risk-based information security system that can be used by an organization to determine which controls are applicable to them.

### **Is the NEN 7510 coverage report a legal binding document?**

No. It is a supporting tool for the customer's internal NEN 7510 assurance process and helps to establish confidence and trust that NEN 7510 compliance is feasible. The report (created by independent auditor, KPMG) has a descriptive status and includes a legal disclaimer.

### **Did Microsoft pay for the report?**

Microsoft created a mapping between its global assurances to the controls in the NEN 7510 standard. Microsoft then hired KPMG (an independent auditor) to perform an independent review on the control mapping to NEN 7510, which resulted in the report.

### **Can we share this report?**

The report is provided with you under a non-disclosure agreement (NDA), on the basis that it is for customer information only and that it will not be copied or disclosed via other channels than the Microsoft Service Trust Portal.

Customers can share the report with their own internal or external auditor as part of their compliance or assurance processes.

## **Resources**

- [About NEN](#)
- [NEN 7510:2011 standard](#)
- [Compliance on the Microsoft Trust Center](#)

# Food and Drug Administration CFR Title 21 Part 11

2/5/2021 • 5 minutes to read • [Edit Online](#)

## FDA CFR Title 21 overview

The Code of Federal Regulations (CFR) contains the rules and regulations for executive departments and agencies of the US federal government. Each of the 50 titles of the CFR addresses a different regulated area.

[FDA CFR Title 21](#) regulates food and drugs manufactured or consumed in the United States, under the jurisdiction of the Food and Drug Administration (FDA), the Drug Enforcement Administration, and the Office of National Drug Control Policy. The regulations outlined in CFR Title 21 Part 11 set the ground rules for the technology systems that manage information used by organizations subject to FDA oversight. Any technology system that governs such GxP processes as Good Laboratory Practices (GLP), Good Clinical Practices (GCP), and Good Manufacturing Practices (GMP) also requires validation of its adherence to GxP.

CFR Title 21 Part 11 sets requirements to ensure that electronic records and signatures are trustworthy, reliable, and equivalent substitutes for paper records and handwritten signatures. It also offers guidelines to improve the security of computer systems in FDA-regulated industries. Subject companies must prove that their processes and products work as they are designed to, and if these process and products change, they must revalidate that proof. The best practices guidelines cover:

- Standard operating procedures and controls that support electronic records and signatures such as data backup, security, and computer system validation.
- Features that ensure that the computer system is secure, contains audit trails for data values, and ensures the integrity of electronic signatures.
- Validation and documentation that supply evidence that the system does what is intended, and that users can detect when the system is not working as designed.

## Microsoft and FDA CFR Title 21

Microsoft enterprise cloud services undergo regular independent third-party SOC 1 Type 2 and SOC 2 Type 2 audits and are certified according to ISO/IEC 27001 and ISO/IEC 27018 standards.

Although these regular audits and certifications do not specifically focus on FDA regulatory compliance, their purpose and objectives are similar in nature to those of CFR Title 21 Part 11, and serve to help ensure the confidentiality, integrity, and availability of data stored in Microsoft cloud services. Our qualification approach is also based on industry best practices, including the International Society for Pharmaceutical Engineering (ISPE) GAMP series of Good Practices Guides and the Pharmaceutical Inspection Cooperation Scheme (PIC/S) Good Practices for Computerized Systems in Regulated GxP Environments.

Customers can request access to the compliance reports, subject to nondisclosure agreement terms and conditions, through their Microsoft account representative, or through the [Service Trust Portal](#). In addition, qualification guidelines for Microsoft Azure and Microsoft Office 365 provide a detailed explanation of how Microsoft audit controls correspond to the requirements of CFR Title 21 Part 11, guidance for implementing an FDA qualification strategy, and a description of areas of shared responsibility.

Learn how to accelerate your FDA CFR Title 21 deployment: [Download the Azure FDA 21 qualification guide](#)

## Microsoft in-scope cloud services

Although there is no certification for complying with CFR Title 21 Part 11, the following Microsoft enterprise

cloud services have undergone independent, third-party audits, which may help customers in their compliance efforts. These services include:

- Azure: Cloud Services, Storage, Traffic Manager, Virtual Machines, and Virtual Network
- Azure DevOps
- Intune
- [Dynamics 365 and Dynamics 365 U.S. Government](#)
- Office 365 and Office 365 U.S. Government

## Audits, reports, and certificates

The audit reports for SOC 1 and SOC 2 Type 2, ISO/IEC 27001 and ISO/IEC 27018 standards attest to the effectiveness of the controls Microsoft has implemented and may help customers in their compliance with FDA CFR Title 21 Part 11.

## Frequently asked questions

### To whom does the standard apply?

FDA CFR Title 21 Part 11 applies to organizations with products and services that deal in FDA-regulated aspects of the research, clinical study, maintenance, manufacturing, and distribution of life science products.

### How do Microsoft enterprise cloud services demonstrate compliance with FDA CFR Title 21 Part 11?

Using the formal audits prepared by third parties for SOC 1 Type 2, SOC 2 Type 2, ISO/IEC 27001, and ISO/IEC 27018, Microsoft is able to show how relevant controls noted within these reports address the requirements.

Audited controls implemented by Microsoft help ensure the confidentiality, integrity, and availability of data, and correspond to the applicable regulatory requirements defined in Title 21 Part 11 that have been identified as the responsibility of Microsoft. The qualification guidelines for Azure and Office 365 detail how Microsoft audit controls correspond to those requirements.

### How can I get copies of the auditor's reports?

The [Service Trust Portal](#) provides independently audited compliance reports. You can use the portal to request audit reports so that your auditors can compare Microsoft's cloud services results with your own legal and regulatory requirement.

### Can I use Microsoft's compliance in the certification process for my organization?

Yes. The independent third-party compliance reports of the IEC/ISO 27001, ISO/IEC 27018, SOC 1, and SOC 2 standards attest to the effectiveness of Microsoft controls. Microsoft enterprise cloud customers may use the audited controls described in these related reports as part of their own CFR Title 21 Part 11 risk analysis and qualification efforts. Customers who build and deploy applications subject to FDA regulation are responsible for ensuring that their applications meet FDA requirements.

### What are Microsoft's responsibilities for maintaining compliance with this standard?

Microsoft ensures that its enterprise cloud services meet the terms defined within the governing [Online Services Terms](#) and applicable Service Level Agreements (SLAs). These terms define our responsibility for implementing and maintaining controls adequate to secure and monitor the system.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium

template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Azure GxP Qualification Guidelines](#)
- [Code of Federal Regulations Title 21](#)
- [FDA guidance for industry Part 11: Electronic records and signatures](#)
- [Qualification guidelines for Azure](#)
- [Qualification guidelines for Office 365](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Microsoft Online Services Terms](#)
- [Microsoft Cloud for Government](#)
- [Compliance on the Microsoft Trust Center](#)

# Good Clinical, Laboratory, and Manufacturing Practices (GxP)

11/30/2020 • 3 minutes to read • [Edit Online](#)

## About GxP

The term *GxP* is a general abbreviation for 'good practice' guidelines and regulations. The 'x' represents a particular field—clinical (GCP), manufacturing (GMP), distribution (GDP), laboratory (GLP), agriculture (GAP), and so on. There is no single regulatory entity or administration; each country has its own guidelines and regulators, although requirements are similar from country to country. GxP regulations include those requirements outlined in the [US Food and Drug Administration \(FDA\) CFR Title 21 Part 11](#) and [EudraLex Volume 4—GMP Guidelines, Annex 11](#) in the European Union (EU).

Regulatory goals aim to make sure that businesses in regulated industries manufacture products that are safe to use and meet stringent quality standards during the production process. Computerized systems that use GxP processes require validation of adherence to GxP requirements and are considered qualified when the system can demonstrate its ability to fulfill them.

## Microsoft and GxP

Microsoft can help organizations that deal with regulated aspects of the research, clinical study, maintenance, manufacturing, and distribution of life science products and services meet their requirements under Good Clinical, Laboratory, and Manufacturing Practices (GxP). These include regulations enforced by the US Food and Drug Administration (FDA) under CFR Title 21 Part 11 for the security of computer systems and the reliability and trustworthiness of electronic records, as well as EudraLex, Volume 4, Annex 11, recognized guidelines for computerized systems in the EU.

There is no GxP certification for cloud service providers; however:

- Microsoft Azure and Microsoft Office 365 have undergone many independent audits for quality management and information security, including ISO 9001 (QMS) and ISO/IEC 27001 (ISMS). This review includes regular audits of Microsoft procedural and technical controls, verified for effectiveness.
- The Microsoft qualification approach is also based on industry best practices, including the *Good Automated Manufacturing Practices* (GAMP) series of Good Practices Guides (from the International Society for Pharmaceutical Engineering (ISPE)), and *Good Practices for Computerized Systems in Regulated GxP Environments* (from the Pharmaceutical Inspection Cooperation Scheme (PIC/S) PI 011-3).

Although these standards and best practices do not specifically focus on GxP regulatory compliance, their purpose and objectives are similar and help ensure the confidentiality, integrity, and availability of data stored in Microsoft cloud services.

Microsoft retained [Montrium](#), an independent organization specializing in quality assurance and regulatory GxP compliance for the life sciences industry, to conduct the GxP qualification review for Microsoft. The resulting Qualification Guidelines ([Azure](#) and [Office 365](#)) are intended for life sciences organizations that plan to use these cloud services to host and support GxP-regulated computerized systems. The guidelines identify the responsibility shared by Microsoft and its customers for meeting GxP requirements, as well as recommend activities and controls that customers using in-scope Microsoft cloud services can establish to maintain control over GxP computerized systems.

Life sciences organizations building GxP solutions on Azure and Office 365 can take advantage of the cloud's

efficiencies while also protecting patient safety, product quality, and data integrity. Customers also benefit from multiple layers of security and governance technologies, operational practices, and compliance policies that enforce data privacy and integrity at specific levels.

## Microsoft in-scope cloud services

- [Azure](#)
- Microsoft 365
- Microsoft Dynamics 365

## How to implement

- [Microsoft 365 GxP Guidelines](#): A whitepaper for using Microsoft 365 while adhering to GxP best practices and regulations.
- [Microsoft Dynamics 365 GxP Guidelines](#): A whitepaper for using Microsoft Dynamics 365 while adhering to GxP best practices and regulations.
- [Azure GxP Guidelines](#): A comprehensive tool set for using Azure while adhering to GxP best practices and regulations.
- [Using Azure with GxP Systems](#): Help for life science organizations in establishing a strategy for building GxP applications.
- FDA CFR Title 21 Part 11 Guides: Get help establishing an [Azure](#) and [Office 365](#) qualification strategy that complies with FDA guidelines for electronic records.

## Frequently asked questions

**Can I use Microsoft GxP compliance in my organization's GxP compliance efforts?**

Customers deploying applications on Azure should determine the GxP requirements that apply to their computerized systems based on the intended use and then follow internal procedures governing qualification and validation processes to demonstrate that they have met those requirements.

## Resources

- [Microsoft and FDA CFR Title 21 Part 11](#)
- [Microsoft and ISO/IEC 27001](#)
- [Microsoft and ISO 9001](#)
- [Compliance on the Microsoft Trust Center](#)

# Trusted Information Security Assessment Exchange (TISAX) Germany

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About TISAX

To help secure the ever-increasing connectivity in the automotive industry, the German Association of the Automotive Industry ([Verband der Automobilindustrie](#), VDA) developed a catalogue of criteria for assessing information security. The VDA Information Security Assessment ([German](#) and [English](#)) is based on the fundamentals of the international ISO/IEC 27001 and 27002 standards adapted to the automotive industry. In 2017, it was updated to cover controls for the use of cloud services.

VDA member companies used this instrument both for internal security assessments and for assessments of suppliers, service providers, and other partners that process sensitive information on their behalf. However, because these evaluations were handled individually by each company, it created a burden on partners and duplicated effort on the part of VDA members.

To help streamline evaluations, the VDA set up a common assessment and exchange mechanism, the [Trusted Information Security Assessment Exchange](#) (TISAX). The catalogue of underlying TISAX requirements, Questionnaire for Checking Information Security Assessment and Information Security Management, Vers. 4 ([German](#) and [English](#)), provides common standards for IT security measures, and enables companies registered in TISAX to share assessment results. The VDA entrusted a neutral third party, the [ENX Association](#), with TISAX implementation. In that capacity, it accredits audit providers (auditors), maintains the accreditation criteria and assessment requirements, and monitors the quality of implementation and assessment results.

## Microsoft and TISAX

European automotive companies rely on trust to develop, build, and operate new cars. They use the Trusted Information Security Assessment Exchange (TISAX) to provide a common information security assessment for internal analysis, an evaluation of suppliers, and as an information exchange mechanism. An independent ENX-accredited auditor, PwC, completed the TISAX assessment of Microsoft datacenters and operations centers against TISAX specifications and IT security requirements.

Automotive companies around the world can now evaluate the TISAX assessment of Microsoft cloud services to create cloud solutions that integrate strong information security and data protection. Companies can use the TISAX assessment of Microsoft cloud services to confidently exchange data with suppliers who use workstations based on Microsoft 365 cloud services.

Microsoft provided a self-assessment of its cloud services, and the auditor performed two levels of assessment based on that. (The assessment level determines the depth of the evaluation and the methods the auditors use.)

- Microsoft datacenters in Northern Europe (Dublin region, Ireland) and Western Europe (Amsterdam region, the Netherlands) were assessed at Level 3 (AL3). The audit included a thorough verification of security processes, a comprehensive onsite inspection, and in-person interviews. An AL3 assessment is required for data with a high need for protection, such as data classified as strictly confidential or secret—, data from crash test and flow simulations and AI (artificial intelligence) systems.
- Selected Microsoft global datacenters were assessed at Level 2 (AL2) based on remote interviews. An AL2 assessment is required for data with a high need for protection, such as data classified as confidential.

## Microsoft in-scope cloud services

The TISAX assessment focused on the following Microsoft services:

- [Azure](#)
- [Dynamics 365](#)
- Intune
- [Microsoft Power BI, whether enrolled standalone or included in an Office 365 or Microsoft Dynamics 365 branded plan or suite](#)

## Audits, reports, and certificates

Industry representatives registered with ENX can find details on the TISAX assessment of in-scope Microsoft cloud services on the [ENX portal](#). To search for Microsoft assessment results, sign in to your existing TISAX account, and search for Microsoft. Alternatively, you may narrow your search using the information below:

- Microsoft Participant ID: PGKYK0
- Microsoft Corp. EU Assessment Level (AL) 3 scope ID: SY869K
- Microsoft Corp. WORLD Assessment Level (AL) 2 scope ID: S08NT9

This assessment is valid for three years.

## How to implement

### Manufacturing use cases

Use case overviews, solution guides, tutorials, and other resources to help build [Azure solutions](#).

## Frequently asked questions

### Why I can't see a copy of the Microsoft TISAX certification?

ENX provides certification confirmation only to registered industry representatives through the ENX portal. For details about how to proceed, see the "Audits, reports, and certificates" section above.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [TISAX Frequently Asked Questions](#)
- [Volkswagen and Microsoft announce strategic partnership](#)
- [Office in your Car: BMW offers Skype for Business \(German\)](#)
- [Connecting vehicles for the long haul: Daimler](#)
- [Continental is adopting Microsoft Office 365 to boost productivity](#)
- [Microsoft and ISO/IEC 27001:2013](#)
- [Compliance on the Microsoft Trust Center](#)



# Content Delivery & Security Association (CDSA) Content Protection & Security (CPS) Standard

2/5/2021 • 3 minutes to read • [Edit Online](#)

## CDSA overview

The Content Delivery & Security Association (CDSA) is a worldwide forum advocating for the innovative and responsible delivery and storage of entertainment, software, and information content.

The CDSA [Content Protection & Security \(CPS\) Standard](#) provides guidance and requirements for securing media assets within a Content Security Management System (CSMS). The standard specifies a set of controls designed to ensure the integrity of intellectual property and the confidentiality and security of media assets at every stage of the digital media supply chain.

The CPS certification audit is administered directly by the CDSA and consists of over 300 distinct controls that help secure and manage physical datacenters, harden services, and protect storage facilities. All controls are optimized to handle sensitive and valuable media assets. Once a system is validated by the CDSA assessor, the CDSA issues a certificate of compliance. To maintain compliance, the certified entity must submit the results of annual audits to the CDSA.

## Microsoft and CDSA — CPS Standard

The Microsoft Azure Media Services CSMS has been validated by the CDSA, awarding Azure Media Services certification to this standard. Microsoft demonstrated a proof of risk assessment against the CPS standard requirements. We also filed a comprehensive Statement of Applicability that articulated the content protection features of Azure Media Services. Microsoft is committed to continuing the annual CDSA audits, and maintaining the internal audits and controls necessary to retain CPS certification.

The CPS certification provides a standards-based method of assuring our customers and yours that the intellectual property rights of media assets stored, managed, and distributed from within Azure are protected. Furthermore, you can use Azure CPS certification toward your own CPS certification efforts.

Azure Media Services was the first hyperscale cloud media platform to offer encryption on the fly for both Video On Demand and live-streaming broadcasts. Azure Media Services provides several security-enhanced upload channels for content, including the ExpressRoute private network connection to Azure, UDP upload via the Aspera client, and HTTPS upload over the Internet.

- Learn about the benefits of CDSA on the Microsoft Cloud: [Learn how the CDSA transforms movie-making in the cloud with Microsoft Azure](#)
- Learn how to accelerate your CDSA deployment with our Azure Security and Compliance Blueprints: [Download the Microsoft Azure — Implementing CDSA-Compliant Content Protection and Security guide](#)

## Microsoft in-scope cloud services

- [Azure Media Services](#)

## Audits, reports, and certificates

Microsoft has successfully completed the six-month renewal of the CDSA CPS certification, and Azure is now on an annual audit cycle.

- [Azure Media Services Certificate of Compliance](#)
- [Azure CDSA CPS Audit Report](#)
- [Azure CDSA implementation guide](#)

## Frequently asked questions

### To whom does the standard apply?

The standard applies to any provider that wants to provide cloud services to the media production industry.

### How do I start my organization's compliance effort?

For guidance, refer to the [CDSA Azure implementation guide](#). To discuss specific requirements and the application process for CPS Standard Certification Program, please [contact the CDSA](#).

### Can I use Microsoft compliance in my organization's certification process?

Yes. You can build on Azure CPS certification within your own CPS certification effort by using the security and encryption features in Azure.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [CDSA](#)
- [CPS Standard](#)
- [Azure Media Services Certificate of Compliance](#)
- [How Azure Media Services earned CDSA security certification](#)
- [Compliance on the Microsoft Trust Center](#)
- [Understanding CDSA and Azure compliance](#)

# Digital Production Partnership (DPP) United Kingdom

2/5/2021 • 2 minutes to read • [Edit Online](#)

## About the DPP

Broadcasters are confronting increasingly frequent cyber-attacks against their websites, IT infrastructure, and systems. In response to these threats, the [Digital Production Partnership \(DPP\)](#) partnered with the [North American Broadcasters Association \(NABA\)](#) to develop the [Broadcasters Cyber Security Requirements for Suppliers](#). Chief information security officers from UK broadcasters have endorsed these as the minimum cybersecurity requirements.

The DPP then worked with broadcasters and supplier security experts to create a self-assessment inventory, the [Committed to Security Program Broadcast Checklist](#), which enables suppliers to demonstrate to broadcasters their deployment of cybersecurity best practices. This work led to establishing a formal [DPP Committed to Security Program](#) launched in October 2017, with two different marks: one for Broadcast and one for Production.

## Microsoft and the DPP

Microsoft Azure has been awarded the DPP Committed to Security Mark for Broadcast after completing the Digital Production Partnership (DPP) self-assessment questionnaire, the *Committed to Security Program Broadcast Checklist*. It required documenting a set of best practices for documentation and testing, authentication, and security controls. [Eurofins Digital Testing](#), a quality assurance expert and DPP member, reviewed and signed off on the Microsoft response and submitted it to the DPP for final validation.

This support means that broadcasters and other media customers using Azure can have confidence that its robust security and resilient service can help meet the unique demands of the broadcast industry, from program development to transmission.

## Microsoft in-scope cloud services

- [Azure](#)

## Audits, reports, and certificates

The Azure Broadcast mark is valid for one year and renewed annually.

- [Azure NABA DPP Broadcaster Security Requirements Checklist](#)
- [DPP Committed to Security Companies Awarded the Marks](#)

## How to implement

- [Asset Management Hardening Guide](#): Best practices in Azure protect pre-release content from unauthorized disclosure, change, or deletion.
- [Azure Media Services](#): Build solutions that achieve high-definition video encoding and broadcast-quality video streaming.

## Resources

- [DPP Committed to Security Program Broadcast Checklist User Guide](#)
- [NABA and DPP Broadcasters Unite to Promote Cyber Security Requirements for Suppliers](#)
- [Compliance on the Microsoft Trust Center](#)

# Federation Against Copyright Theft (FACT)

11/30/2020 • 2 minutes to read • [Edit Online](#)

## FACT overview

Copyrighted content comes in many forms, pictures, videos, music, contracts, scripts, workflows, art, architecture, and more, and represents the core assets of many businesses. Piracy threatens to undermine the very existence of these businesses through the unlawful distribution of intellectual property for illicit gain or market disruption. As production and post-production workflows increasingly move to the cloud, the black market for intellectual property is similarly moving away from physical media toward online mechanisms.

## Microsoft and Federation Against Copyright Theft (FACT)

To underscore Microsoft's commitment to protect customers when they entrust such assets to the public cloud, Microsoft Azure has been certified by the Federation Against Copyright Theft (FACT) in the United Kingdom. FACT certification is based on ISO 27001, focusing on physical and digital security, staff screening and training, and access control. The FACT content protection and security program incorporates expertise across law enforcement, technology partners, and industry associations to fight copyright infringement and content theft, such as peer-to-peer sharing, illegal disc duplication, and signal theft.

Based on the voluntary submission by Microsoft to a FACT audit, the FACT auditor certified Azure. Azure was the first multi-tenant public cloud service to achieve FACT certification, adding to Azure's portfolio of media-related certifications, including CDSA certification and a formal assessment by the MPAA.

## Microsoft in-scope cloud services

[Azure and Azure Government](#)

## Audits, reports, and certificates

The Azure certification is renewed annually: [Azure FACT certificate](#)

## Frequently asked questions

### Why is FACT important?

Content security is critical for feature film and television development, as there are multiple points along the workflow where digital assets can be compromised or stolen. Dailies, rough cuts, and visual effects are just some of the materials exposed during a normal film production cycle, and the box-office impacts of a security breach on a blockbuster project can reach tens of millions of dollars. By passing the FACT audit, Azure provides another layer of assurance to customers by helping to prevent the illegal distribution and sale of motion picture and television assets.

### Does my organization still need to undergo a FACT audit, or can we use the Azure audit?

Compliance with FACT is voluntary, but Microsoft elected to carry out an independent assessment so that media customers can be confident in the content security and protection capabilities of Azure. However, customers' individual cloud environments are not managed by Azure, and thus may be subject to additional regulation that is best addressed by an individual audit.

## Resources

- Federation Against Copyright Theft
- [Fact Security Certification Program](#)
- [CDSA certification of Azure Media Services](#)
- [Azure ISO 27001 certification](#)
- [MPAA Assessment](#)
- [Azure Responses to CSA CAIQ v3.0.1](#)
- [Compliance on the Microsoft Trust Center](#)

# Motion Picture Association of America (MPAA)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## MPAA overview

The Motion Picture Association of America (MPAA) provides best-practices guidance and control frameworks to help major studio partners and vendors design infrastructure and solutions to ensure the security of digital film assets. The MPAA also performs content security assessments on behalf of its member companies: Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, and Warner Bros. Entertainment Inc.

## Microsoft and MPAA

In February 2016, Microsoft Azure became the first hyperscale, multitenant cloud service to successfully complete a formal assessment by independent MPAA auditors and comply with all three of the MPAA content security best practices frameworks: Common, Application, and Cloud Security Guidelines.

The MPAA assessment covers 48 security topics in the Common Guidelines, and an additional six in the Application and Cloud Security Guidelines. These are built on industry-accepted security standards such as ISO/IEC 27001 and NIST 800-53, and are aligned to best practices, such as the Cloud Security Alliance (CSA) Cloud Controls Matrix.

The formal assessment of Azure compliance means that companies who do business with major studios can use Azure to help reduce the IT costs that are normally associated with the secure creation, management, storage, and distribution of content — all while complying with MPAA requirements. Azure Media Services, Storage, Virtual Networks, and more than 30 other services provide a content workflow engine in the cloud that is more secure and scalable than traditional on-premises production processes and more effective at protecting media assets downstream.

## Microsoft in-scope cloud services

- [Azure complies with MPAA best-practices guidelines](#)

## Audits, reports, and certificates

- [Azure MPAA common guidelines](#)
- [Azure MPAA application and cloud security guidelines](#)

## Frequently asked questions

### How can I get copies of Microsoft responses to the MPAA audit?

The [Service Trust Portal](#) provides access to Microsoft responses to the Common Guidelines and the Application and Cloud Security Guidelines. You can also review copies of the Azure ISO/IEC 27001 Audit Report and the CDSA CPS Audit Report and Statement of Applicability in the portal.

### Why is the MPAA important?

Content security is critical for feature film development, as there are multiple points along the workflow where digital assets could be compromised or stolen. Dailies, rough cuts, and visual effects are just some of the materials exposed during a normal production cycle, and the box-office impacts of a security breach on a

blockbuster project can reach tens of millions of dollars.

MPAA guidelines provide major studio vendors and partners with a set of best practices for creating, processing, storing, and distributing digital assets. Service providers such as Azure who undergo the formal assessment can provide an additional layer of assurance that content uploaded to the cloud will be managed in accordance with established industry requirements for encryption, authentication, access control, and resiliency, among others.

### **Does my organization still need to undergo an MPAA audit, or can we use the Azure audit?**

Production facilities, visual effects houses, and other service partners should work with their executive producers and directors to understand the new security requirements, and whether a formal MPAA audit is necessary. Compliance with MPAA guidelines is voluntary, but Microsoft elected to carry out an independent assessment so that media customers can be confident in the content security and protection capabilities of Azure. However, Azure does not manage the individual cloud environments of customers, which may be subject to additional MPAA regulation that is best addressed by your own audit of your environment.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Motion Picture Association of America](#)
- [MPAA Common Guidelines](#)
- [MPAA Application and Cloud Guidelines](#)
- [CSA STAR Azure Self-Assessment](#)
- [Azure Responses to CSA CAIQ v3.0.1](#)
- [Compliance on the Microsoft Trust Center](#)



# Title 23 NYCRR Part 500

2/5/2021 • 4 minutes to read • [Edit Online](#)

## Title 23 NYCRR Part 500 overview

In response to the significant and ever-increasing threats to the cybersecurity of information and financial systems, in 2017, the State of New York Department of Financial Services imposed a new set of cybersecurity requirements on financial institutions that are licensed or authorized to do business in the state. This regulation — Title 23 New York Codes, Rules, and Regulation Part 500: Cybersecurity Requirements for Financial Services Companies — is designed to protect customer data and the information technology systems of financial institutions such as state-chartered, private, and international banks, mortgage brokers, and insurance companies.

## Microsoft and Title 23 NYCRR Part 500

Microsoft provides a comprehensive guide, [Microsoft Cloud Services: Supporting Compliance with NYDFS Cybersecurity Requirements](#), for financial services regulated under Title 23 NYCRR Part 500. It explains in depth how Azure, Office 365, and Power BI cloud services support compliance with the requirements. Financial institutions that seek to operate in the global financial center of New York must meet them, so compliance is critical for many institutions.

Follow this guidance to accelerate your compliance with Title 23 NYCRR Part 500: [Microsoft Cloud Services: Supporting Compliance with NYDFS Cybersecurity Requirements](#)

The New York regulations require each financial institution to:

- **Develop and maintain a robust cybersecurity program** starting with an assessment of the institution's specific risk profile and then designing a program that addresses them. The [Microsoft Cloud Financial Services Compliance Program](#) was created to help financial services assess the risks of using Microsoft cloud services. It includes direct engagement with our engineers and corporate risk officers and access to our compliance and security experts.
- **Implement a comprehensive cybersecurity policy** that addresses information security, data governance and classification, access controls, business continuity, and the like. Microsoft offers guidance for developing this policy with in-depth information about our certifications and risk assessments; business continuity and disaster recovery metrics; and diagnostics for logging and auditing.
- **Designate a chief information security officer (CISO)** to manage the cybersecurity program and enforce policy. To help your CISO, Microsoft provides in-depth cybersecurity information about Microsoft cloud deployments through [Azure Security Center](#), [Office 365 Advanced Threat Analytics](#), and [Power BI Security](#).
- **Monitor and test the effectiveness of its cybersecurity program:** Microsoft provides information from audits of its cybersecurity practices that include continuous monitoring, periodic penetration testing, and vulnerability assessments. Customers can conduct their own tests without advance permission from Microsoft.
- **Maintain an audit trail.** Built-in audit functionalities of Azure, Office 365, and Power BI customers generate information that can be used to reconstruct financial transactions and develop audit trail information.
- **Limit access to information systems that contain nonpublic information:** Measures that Azure, Office 365, and Power BI offer a role-based access control (RBAC) process native to each service, strict security and access requirements for every Microsoft administrator, and audits of every request for elevated access privileges.

- **Institute procedures to assess and test the security of externally developed applications:** For developers using Visual Studio, [Security Rules](#) for managed code can help ensure that application cybersecurity threats are detected and mitigated before the code is deployed.
- **Use periodic risk assessments to design and enhance cybersecurity programs:** For customers, Microsoft aggregates information about security threats, provides roadmaps of change management, and regularly updates information about subcontractors. Microsoft also regularly conducts risk assessments of its own services, the results of which are available to customers.
- **Use qualified personnel to manage cybersecurity risks and oversee cybersecurity functions:** Microsoft employs stringent procedures for our employee access to your customer data. If we hire subcontractors, we remain responsible for service delivery, and ensure that subcontractors fully comply with Microsoft privacy and security commitments, including requirements for handling sensitive data, background checks, and non-disclosure agreements.
- **Implement policies and procedures to ensure the security of information held by third-party service providers:** Azure, Office 365, and Power BI make multi-factor authentication available for all inbound connections to company networks; implement controls, including encryption, to protect nonpublic information in transit over external networks and at rest; and offer [Microsoft Online Services Terms](#) that provide for customer notification, incident investigation, and risk mitigation for security incidents.
- **Implement data retention and deletion policies and procedures:** You can always access and extract your customer data stored in Azure, Office 365, and Power BI.
- **Monitor the activity of authorized users, detect unauthorized access, and offer regular cybersecurity awareness training to employees:** Azure, Office 365, and Power BI include outside-in monitoring to raise alerts about incidents, and extensive diagnostics for logging and auditing. [Microsoft Virtual Academy](#) offers online training that covers the cybersecurity of Microsoft cloud services.
- **Develop plans to respond to and recover from cybersecurity incidents:** Microsoft helps you prepare for cybersecurity incidents using a defensive strategy to detect, predict, and prevent security breaches before they occur. When developing your own plans, you can draw on our incident management plan for responding to cybersecurity breaches.

## Microsoft in-scope cloud services

- [Azure](#)
- Intune
- [Office 365](#)
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Frequently asked questions

### What institutions are covered under this regulation?

Consult the New York Department of Financial Services [Who We Supervise](#) to determine whether your institution is governed by this regulation.

## Resources

- [Featured resources](#)
- [New York State Department of Financial Services 23 NYCRR 500: Cybersecurity Requirements For Financial Services Companies](#)
- [FAQs: 23 NYCRR Part 500–Cybersecurity](#)
- [Microsoft Cloud Services: Supporting Compliance with NYDFS Cybersecurity Requirements](#)
- [Compliance on the Microsoft Trust Center](#)

## Other Microsoft resources for financial services

- [Microsoft business cloud services and financial services](#)
- [Microsoft Cloud Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Shared responsibilities for cloud computing-](#)

# Dutch Authority for the Financial Markets and the Central Bank of the Netherlands

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the AFM and DNB

The primary financial regulators in the Netherlands are the [Dutch Authority for the Financial Markets \(Autoriteit Financiële Markten, AFM\)](#) and the [Central Bank of the Netherlands \(De Nederlandsche Bank, DNB\)](#). The AFM, whose role is comparable to the SEC in the United States, is the independent supervisory authority for the savings, lending, investment, and insurance markets.” The DNB, within the European System of Central Banks, determines, and implements monetary policy and exercises prudential supervision of financial organizations for the Netherlands.

Both of these institutions act in concert with the European Banking Authority (EBA), “an independent EU authority that works to ensure effective and consistent prudential regulation and supervision across the European banking sector.” To that end, the EBA has outlined a comprehensive approach to the use of cloud computing by financial institutions in the EU, [Recommendations on outsourcing to cloud services providers](#).

In general, the laws and guidelines support the point of view that cloud computing involving third-party services qualifies as a form of outsourcing, and financial institutions in the Netherlands must address the associated risks before moving business activities to the cloud. These include:

- The Financial Supervision Act (FSA) ([Dutch](#) and [English](#)), issued by the Dutch legislature in 2018, attaches conditions for financial institutions to control the risks associated with outsourcing and ensure that it doesn't impede regulatory supervision.
- The Circulaire Cloud Computing ([Dutch](#) and [English](#)), issued by the DNB, requires that before supervised Dutch institutions engage in cloud computing, they must inform the DNB of their prospective outsourcing arrangements to ensure that operational processes and risks are under control.

Using a template that the DNB provides, they must submit a mandatory risk analysis that includes:

- An assessment regarding: compliance with current legislation, mutual understanding between the parties regarding the services offered, the stability and reliability of the service provider, where the services are to be provided, and the importance of and degree of reliance on the outsourced services.
- Explicit attention to addressing risks associated with data integrity, confidentiality, and availability.

The [Commission Delegated Regulation EU 2017/565](#) describes at great length the requirements for an outsourcing agreement between investment firms and cloud service providers.

## Microsoft and the AFM and DNB

To help guide financial institutions in the Netherlands considering outsourcing business functions to the cloud, Microsoft has published [a compliance checklist for financial institutions in the Netherlands](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When financial institutions in the Netherlands outsource business activities to the cloud, they must comply with the rules and guidelines of the Dutch Authority for Financial Markets (AFM) and the Central Bank of the Netherlands (DNB) within the broad policy framework of the European Banking Authority (EBA).

The Microsoft checklist helps financial firms in the Netherlands conducting due-diligence assessments of

Microsoft business cloud services and includes:

- An overview of the regulatory landscape for context.
- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Compliance checklist: Netherlands](#): Financial firms can get help when conducting risk assessments of Microsoft business cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Case overviews, tutorials, and other resources to build Azure solutions for financial services.

## Frequently asked questions

### Is regulatory approval required?

No. However, the Circulaire Cloud Computing states that the DNB expects supervised Dutch institutions to submit a risk analysis concerning prospective outsourcing arrangements before engaging in cloud computing.

### Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. The provisions and arrangements to be included in cloud contracts depend on the type of financial institution. Requirements, such as those described in Art. 31 of the Commission Delegated Regulation (EU) 2017/565, are set out in Part 2 of the checklist.

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Compliance on the Microsoft Trust Center](#)

# Financial Authority (AMF) and Prudential Authority (ACPR) France

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the AMF and ACPR

The [Financial Authority \(Autorité des Marchés Financiers, AMF\)](#) and the [Prudential Authority \(Autorité de Contrôle Prudentiel et de Résolution, ACPR\)](#) are the primary financial regulators in France. In its capacity as the stock market regulator, the AMF is responsible for the supervision of financial markets and investment firms. The ACPR, an independent administrative authority under the central bank, the [Banque de France](#), supervises the banking and insurance sectors.

The AMF and ACPR act in concert with the European Banking Authority (EBA), “an independent EU authority, which works to ensure effective and consistent prudential regulation and supervision across the European banking sector.” To that end, the EBA has outlined a comprehensive approach to the use of cloud computing by financial institutions in the EU, [Recommendations on outsourcing to cloud services providers](#).

There are several requirements and guidelines that financial institutions in France should be aware of when moving operational functions to the cloud:

- The AMF General Regulation ([French](#) and [English](#)) sets rules and procedures to enforce financial legislation. In particular, Article 313-75 sets forth conditions that must be reflected in contracts that financial institutions enter into with cloud service providers.
- ACPR published [The risks associated with cloud computing \(French and English\)](#), which encourages organizations under ACPR supervision to take suitable measures to manage risk when they outsource business functions to the cloud. In addition, [Article 239 in the ACPR Order of 3 November 2014 on the internal control of companies \(French\)](#) under ACPR supervision also specifies mandatory terms to be included in contracts with cloud service providers.
- In certain cases, regulated institutions must notify the AMF and ACPR regarding material outsourcing arrangements, particularly if they have the potential to significantly impact their business operations.
- In its role as the data protection authority for France, the [CNIL](#) (Commission Nationale de l’Informatique et des Libertés) has issued many cloud computing guidelines, including [Recommendations for companies planning to use cloud computing services \(French and English\)](#).

## Microsoft and the AMF and ACPR

To help guide financial institutions in France considering outsourcing business functions to the cloud, Microsoft has published [Navigating your way to the cloud: a checklist for financial institutions in France](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When financial institutions in France outsource business activities to the cloud, they must comply with the requirements of the Financial Authority (AMF) and Prudential Authority (ACPR) of France within the broad policy framework of the European Banking Authority (EBA). In particular, they must be aware of Article 313-75 of the AMF General Regulation, and the ACPR guidelines on cloud computing risks and its mandatory requirements for contracts with cloud service providers.

The Microsoft checklist helps French financial firms conducting due-diligence assessments of Microsoft business cloud services and includes:

- An overview of the regulatory landscape for context.
- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Compliance checklist: France](#): Financial firms can get help conducting risk assessments of Microsoft business cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Use-case overviews, tutorials, and other resources to build Azure solutions for financial services.

## Frequently asked questions

### Is regulatory approval required?

The EBA publication, [Recommendations on outsourcing to cloud services providers] (<https://eba.europa.eu/sites/default/documents/files/documents/10180/1848359/c1005743-567e-40fc-a995-d05fb93df5d1/Draft%20Recommendation%20on%20outsourcing%20to%20Cloud%20Service%20%20%28EBA-CP-2017-06%29.pdf> /5fa5cdde-3219-4e95-946d-0c0d05494362), outlines a comprehensive approach to material outsourcing by financial institutions in the EU. Also, in certain instances, financial firms must notify the AMF or ACPR of their outsourcing arrangements, as described on pages 8 and 9 of the [checklist](#). While it is unlikely these circumstances would apply to the use of Microsoft cloud services, financial services should verify their applicability by reviewing the checklist.

### Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. Article 239 of the [ACPR Order of 3 November 2014](#) and Article 313-75 of the [AMF General Regulation](#) set forth conditions that must be reflected in contracts that financial institutions enter into with cloud service providers. Part 2 of the Microsoft [checklist](#) (page 62) maps these against the sections in Microsoft contractual documents where they are addressed.

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Compliance on the Microsoft Trust Center](#)

# Content Delivery & Security Association (CDSA) Content Protection & Security (CPS) Standard

2/5/2021 • 3 minutes to read • [Edit Online](#)

## CDSA overview

The Content Delivery & Security Association (CDSA) is a worldwide forum advocating for the innovative and responsible delivery and storage of entertainment, software, and information content.

The CDSA [Content Protection & Security \(CPS\) Standard](#) provides guidance and requirements for securing media assets within a Content Security Management System (CSMS). The standard specifies a set of controls designed to ensure the integrity of intellectual property and the confidentiality and security of media assets at every stage of the digital media supply chain.

The CPS certification audit is administered directly by the CDSA and consists of over 300 distinct controls that help secure and manage physical datacenters, harden services, and protect storage facilities. All controls are optimized to handle sensitive and valuable media assets. Once a system is validated by the CDSA assessor, the CDSA issues a certificate of compliance. To maintain compliance, the certified entity must submit the results of annual audits to the CDSA.

## Microsoft and CDSA — CPS Standard

The Microsoft Azure Media Services CSMS has been validated by the CDSA, awarding Azure Media Services certification to this standard. Microsoft demonstrated a proof of risk assessment against the CPS standard requirements. We also filed a comprehensive Statement of Applicability that articulated the content protection features of Azure Media Services. Microsoft is committed to continuing the annual CDSA audits, and maintaining the internal audits and controls necessary to retain CPS certification.

The CPS certification provides a standards-based method of assuring our customers and yours that the intellectual property rights of media assets stored, managed, and distributed from within Azure are protected. Furthermore, you can use Azure CPS certification toward your own CPS certification efforts.

Azure Media Services was the first hyperscale cloud media platform to offer encryption on the fly for both Video On Demand and live-streaming broadcasts. Azure Media Services provides several security-enhanced upload channels for content, including the ExpressRoute private network connection to Azure, UDP upload via the Aspera client, and HTTPS upload over the Internet.

- Learn about the benefits of CDSA on the Microsoft Cloud: [Learn how the CDSA transforms movie-making in the cloud with Microsoft Azure](#)
- Learn how to accelerate your CDSA deployment with our Azure Security and Compliance Blueprints: [Download the Microsoft Azure — Implementing CDSA-Compliant Content Protection and Security guide](#)

## Microsoft in-scope cloud services

- [Azure Media Services](#)

## Audits, reports, and certificates

Microsoft has successfully completed the six-month renewal of the CDSA CPS certification, and Azure is now on an annual audit cycle.



- [Azure Media Services Certificate of Compliance](#)
- [Azure CDSA CPS Audit Report](#)
- [Azure CDSA implementation guide](#)

## Frequently asked questions

### To whom does the standard apply?

The standard applies to any provider that wants to provide cloud services to the media production industry.

### How do I start my organization's compliance effort?

For guidance, refer to the [CDSA Azure implementation guide](#). To discuss specific requirements and the application process for CPS Standard Certification Program, please [contact the CDSA](#).

### Can I use Microsoft compliance in my organization's certification process?

Yes. You can build on Azure CPS certification within your own CPS certification effort by using the security and encryption features in Azure.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [CDSA](#)
- [CPS Standard](#)
- [Azure Media Services Certificate of Compliance](#)
- [How Azure Media Services earned CDSA security certification](#)
- [Compliance on the Microsoft Trust Center](#)
- [Understanding CDSA and Azure compliance](#)

# Center for Internet Security (CIS) Benchmarks

2/5/2021 • 4 minutes to read • [Edit Online](#)

## About CIS Benchmarks

The [Center for Internet Security](#) is a nonprofit entity whose mission is to 'identify, develop, validate, promote, and sustain best practice solutions for cyberdefense.' It draws on the expertise of cybersecurity and IT professionals from government, business, and academia from around the world. To develop standards and best practices, including CIS benchmarks, controls, and hardened images, they follow a consensus decision-making model.

[CIS benchmarks](#) are configuration baselines and best practices for securely configuring a system. Each of the guidance recommendations references one or more [CIS controls](#) that were developed to help organizations improve their cyberdefense capabilities. CIS controls map to many established standards and regulatory frameworks, including the NIST Cybersecurity Framework (CSF) and NIST SP 800-53, the ISO 27000 series of standards, PCI DSS, HIPAA, and others.

Each benchmark undergoes two phases of consensus review. The first occurs during initial development when experts convene to discuss, create, and test working drafts until they reach consensus on the benchmark. During the second phase, after the benchmark has been published, the consensus team reviews the feedback from the internet community for incorporation into the benchmark.

CIS benchmarks provide two levels of security settings:

- **Level 1** recommends essential basic security requirements that can be configured on any system and should cause little or no interruption of service or reduced functionality.
- **Level 2** recommends security settings for environments requiring greater security that could result in some reduced functionality.

[CIS Hardened Images](#) are securely configured virtual machine images based on CIS Benchmarks hardened to either a Level 1 or Level 2 CIS benchmark profile. Hardening is a process that helps protect against unauthorized access, denial of service, and other cyberthreats by limiting potential weaknesses that make systems vulnerable to cyberattacks.

## Microsoft and the CIS Benchmarks

The Center for Internet Security (CIS) has published benchmarks for Microsoft products and services including the Microsoft Azure and Microsoft 365 Foundations Benchmarks, the Windows 10 Benchmark, and the Windows Server 2016 Benchmark.

CIS benchmarks are internationally recognized as security standards for defending IT systems and data against cyberattacks. Used by thousands of businesses, they offer prescriptive guidance for establishing a secure baseline configuration. System and application administrators, security specialists, and others who develop solutions using Microsoft products and services can use these best practices to assess and improve the security of their applications.

Like all CIS benchmarks, the Microsoft benchmarks were created using a consensus review process based on input from subject matter experts with diverse backgrounds spanning software development, audit and compliance, security research, operations, government, and law. Microsoft was an integral partner in these CIS efforts. For example, Office 365 was tested against the listed services, and the resulting Microsoft 365 Foundations Benchmark covers a broad range of recommendations for setting appropriate security policies that cover account and authentication, data management, application permissions, storage, and other security policy

areas.

In addition to the benchmarks for Microsoft products and services, CIS has also published [CIS Hardened Images for use on Azure virtual machines](#) configured to meet CIS benchmarks. These include the CIS Hardened Image for Microsoft Windows Server 2016 certified to run on Azure. CIS states that, 'All CIS hardened images that are available on the [Azure Marketplace](#) are certified to run on Azure. They have been pre-tested for readiness and compatibility with the Azure public cloud, the Microsoft Cloud Platform hosted by service providers through the Cloud OS Network, and on-premise private cloud Windows Server Hyper-V deployments managed by customers.'

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- [Office and Microsoft 365](#)
- SQL Server
- Windows 10
- Windows Server 2016

## Audits, reports, and certificates

Get a [complete list of CIS benchmarks](#) for Microsoft products and services.

- [CIS Azure Foundations Benchmark](#)
- [CIS Microsoft 365 Foundations Benchmark](#)
- [Windows 10 Benchmark](#)
- [Windows Server 2016 Benchmark](#)

## How to implement

- [CIS Benchmark for Azure](#): Get prescriptive guidance for establishing a secure baseline configuration for Azure.
- [Microsoft 365 security roadmap](#): Minimize the potential of a data breach or compromised account by following this roadmap.
- [Windows security baselines](#): Follow these guidelines for effective use of security baselines in your organization.
- [CIS Controls Cloud Companion Guide](#): Get guidance on applying security best practices in CIS Controls Version 7 to cloud environments.

## Frequently asked questions

### Will following CIS Benchmark settings ensure the security of my applications?

CIS benchmarks establish the basic level of security for anyone adopting in-scope Microsoft products and services. However, they should not be considered as an exhaustive list of all possible security configurations and architecture but as a starting point. Each organization must still evaluate its specific situation, workloads, and compliance requirements and tailor its environment accordingly.

### How often are CIS Benchmarks updated?

The release of revised CIS Benchmarks changes depending on the community of IT professionals who developed it and on the release schedule of the technology the benchmark supports. CIS distributes monthly reports that announce new benchmarks and updates to existing benchmarks. To receive these, register for the [CIS Workbench](#) (it's free) and check Receive newsletter in your profile.

## Who contributed to the development of Microsoft CIS Benchmarks?

CIS notes that its 'Benchmarks are developed through the generous volunteer efforts of subject matter experts, technology vendors, public and private CIS Benchmark community members, and the CIS Benchmark Development team.' For example, you'll find a list of Azure contributors on [CIS Microsoft Azure Foundations Benchmark v1.0.0 Now Available](#).

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [CIS best practices for securely using Microsoft 365](#)
- [Windows 10 security policy settings](#)
- [Windows 10 enterprise security](#)
- [Compliance on the Microsoft Trust Center](#)

# Cloud Security Alliance (CSA) STAR attestation

2/17/2021 • 3 minutes to read • [Edit Online](#)

## CSA STAR attestation overview

The Cloud Security Alliance (CSA) maintains the Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry where cloud service providers (CSPs) can publish their CSA-related assessments. STAR consists of three levels of assurance aligned with control objectives in the CSA Cloud Controls Matrix (CCM). (The CCM covers fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a cloud service.):

- Level 1: STAR Self-Assessment
- Level 2: STAR Attestation, STAR Certification, and C-STAR Assessment (which are based on audits by third parties)
- Level 3: STAR Continuous Monitoring (program requirements are still under development by CSA)

STAR Attestation involves a rigorous independent audit of a cloud provider's security posture based on a SOC 2 Type 2 audit with CCM criteria. The independent auditor that evaluates a cloud provider's offerings for STAR Attestation must be a certified public accountant (CPA) and is required to have the CSA Certificate in Cloud Security Knowledge (CCSK).

A SOC 2 Type 2 audit is based on American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria, including security, availability, confidentiality, and processing integrity, and the criteria in the CCM. STAR Attestation provides an auditor's findings on the design suitability and operating effectiveness of SOC 2 controls in Microsoft cloud services. The objective is to meet both the AICPA criteria mentioned above and requirements set forth in the CCM.

## Microsoft in-scope cloud services

Microsoft Azure and Microsoft Intune have been awarded CSA STAR Attestation. STAR Attestation provides an auditor's findings on the design suitability and operating effectiveness of SOC 2 controls in Microsoft cloud services.

- [Azure and Azure Government](#)
- [Azure Germany](#)
- Microsoft Cloud App Security
- Microsoft Graph
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI

## Audits, reports, and certificates

- [CSA STAR Attestation and Certification](#)

# Frequently asked questions

## Which industry standards does the CSA CCM align with?

The CCM corresponds to industry-accepted security standards, regulations, and control frameworks such as ISO/IEC 27001, PCI DSS, HIPAA, AICPA SOC 2, NERC CIP, FedRAMP, NIST, and many more. For the most current list, visit the [CSA website](#).

## Where can I see the CSA STAR Attestation for Microsoft cloud services?

You can download the [CSA STAR Attestation](#) for Azure, which also covers Intune, from the CSA Registry.

## Which CSA STAR levels of assurance have Microsoft business cloud services attained?

- **Level 1: CSA STAR Self-Assessment:** Azure, Microsoft Dynamics 365, and Microsoft Office 365. The [Self-Assessment](#) is a complimentary offering from cloud service providers to document their security controls to help customers assess the security of the service.
- **Level 2: CSA STAR Certification:** Azure, Microsoft Cloud App Security, Intune, and Microsoft Power BI. STAR Certification is based on achieving ISO/IEC 27001 certification and meeting criteria specified in the CCM. It is awarded after a rigorous third-party assessment of the security controls and practices of a cloud service provider.
- **Level 2: CSA STAR Attestation:** Azure and Intune. CSA and the AICPA have collaborated to provide guidelines for CPAs to use in conducting SOC 2 engagements, using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA CCM. [STAR Attestation](#) is based on these guidelines and is awarded after rigorous independent assessments of cloud providers.

# Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Azure standard response for request for information](#)
- [Azure Cloud Security Alliance CAIQ](#)
- [Office 365 Mapping of CSA Cloud Control Matrix](#)
- [Cloud Security Alliance](#)
- [CSA Security, Trust & Assurance Registry \(STAR\)](#)
- [SOC 1, 2, and 3 Reports](#)
- [Cloud Controls Matrix \(CCM\)](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Compliance on the Microsoft Trust Center](#)

# US DoE 10 CFR Part 810

11/30/2020 • 2 minutes to read • [Edit Online](#)

## Microsoft and DoE 10 CFR Part 810

Microsoft Azure Government can help support customers subject to the export control requirements of US Department of Energy (DoE) 10 CFR Part 810 through two authorizations:

- The FedRAMP High Provisional Authorization to Operate (P-ATO) issued by the Joint Authorization Board (JAB)
- The Level 4 and 5 Provisional Authorizations from the Department of Defense (DoD) Defense Information Systems Agency

FedRAMP offers an appropriate baseline to provide assurances that Azure Government delivers core infrastructure and virtualization technologies and services such as compute, storage, and networking that are designed with stringent NIST controls. These help meet customer data separation requirements and help enable secure connections to customers' on-premises environments.

Furthermore, Azure Government is a US government community cloud that is physically separated from the Azure cloud. It provides additional assurances regarding specific background screening requirements by the US government, including specific controls that restrict access to information and systems to screened US citizens among Azure operations personnel.

## Microsoft in-scope cloud services

- [Azure Government](#)
- Intune

## How to implement

- [NERC CIP Standards & Cloud Computing](#): Guidance for electric utilities and Registered Entities deploying workloads on Azure or Azure Government.

## About DoE 10 CFR Part 810

The US Department of Energy (DoE) export control regulation [10 CFR Part 810](#) governs the export of unclassified nuclear technology and assistance. It helps ensure that nuclear technologies exported from the United States will be used only for peaceful purposes. The revised Part 810 (Final Rule) took effect in March 2015 and is administered by the [National Nuclear Security Administration](#). Section 810.6 states that specific DoE authorization is required for both provisions of assistance and transfers of sensitive nuclear technology that are "generally authorized," as well as those requiring specific authorization (such as for assistance involving sensitive nuclear technologies like enrichment and heavy water production).

## Frequently asked questions

**Do the 10 CFR Part 110 regulations of the US Nuclear Regulatory Commission apply to Azure Government?**

No. The [US Nuclear Regulatory Commission](#) (NRC) regulates the [export and import](#) of nuclear facilities and related equipment and materials under [10 CFR Part 110](#). The NRC does not regulate nuclear technology and assistance related to these items that fall under DoE jurisdiction. Therefore, NRC 10 CFR Part 110 regulations

would not apply to Azure Government.

### **How can I supply evidence that I am complying with DoE 10 CFR Part 810?**

If your organization is deploying data to Azure Government, you can rely on the Azure Government FedRAMP High P-ATO as evidence that you are handling data in an appropriately restricted manner. However, you are responsible for getting DoE authorization of your own systems, including the use of cloud services.

### **What are my responsibilities for classifying data deployed to Azure Government?**

Customers deploying data to Azure Government are responsible for their own security classification process. For customer data subject to DoE export controls, the classification system is augmented by the Unclassified Controlled Nuclear Information (UCNI) controls established by Section 148 of the [US Atomic Energy Act](#).

## Resources

- [Azure Cloud Services and US Export Controls](#)
- [Microsoft and FedRAMP](#)
- [Microsoft and DoD](#)
- [Microsoft Government Cloud](#)
- [Compliance on the Microsoft Trust Center](#)



# Digital Production Partnership (DPP) United Kingdom

2/5/2021 • 2 minutes to read • [Edit Online](#)

## About the DPP

Broadcasters are confronting increasingly frequent cyber-attacks against their websites, IT infrastructure, and systems. In response to these threats, the [Digital Production Partnership](#) (DPP) partnered with the [North American Broadcasters Association](#) (NABA) to develop the [Broadcasters Cyber Security Requirements for Suppliers](#). Chief information security officers from UK broadcasters have endorsed these as the minimum cybersecurity requirements.

The DPP then worked with broadcasters and supplier security experts to create a self-assessment inventory, the [Committed to Security Program Broadcast Checklist](#), which enables suppliers to demonstrate to broadcasters their deployment of cybersecurity best practices. This work led to establishing a formal [DPP Committed to Security Program](#) launched in October 2017, with two different marks: one for Broadcast and one for Production.

## Microsoft and the DPP

Microsoft Azure has been awarded the DPP Committed to Security Mark for Broadcast after completing the Digital Production Partnership (DPP) self-assessment questionnaire, the *Committed to Security Program Broadcast Checklist*. It required documenting a set of best practices for documentation and testing, authentication, and security controls. [Eurofins Digital Testing](#), a quality assurance expert and DPP member, reviewed and signed off on the Microsoft response and submitted it to the DPP for final validation.

This support means that broadcasters and other media customers using Azure can have confidence that its robust security and resilient service can help meet the unique demands of the broadcast industry, from program development to transmission.

## Microsoft in-scope cloud services

- [Azure](#)

## Audits, reports, and certificates

The Azure Broadcast mark is valid for one year and renewed annually.

- [Azure NABA DPP Broadcaster Security Requirements Checklist](#)
- [DPP Committed to Security Companies Awarded the Marks](#)

## How to implement

- [Asset Management Hardening Guide](#): Best practices in Azure protect pre-release content from unauthorized disclosure, change, or deletion.
- [Azure Media Services](#): Build solutions that achieve high-definition video encoding and broadcast-quality video streaming.

## Resources

- [DPP Committed to Security Program Broadcast Checklist User Guide](#)
- [NABA and DPP Broadcasters Unite to Promote Cyber Security Requirements for Suppliers](#)
- [Compliance on the Microsoft Trust Center](#)

# US Export Administration Regulations (EAR)

2/5/2021 • 5 minutes to read • [Edit Online](#)

## About the EAR

The US Department of Commerce enforces the Export Administration Regulations (EAR) through the [Bureau of Industry and Security \(BIS\)](#). The EAR broadly governs and imposes controls on the export and re-export of most commercial goods, software, and technology, including “dual-use” items that can be used both for commercial and military purposes and certain defense items.

BIS guidance holds that, when data or software is uploaded to the cloud or transferred between user nodes, the customer, not the cloud provider, is the “exporter” who has the responsibility to ensure that transfers of, storage of, and access to that data or software complies with the EAR.

According to the BIS, *export* refers to the transfer of protected technology or technical data to a foreign destination or its release to a foreign person in the United States (also referred to as a *deemed export*). The EAR broadly governs:

- Exports from the United States.
- Re-exports or retransfers of US-origin items and certain foreign-origin items with more than a *de minimis* portion of US-origin content.
- Transfers or disclosures to persons from other countries.

Items subject to the EAR can be found on the Commerce Control List (CCL) where each item is assigned a unique [Export Control Classification Number \(ECCN\)](#). Items not listed on the CCL are designated as EAR99 and most EAR99 commercial products will not require a license to be exported. However, depending on the destination, end user, or end use of the item, even an EAR99 item may require a BIS export license.

The [final rule](#), published in June 2016, clarified that EAR licensing requirements also would not apply to the transmission and storage of unclassified technical data and software if they were encrypted end-to-end using FIPS 140-2 validated cryptographic modules and were not intentionally stored in a military-embargoed country or in the Russian Federation.

## Microsoft and the EAR

Microsoft technologies, products, and services are subject to the US Export Administration Regulations (EAR). While there is no compliance certification for the EAR, Microsoft Azure, Microsoft Azure Government, and Microsoft Office 365 Government (GCCHigh and DoD environments) offer important features and tools to help eligible customers subject to the EAR manage export control risks and meet their compliance requirements.

The US Commerce Department, which enforces the EAR, has taken the position that customers, not cloud service providers such as Microsoft, are considered to be exporters of their own customer data. While most customer data is not considered “technology” or “technical data” subject to EAR export controls, Microsoft in-scope cloud services are structured to help customers manage and significantly mitigate the potential export control risks they face. Microsoft generally, but not exclusively, recommends the use of its government cloud services for eligible customers. With appropriate planning, customers can use the following tools and their own internal procedures to help ensure full compliance with US export controls.

- **Controls on data location.** Customers have visibility into where their data is stored and access to robust tools to restrict its storage. They may therefore ensure that their data is stored in the United States and minimize transfer of controlled technology or technical data outside the United States. Furthermore, customer data is not stored in a non-conforming location, consistent with EAR prohibitions on where data is

“intentionally stored”: no Azure datacenter is located in any of the 25 Group D:5 countries or the Russian Federation.

- **End-to-end encryption.** By taking advantage of the end-to-end encryption safe harbor for physical storage locations specified in the EAR, Microsoft in-scope cloud services deliver encryption features that can help protect against export control risks. They also offer customers a [wide range of options for encrypting data](#) in transit and at rest, and the flexibility to choose among encryption options.
- **Tools and protocols to prevent unauthorized deemed export.** The use of encryption also helps protect against a potential deemed export (or deemed re-export) under the EAR, because even if a non-US person has access to encrypted data, nothing is revealed if they cannot read or understand the data while it is encrypted; thus there is no “release” of controlled data.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- [Office 365 Government \(GCC-High and DoD\)](#)
- Intune

## How to implement

Overview of US export controls and guidance for customers assessing their obligations under the EAR.

- [Azure](#)
- [Office 365](#)

## Frequently asked questions

### What should I do to comply with export controls when using Microsoft cloud services?

Under the EAR, when data is uploaded to a cloud server such as the Microsoft cloud, the customer who owns the data — not the cloud services provider — is considered to be the exporter. For that reason, the owner of the data — that is, the Microsoft customer — must carefully assess how their use of the Microsoft cloud may implicate US export controls and determine whether any of the data they want to use or store there may be subject to EAR controls, and if so, what controls apply. Learn more about how [Azure](#) and [Office 365](#) cloud services can help customers ensure their full compliance with US export controls.

### Are Microsoft technologies, products, and services subject to the EAR?

Most Microsoft technologies, products, and services either:

- Are not subject to the EAR and thus are not on the Commerce Control List and have no ECCN;
- Or they are EAR99 or 5D992 Mass Market-eligible for self-classification by Microsoft and may be exported to non-embargoed countries without a license as No License Required (NLR).

That said, a few Microsoft products have been assigned an ECCN that may or may not require a license. Consult the EAR or legal counsel to determine the appropriate license type and eligible countries for export purposes.

### What’s the difference between the EAR and International Traffic in Arms Regulations (ITAR)?

The primary US export controls with the broadest application are the EAR, administered by the US Department of Commerce. The EAR is applicable to dual-use items that have both commercial and military applications, and to items with purely commercial applications.

The United States also has separate and more specialized export control regulations, such as the ITAR, that governs the most sensitive items and technology. Administered by the US Department of State, they impose controls on the export, temporary import, re-export, and transfer of many military, defense, and intelligence items (also known as “defense articles”), including related technical data.

## Resources

- [Exporting Microsoft Products: Overview](#)
- [Exporting Microsoft Products: FAQ](#)
- [Exporting Microsoft Products: Product Lookup](#)
- [Export restrictions on cryptography](#)
- [Microsoft and FIPS 140-2](#)
- [Microsoft and ITAR](#)
- [Compliance on the Microsoft Trust Center](#)

# ENISA Information Assurance Framework

11/30/2020 • 2 minutes to read • [Edit Online](#)

## About the ENISA Information Assurance Framework

The [European Network and Information Security Agency](#) (ENISA) is a center of network and information expertise. It works closely with EU member states and the private sector to provide advice and recommendations on good cybersecurity practices. ENISA also supports the development and implementation of EU policy and law relating to national information security.

The [Information Assurance Framework](#) (IAF) is a set of assurance criteria that organizations can review with cloud service providers to ensure that they sufficiently protect customer data. The IAF is intended to help organizations assess the risk of adopting cloud services, better compare the offers from different cloud services, and reduce the assurance burden on cloud service providers.

## Microsoft and the ENISA IAF

The ENISA Information Assurance Framework is based on the broad classes of controls from ISO/IEC 27001, the international information security management standard, and the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v3.0.1. The CCM is a controls framework covering fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a cloud service provider (CSP).

For the CSA STAR self-assessment, Microsoft submitted a report documenting Microsoft Azure compliance with the CSA CCM. (Microsoft also publishes a completed Consensus Assessments Initiative Questionnaire (CAIQ) for Azure.) That self-assessment of compliance aligns it with the ENISA IAF.

Azure compliance is listed on the CSA STAR Registry, a free publicly accessible registry where CSPs publish their CSA-related assessments. There, Azure also maintains a formal CSA STAR Certification and CSA STAR Attestation.

Because these self-assessment reports are publicly available, Azure customers gain visibility into Microsoft security practices and can compare various CSPs using the same baseline.

## Microsoft in-scope cloud services

- [Azure](#)

## Audits, reports, and certificates

Microsoft attests to Azure compliance with the CSA CCM framework based on self-assessment, aligning services with the ENISA IAF.

- [CSA STAR Registry](#)

## Resources

- [Azure standard response for request for information](#)
- [Microsoft and the CSA STAR Self-Assessment](#)

- [Microsoft and ISO/IEC 27001](#)

# European Union Model Clauses

11/30/2020 • 4 minutes to read • [Edit Online](#)

## European Union Model Clauses overview

European Union (EU) data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA), which includes all EU countries and Iceland, Liechtenstein, and Norway. The EU Model Clauses are standardized contractual clauses used in agreements between service providers (such as Microsoft) and their customers to ensure that any personal data leaving the EEA will be transferred in compliance with EU data-protection law and meet the requirements of the EU Data Protection Directive 95/46/EC.

On a practical level, compliance with EU data protection laws also means that customers need fewer approvals from individual authorities to transfer personal data outside of the EU, since most EU member states do not require additional authorization if the transfer is based on an agreement that complies with the Model Clauses.

## Microsoft and European Union Model Clauses

Microsoft has invested in the operational processes necessary to meet the exacting requirements of the Model Clauses for the transfer of personal data to processors. Microsoft offers customers Model Clauses, referred to as Standard Contractual Clauses, that make specific guarantees around transfers of personal data for in-scope Microsoft services. This ensures that Microsoft customers can freely move data through the Microsoft cloud from the EEA to the rest of the world.

However, Microsoft enterprise customers, who are the controllers of the personal data, carry the primary obligation to protect that data. This means that EEA enterprise customers have a strong interest in ensuring that their service provider abides by EU data protection laws, or the customer can face liability — and even blockage of its ability to use a service.

Microsoft provided its Standard Contractual Clauses to the EU's Article 29 Working Party for review and approval. The Article 29 Working Party includes representatives from the European Data Protection Supervisor, the European Commission, and each of the 28 EU data protection authorities (DPAs).

The group determined that implementation of the provisions in Microsoft agreements was in line with their stringent requirements. (Microsoft was the first cloud service provider to receive a letter of endorsement and approval from the group.) Approval covered the engagements reflected in Model Clauses 2010/87/EU but not in the appendices, which describe the transfers of data and the security measures implemented by the data importer. The appendices may be analyzed separately by the DPA.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Microsoft Cloud App Security
- Microsoft Professional Services: Premier and On Premises for Azure, Dynamics 365, Intune, and for Medium Business and Enterprise customers of Microsoft 365 for business
- [Dynamics 365](#)
- Intune: Cloud service portion of the Intune Add-on Product and Mobile Device Management for Office 365
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- [Office 365](#)



- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- Azure DevOps Services
- Windows Defender Advanced Threat Protection for the following cloud service portions: Endpoint Detection & Response, Automatic Investigation & Remediation, Secure Score.

## Audits, reports, and certificates

Microsoft continually assesses the EU standards, and updates its services as needed.

## Frequently asked questions

### What is the EU Data Protection Directive 95/46/EC?

This directive sets the baseline for handling personal data in the EU. It provides the regulatory framework under which Microsoft transfers personal data out of the EU. Under this directive and our contractual agreements, Microsoft acts as the data processor of customer data. The customer acts as the data controller, with final ownership and responsibility for ensuring that the data can be legally provided to Microsoft for processing outside of the EEA.

### Why is compliance with the Model Clauses important?

A service provider that commits contractually to the Model Clauses gives its customers assurance that personal data will be transferred and processed in compliance with EU data protection law. Use of the Model Clauses also means that customers need to get fewer approvals from individual data-protection authorities to transfer personal data outside the EU.

### Where can I see compliance information for Microsoft services?

Compliance is a contractual commitment. Microsoft Standard Contractual Clauses are available to all cloud customers in the [Online Services Terms](#); for other services, see your existing agreement with Microsoft.

### What is a 'sub-processor'?

A sub-processor is someone who processes personal data following the data controller's instructions, and the terms of the EU Model Clauses and the subcontract. Microsoft customers—independent software vendors (ISVs), in particular — are sometimes themselves data processors. In those instances, Microsoft is the sub-processor.

### Where do I start with my own organization's compliance efforts?

You can enter an agreement such as the [Online Services Terms](#), or explore amending your existing agreement to incorporate the Standard Contractual Clauses.

## Resources

- [EU Standards Organization](#)
- [EU Model Clauses](#)
- [EU Data Protection Directive](#)
- [European Data Protection Board](#)
- [EU Model Clauses FAQ for Dynamics 365 and Office 365](#)
- [Microsoft and the EU-U.S. Privacy Shield](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

# European Banking Authority (EBA)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the EBA

The [European Banking Authority \(EBA\)](#) is 'an independent authority that works to ensure effective and consistent prudential regulation and supervision across the EU banking sector'. In December 2017, the EBA issued its [Final Report: Recommendations on outsourcing to cloud services providers](#), which outlined a comprehensive approach to the outsourcing of cloud computing by financial institutions in the EU. The recommendations clarify when outsourcing to the cloud is permitted, apply a principles-based approach towards measuring risk from a technology-neutral perspective, and strive towards greater harmonization within Europe and beyond.

The EBA recommendations took effect in July 2018, and they build on and add clarity to the general outsourcing guidelines published in 2006 by the Committee of European Banking Supervisors. In fact, the issuance of these recommendations comes after a consultation period during which Microsoft provided substantive feedback. Many of the final recommendations account for comments Microsoft provided to the EBA.

## Microsoft and the EBA

To help financial institutions in the EU follow the European Banking Authority (EBA) recommendations for cloud adoption, Microsoft published [European Banking Authority Guidance Addresses Cloud Computing for the First Time](#). This document addresses key requirements and explains how Microsoft Azure and Microsoft 365 can be used to satisfy them. The guidance can help financial institutions adopt Azure and Microsoft with the confidence that they can meet their obligations under the EBA framework.

The Microsoft guidance addresses, point by point, each of the EBA recommendations:

- **Audit rights.** Microsoft provides contractual audit rights for customers and rights of examination for regulators in its industry-leading Financial Services Amendment.
- **Notification regarding outsourcing.** Microsoft can assist customers with notifying regulators of material activities to be outsourced.
- **Data residency.** With 36 regions, including six in Europe, Microsoft offers the largest number of datacenters worldwide of any cloud service provider. Organizations can deploy workloads in one region without being required to host data in Europe.
- **Notification regarding subcontractors.** Microsoft leads the industry with a contractual commitment to provide customers with 180-day notice of new subcontractors, and a right to terminate if the customer does not approve of the appointment of a new subcontractor.
- **Business continuity.** Microsoft provides business continuity and resolution provisions in our Financial Services Amendment, including the willingness to provide transition assistance through Microsoft Consulting Services.
- **Risk assessment and security monitoring.** Microsoft enables customers to conduct their own risk assessments and provides tools and dashboards so they can supervise and monitor our cloud services.

For financial institutions in the EU, Microsoft has also published [Risk Assessment and Compliance Guide for Financial Institutions in the Microsoft Cloud](#), a checklist modeled after EBA guidance. It explains how to establish a governance model optimized to meet regulatory requirements, and efficiently evaluate the risks of using Microsoft cloud services, followed by submission for regulatory approval. Our guide includes a list of questions to be answered in a regulatory submission that are drawn from, and responsive to, EBA guidance on outsourcing to cloud service providers.

# Microsoft in-scope cloud services

- [Azure](#)
- [Microsoft 365](#)

## How to implement

- [Response to EBA guidance](#): Microsoft guidance helps EU financial institutions follow EBA recommendations for cloud adoption.
- [Financial use cases](#): Use-case overviews, tutorials, and other resources to build Azure solutions for financial services.
- [Financial Compliance Program](#): Financial institutions can get help with assessing the risks of using Microsoft cloud services.

## Frequently asked questions

### What information should be included in a submission to regulators?

The Microsoft publication, [Risk Assessment and Compliance Guide for Financial Institutions in the Microsoft Cloud](#), offers a checklist of questions that the EBA guidance recommends answering in a regulatory submission, and provides suggestions on how to answer those questions.

## Resources

- [Microsoft Service Trust Portal](#)
- [Microsoft Cloud Checklist for Financial Institutions in Europe](#)
- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Microsoft Financial Services Blog](#)
- [Compliance on the Microsoft Trust Center](#)

# EU-US and Swiss-US Privacy Shield Frameworks

2/5/2021 • 4 minutes to read • [Edit Online](#)

## About the EU-U.S. and Swiss-U.S. Privacy Shield frameworks

According to the Privacy Shield Program, “the [EU-U.S. and Swiss-U.S. Privacy Shield Frameworks](#) were designed by the US Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States.” The International Trade Administration within the Department of Commerce administers the Privacy Shield Program in the United States.

The transfer of personal data outside of the EU and Switzerland is governed by EU and Swiss law, which generally prohibit personal data from being transferred to countries outside the EEA unless “adequate” levels of protection are ensured. The Privacy Shield Frameworks and the Standard Contractual Clauses (or [EU Model Clauses](#)) are two mechanisms designed to provide this level of data protection.

The 23 [Privacy Shield Principles](#) define a set of requirements that govern the use and handling of personal data transferred from the EU as well as access and dispute resolution mechanisms that participating companies must provide to EU citizens. Companies must let individuals know how their data is processed, limit the purposes for which it is used, protect data for as long as it is held, and ensure accountability for data transferred to third parties. Requirements also include providing free and accessible dispute resolution and transparency related to government requests for personal data.

## Microsoft and the EU-U.S. and Swiss-U.S. Privacy Shield frameworks

To join the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks — an action that is voluntary — US-based companies must publicly commit to complying with framework requirements and self-certify their compliance to the US Department of Commerce. Once they publicly commit and self-certify, that commitment becomes enforceable under US law.

Microsoft has publicly committed to the [Privacy Shield Principles](#) and has self-certified its compliance with its requirements. Our participation applies to all personal data processed by Microsoft that is transferred to the United States from the European Union, European Economic Area (EEA), and Switzerland. In addition, customers of Microsoft business cloud services benefit from compliance with the Standard Contractual Clauses (also known as [EU Model Clauses](#)) under the [Microsoft Online Services Terms](#), unless the customer has opted out of those clauses.

Microsoft cooperates with EU and Swiss national data protection authorities (DPAs) and complies with their advice for resolving any disputes that arise under the Privacy Shield. We will also meet Privacy Shield obligations for transparency about government requests for access to personal information. Our [Law Enforcement Requests Report](#) and [U.S. National Security Orders Report](#) make this information publicly available twice a year.

## Microsoft in-scope cloud services

- [Azure and Azure DevOps](#)
- [Dynamics 365 MT & GCC](#)
- Intune
- [Microsoft 365](#)

- Power BI cloud service as a standalone service or as included in an Office 365 branded plan or suite
- Professional Services
- Windows 10 and Windows Server

## Audits, reports, and certificates

Microsoft has certified to the US Department of Commerce that it adheres to the Privacy Shield Principles and submitted its self-certification to the EU-U.S. and Swiss-U.S. Privacy Shield. It is listed by the Privacy Shield Framework as an [Active Participant](#).

## How to implement

Privacy in the Microsoft Cloud — Get details on Microsoft privacy principles and standards and our approach to regulatory compliance.

- [Learn more](#)

Data protection in Azure — Azure provides customers with strong data security, both by default and as customer options.

- [Learn more](#)

## Frequently asked questions

### **What data is transferred from the EU or Switzerland to the United States under the Microsoft Privacy Shield agreement?**

As specified in our Online Services Terms, personal data that Microsoft processes on the customer's behalf may be transferred to, stored, and processed in the United States or any other country in which Microsoft or its affiliates or subcontractors maintain facilities. Any such transfers from the EU, however, must meet the requirements of EU law.

When personal data is transferred from the EU to the United States by:

- Online services other than the core online services (as defined in the Online Services Terms), the transfer is subject to Microsoft commitments under the Microsoft Privacy Shield Agreement.
- The core online services, the transfer is subject to Microsoft commitments under the Standard Contractual Clauses.

### **How is Microsoft accountable for EU personal data transferred to a third party?**

Microsoft accountability for personal data that it receives under the Privacy Shield and later transfers to a third party is described in the Privacy Shield Principles. In particular, Microsoft remains responsible and liable if third-party agents that it engages to process the personal data do so in a manner inconsistent with the Principles. Microsoft is, however, not liable if it proves that it is not responsible for the event giving rise to the damage.

### **Is the transfer of data under the EU-U.S. and Swiss-U.S. Privacy Shield compliant with the GDPR?**

Privacy Shield is not a GDPR compliance mechanism, but rather a framework that enables participating companies to meet the EU requirements for transferring personal data outside of the EU.

### **How does Microsoft handle complaints under the EU-U.S. and Swiss-U.S. Privacy Shield?**

If you have a complaint that is Privacy Shield-related, please let us know using the [How to Contact Us](#) section of the [Microsoft Privacy Statement](#). For any complaints that you cannot resolve with Microsoft directly, we cooperate with EU DPAs and will comply with the advice they provide. Contact us to be directed to the relevant DPA contacts. As further explained in the [Privacy Shield Principles](#), you can take advantage of a binding arbitration option to address complaints unresolved by other means.

# Resources

- [EU Data Protection Directive](#)
- [Privacy Shield Frequently Asked Questions](#)
- [Microsoft and the EU Model Clauses](#)
- [Privacy at Microsoft](#)
- [Privacy considerations in the cloud](#)
- [Compliance on the Microsoft Trust Center](#)

# Federation Against Copyright Theft (FACT)

11/30/2020 • 2 minutes to read • [Edit Online](#)

## FACT overview

Copyrighted content comes in many forms, pictures, videos, music, contracts, scripts, workflows, art, architecture, and more, and represents the core assets of many businesses. Piracy threatens to undermine the very existence of these businesses through the unlawful distribution of intellectual property for illicit gain or market disruption. As production and post-production workflows increasingly move to the cloud, the black market for intellectual property is similarly moving away from physical media toward online mechanisms.

## Microsoft and Federation Against Copyright Theft (FACT)

To underscore Microsoft's commitment to protect customers when they entrust such assets to the public cloud, Microsoft Azure has been certified by the Federation Against Copyright Theft (FACT) in the United Kingdom. FACT certification is based on ISO 27001, focusing on physical and digital security, staff screening and training, and access control. The FACT content protection and security program incorporates expertise across law enforcement, technology partners, and industry associations to fight copyright infringement and content theft, such as peer-to-peer sharing, illegal disc duplication, and signal theft.

Based on the voluntary submission by Microsoft to a FACT audit, the FACT auditor certified Azure. Azure was the first multi-tenant public cloud service to achieve FACT certification, adding to Azure's portfolio of media-related certifications, including CDSA certification and a formal assessment by the MPAA.

## Microsoft in-scope cloud services

[Azure and Azure Government](#)

## Audits, reports, and certificates

The Azure certification is renewed annually: [Azure FACT certificate](#)

## Frequently asked questions

### Why is FACT important?

Content security is critical for feature film and television development, as there are multiple points along the workflow where digital assets can be compromised or stolen. Dailies, rough cuts, and visual effects are just some of the materials exposed during a normal film production cycle, and the box-office impacts of a security breach on a blockbuster project can reach tens of millions of dollars. By passing the FACT audit, Azure provides another layer of assurance to customers by helping to prevent the illegal distribution and sale of motion picture and television assets.

### Does my organization still need to undergo a FACT audit, or can we use the Azure audit?

Compliance with FACT is voluntary, but Microsoft elected to carry out an independent assessment so that media customers can be confident in the content security and protection capabilities of Azure. However, customers' individual cloud environments are not managed by Azure, and thus may be subject to additional regulation that is best addressed by an individual audit.

## Resources

- [Federation Against Copyright Theft](#)
- [Fact Security Certification Program](#)
- [CDSA certification of Azure Media Services](#)
- [Azure ISO 27001 certification](#)
- [MPAA Assessment](#)
- [Azure Responses to CSA CAIQ v3.0.1](#)
- [Compliance on the Microsoft Trust Center](#)



# United Kingdom Financial Conduct Authority (FCA)

12/14/2020 • 3 minutes to read • [Edit Online](#)

## FCA (UK) overview

The [Financial Conduct Authority](#) (FCA), an independent public body that is accountable to the Treasury, regulates 58,000 financial firms and markets in the UK and serves as the prudential regulator for over 18,000 of those organizations. [Prudential Regulation Authority](#) (PRA), which also serves as the prudential regulator for the Bank of England and regulates 1,500 of the larger financial services institutions such as banks, building societies, credit unions, insurers, and investment firms. (The FCA picks up prudential regulation for firms that do not fall under the PRA remit.)

The FCA had received feedback that financial institutions and cloud service providers were unclear about how to apply its rules for outsourcing to the cloud, a potential barrier to cloud use. Given that the FCA mandate includes promoting effective competition (for which innovation can be a driver), the FCA wanted to support the use of cloud services, stating “We see no fundamental reason why cloud services (including public cloud services) cannot be implemented, with appropriate consideration, in a manner that complies with our rules.” So the FCA clarified its requirements for outsourcing to the cloud, publishing final guidance in November 2016 in the [Guidance for firms outsourcing to the cloud and other third-party IT services](#) intended to help financial firms and cloud service providers understand FCA expectations when firms outsource to the cloud (or plan to do so). Although this guidance is not binding, the FCA expects firms to use it where appropriate. (Note that the PRA has different statutory objectives, so firms it regulates must confirm their approach with the PRA.) This is a detailed document and offers specific guidance for the use, evaluation, and ongoing monitoring of third parties in the delivery of IT services. It divides considerations into 13 areas of interest, ranging from legal, and regulatory considerations and risk management to continuity planning and plans for exiting outsourcing arrangements

## Microsoft and FCA (UK)

Microsoft has published a comprehensive guide, [Enabling compliance: The Microsoft approach to FCA finalized cloud guidance](#), detailing how Azure can help financial services customers that are authorized and regulated by the UK Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) when moving IT operations to the cloud.

The Microsoft guide describes in great detail our compliance with numerous recognized international standards, our transparency around how your customer data is handled to give you control over it, and the contractual provisions that address-specific financial regulatory requirements.

Sections in the Microsoft guide map in depth to each area of interest in the FCA guidance. For example, a key aspect of the regulatory outsourcing requirements is that financial services firms must identify and manage any risks which outsourcing may introduce into their business. Microsoft discusses its approach in carrying out a risk assessment, documenting it, identifying current best practices, and so on. We help you assess the relevant risks and make available a wide range of resources to facilitate your due diligence.

Learn how Azure is enabling FCA compliance in UK banks: [Read Microsoft collaborates with ClearBank: Launch of first new UK clearing bank in over 250 years](#)

## Accelerate your deployment on Azure

[Download Microsoft approach to FCA finalized cloud guidance](#)

## Microsoft in-scope cloud services

- [Azure](#)
- Intune
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Frequently asked questions

**Can I use Microsoft responses to this framework in my organization's compliance process?**

Yes. However, although Microsoft responses to this framework are confirmed compliant by third parties, customers are responsible for validating the compliance of solutions they have implemented on Azure or Power BI.

## Resources

- [Microsoft Cloud Checklist for Financial Institutions in the UK](#)
- [FG 16/5 — Guidance for firms outsourcing to the cloud and other third-party IT services](#)
- [Enabling compliance: The Microsoft approach to FCA finalized cloud guidance](#)
- [Microsoft Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)
- [Compliance on the Microsoft Trust Center](#)

# Federal Financial Institutions Examination Council (FFIEC)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## FFIEC overview

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body comprising five banking regulators that are responsible for US federal government examinations of financial institutions in the United States. The FFIEC Examiner Education Office publishes IT Examination Handbooks intended for field examiners from FFIEC member agencies.

The [FFIEC Audit IT Examination Handbook](#) contains guidance for these examiners to assess the quality and effectiveness of IT audit programs of both financial institutions and TSPs. Specifically, it includes mention of SOC 1, SOC 2, and SOC 3 attestation reports of the American Institute of Certified Public Accountants (AICPA) as examples of independent audit reports. However, the FFIEC recommends that financial institutions not rely solely on the information contained in these reports, but also use verification and monitoring procedures discussed in detail in the [FFIEC Outsourcing Technology Services IT Examination Handbook](#).

## Microsoft and FFIEC

Microsoft Azure, Microsoft Power BI, and Microsoft Office 365 are built to meet the stringent requirements of Providing cloud services for financial services institutions. As part of our support, we offer guidance to help you comply with FFIEC audit requirements for information technology and the ability to use Azure SOC attestations when pursuing your FFIEC compliance obligations.

To help financial institution clients meet their FFIEC compliance requirements with Azure, Microsoft has developed the [Azure Security and Compliance Blueprint for FFIEC Regulated Services Workloads](#). It offers guidance on the use of Azure cloud services and considerations for customer compliance with FFIEC requirements and risk assessment guidelines.

To further help you comply with FFIEC requirements, Microsoft cloud services provide [SOC attestation reports](#) produced by an independent CPA firm. For example, the SOC 1 Type 2 attestation is based on the AICPA SSAE 18 standard (see AT-C Section 105) that replaced SAS 70, and is appropriate for reporting on certain controls for financial reporting. The SOC reports include the auditor's opinion on the effectiveness of Microsoft controls in achieving the related control objectives during the specified monitoring period. Financial institutions can use this formal audit when pursuing FFIEC-specific compliance obligations for assets deployed on Azure, Power BI, and Office 365.

## Microsoft in-scope cloud services

- [Azure](#)
- Intune
- [Office 365](#)
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Audits, reports, and certificates

Azure and Office 365 SOC attestation reports.

## Frequently asked questions

### Can I use Microsoft compliance with SOC standards to meet the FFIEC compliance obligations for my institution?

To help you meet these obligations, Microsoft supplies the specifics about our compliance with SOC standards as described above. However, ultimately, it is up to you to determine whether our services comply with the specific laws and regulations applicable to your institution. The FFIEC also advises that 'users of audit reports or reviews should not rely solely on the information contained in the report to verify the internal control environment of the TSP. They should use other verification and monitoring procedures as discussed more fully in the [Outsourcing Technology Booklet](#) of the FFIEC IT Examination Handbook.'

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Federal Financial Institutions Examination Council \(FFIEC\)](#)
- [Compliance Map of Cloud Computing and Regulatory Principles in the US](#)
- [FFIEC Audit IT Examination Handbook](#)
- [FFIEC Outsourcing Technology Services IT Examination Handbook](#)
- [Azure Security and Compliance FFIEC Financial Services Blueprint](#)

## Other Microsoft resources for financial services

- [Microsoft Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)
- [Shared responsibilities for cloud computing](#)
- [Compliance on the Microsoft Trust Center](#)

# Financial Market Supervisory Authority (FINMA) Switzerland

2/5/2021 • 2 minutes to read • [Edit Online](#)

## About FINMA

The [Financial Market Supervisory Authority \(Eidgenössische Finanzmarktaufsicht, FINMA\)](#) is the regulator of independent financial markets in Switzerland and is responsible for ensuring that Swiss financial markets function effectively. It has prudential supervision over banks, insurance companies, exchanges, securities dealers, and other financial institutions.

The FINMA published [Circular 2018/3 Outsourcing—banks and insurers](#) to define the requirements that banks, securities dealers, and insurance companies must abide by when they outsource to a service provider any functions that are significant to the company's business activities. Any company that outsources its business activities is accountable to the FINMA just as it would be if it carried out the outsourced functions itself.

## Microsoft and FINMA

To help guide financial institutions in Switzerland considering outsourcing business functions to the cloud, Microsoft has published [A compliance checklist for financial institutions in Switzerland](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When Swiss financial institutions outsource business activities, they must comply with the requirements of the Swiss Financial Market Supervisory Authority (FINMA) and be cognizant of other requirements and guidelines that include those of the Swiss Bank Act, the Swiss Bank Ordinance, and the Swiss Insurance Supervision Act.

The Microsoft checklist helps Swiss financial firms conducting due-diligence assessments of Microsoft business cloud services and includes:

- An overview of the regulatory landscape for context.
- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Compliance checklist: Switzerland](#): Financial firms can get help in conducting risk assessments of Microsoft business cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Use case overviews, tutorials, and other resources to build Azure solutions for financial services.

# Frequently asked questions

## Is regulatory approval required?

No. The use of public cloud computing is permitted without an approval by the FINMA, subject always to compliance with the requirements set out in the regulations and guidelines listed above.

## Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. In Part 2 of the Compliance Checklist, we have mapped these terms against the sections in the Microsoft contractual documents where you find them addressed. In addition, the Swiss Federal Data Protection and Information Commissioner (FDPIC) supplies a sample contract for transborder outsourcing of data processing. This is the same as the Standard Contractual Clauses (also known as [EU Model Clauses](#)) under the [Microsoft Online Services Terms](#).

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Compliance on the Microsoft Trust Center](#)

# Gramm-Leach-Bliley Act (GLBA)

2/5/2021 • 2 minutes to read • [Edit Online](#)

## GLBA overview

The Gramm-Leach-Bliley Act (GLBA) is a US law that reformed the financial services industry, allowing commercial and investment banks, securities firms, and insurance companies to consolidate, and addressed concerns about protecting consumer privacy. It required the Federal Trade Commission (FTC) and other financial services regulators to implement regulations to address such privacy provisions as the Financial Privacy Rule and the Safeguards Rule. GLBA requirements to safeguard sensitive consumer data apply to financial institutions that offer financial products and services to consumers, such as loans, investment advice, and insurance. The FTC is charged with enforcing compliance.

## Microsoft and GLBA

Microsoft Azure, Microsoft Office 365, Dynamics 365, and Microsoft Power BI can help meet the stringent requirements of providing cloud services for financial services institutions. As part of our support, we offer guidance to help you comply with the requirements of the GLBA by providing technical and organizational safeguards to help maintain security and prevent unauthorized usage.

Microsoft has developed risk assessment tools for both [Azure](#) and [Office 365](#) to help you more efficiently conduct a risk assessment of Azure and Office 365 services. The tool (an Excel spreadsheet) features 19 information security domains (such as security policy and risk management) that track the requirements of financial services regulations and other relevant standards, including GLBA (in Column R in the Azure spreadsheet and Column Q in the Office 365 spreadsheet). The tools explain how Azure and Office 365 comply with each requirement applicable to cloud service providers and can help you meet GLBA security requirements.

## Promote your GLBA compliance

- [Download the Azure Financial Services Cloud Risk Assessment Tool](#)
- [Download the Office 365 Cloud Risk Assessment Tool](#)

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- Intune
- [Office 365](#)
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Frequently asked questions

**How do I know if my financial institution must comply with the GLB Act?**

The FTC answers this in detail on its GLB Act page, [Who is covered by the privacy rule?](#)

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium

template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Gramm-Leach-Bliley Act](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Office 365 Cloud Risk Assessment Tool](#)
- [Compliance on the Microsoft Trust Center](#)

## Other Microsoft resources for financial services

- [Microsoft Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)
- [Shared responsibilities for cloud computing](#)



# Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)

2/17/2021 • 6 minutes to read • [Edit Online](#)

## HITRUST — CSF overview

The Health Information Trust Alliance (HITRUST) is an organization governed by representatives from the healthcare industry. HITRUST created and maintains the Common Security Framework (CSF), a certifiable framework to help healthcare organizations and their providers demonstrate their security and compliance in a consistent and streamlined manner.

The CSF builds on HIPAA and the HITECH Act, which are US healthcare laws that have established requirements for the use, disclosure, and safeguarding of individually identifiable health information, and that enforce noncompliance. HITRUST provides a benchmark — a standardized compliance framework, assessment, and certification process — against which cloud service providers and covered health entities can measure compliance. The CSF also incorporates healthcare-specific security, privacy, and other regulatory requirements from such existing frameworks as the Payment Card Industry Data Security Standard ([PCI-DSS](#)), [ISO/IEC 27001](#) information security management standards, and Minimum Acceptable Risk Standards for Exchanges ([MARS-E](#)).

The CSF is divided into 19 different domains, including endpoint protection, mobile device security, and access control. HITRUST certifies IT offerings against these controls. HITRUST also adapts requirements for certification to the risks of an organization based on organizational, system, and regulatory factors.

Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)

HITRUST offers three degrees of assurance, or levels of assessment: self-assessment, CSF validated, and CSF-certified. Each level builds with increasing rigor on the one below it. An organization with the highest level, CSF-certified, meets all the certification requirements of the CSF. Microsoft Azure and Office 365 are the first hyperscale cloud services to receive certification for the HITRUST CSF. Coalfire, a HITRUST assessor firm, performed the assessments based on how Azure and Office 365 implement security, privacy, and regulatory requirements to protect sensitive information. Microsoft supports the HITRUST Shared Responsibility Program.

Learn how to accelerate your HITRUST deployment with our Azure Security and Compliance Blueprint.

[Download the Microsoft Azure HITRUST Customer Responsibility Matrix \(CRM\) blueprint v9.0d](#)

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- [Intune](#)
- [Microsoft Managed Desktop](#)
- [Office 365 and Office 365 U.S. Government](#)

## Audits, reports, and certificates

The HITRUST CSF certification of Azure and Office 365 is valid for two years.

- [Azure HITRUST Letter of Certification](#)
- [Office 365 HITRUST Letter of Certification](#)

# Accelerate your deployment of HIPAA/HITRUST solutions on Azure

Get a head start on taking advantage of the benefits of the cloud for health data solutions with the Azure Security and Compliance Blueprint — HIPAA/HITRUST Health Data and AI. This blueprint provides tools and guidance to get you started building HIPAA/HITRUST solutions today.

[Start using the Azure HIPAA/HITRUST Blueprint](#)

## Accelerate your HIPAA/HITRUST compliance when using Office 365

Use Office 365 to manage health information in a secure and compliant way with Compliance Score, which enables you to perform risk assessments against health regulations like HIPAA and security control frameworks like NIST CSF and NIST 800-53. You can follow step-by-step guidance to know how to implement and maintain data protection controls that help you meet healthcare compliance obligations.

[Start using Compliance Score](#)

## Collaborate with Microsoft in the HITRUST Shared Responsibility Program

Accelerate achieving HITRUST compliance for your solution hosted on Microsoft Azure by pre-populating your assessment with fully inherited or shared responsibility controls for Azure in the HITRUST MyCSF tool, and collaborating with Microsoft on your assessment.

[Learn more](#)

## Frequently asked questions

### Can I use the Azure HITRUST compliance to build on my organization's certification process?

Yes. If your business requires a HITRUST certification for implementations deployed on Microsoft services, you can build on Azure HITRUST compliance when you conduct your compliance assessment. However, you are responsible for evaluating the HITRUST requirements and controls within your own organization.

### How can I get a copy of the HITRUST certification?

You can download a copy of letter of certification for [Azure](#) and [Office 365](#).

### What are the in-scope services for Office 365?

The in-scope services of HITRUST CSF certification are Exchange Online Archiving, Exchange Online Protection, Exchange Online, Skype for Business, Admin Center, SharePoint Online, Project Online, OneDrive for Business, Office Online, MyAnalytics, Microsoft Teams, Microsoft 365 Apps for enterprise in Office 365 Multi-tenant cloud and Office 365 GCC.

#### **NOTE**

Microsoft 365 Apps for enterprise enables access to various cloud services, such as Roaming Settings, Licensing, and OneDrive consumer cloud storage, and may enable access to additional cloud services in the future. Roaming Settings and Licensing support the standards for HITRUST. OneDrive consumer cloud storage does not, and other cloud services that are accessible through Microsoft 365 Apps for enterprise and that Microsoft may offer in the future also may not, support these standards.\*

### Why are some Office 365 services not in the scope of this certification?

Microsoft provides the most comprehensive offerings compared to other cloud service providers. To keep up

with our broad compliance offerings across regions and industries, we include services in the scope of our assurance efforts based on the market demand, customer feedback, and product lifecycle. If a service is not included in the current scope of a specific compliance offering, your organization has the responsibility to assess the risks based on your compliance obligations and determine the way you process the data in that service. We continuously collect feedback from customers and work with regulators and auditors to expand our compliance coverage to meet your security and compliance needs.

### **Does Microsoft certification mean that if my organization uses Azure or Office 365, it is compliant with HITRUST CSF?**

When you store your data in a SaaS like Office 365, it's a shared responsibility between Microsoft and your organization to achieve compliance. Microsoft manages majority of the infrastructure controls including physical security, network controls, application level controls, etc., and your organization has the responsibility to manage access controls and protect your sensitive data. The Office 365 HITRUST certification demonstrates the compliance of Microsoft's control framework. Building on that, your organization needs to implement and maintain your own data protection controls to meet HITRUST CSF requirements.

### **Does Microsoft provide guidance for my organization to implement appropriate controls when using Office 365?**

Yes, you can find recommended customer actions in Compliance Score, cross-Microsoft Cloud solutions that help your organization meet complex compliance obligations when using cloud services. Specifically, for HITRUST CSF, we recommend that you perform risk assessments using the NIST 800-53 and NIST CSF assessments in Compliance Score. In the assessments, we provide you with step-by-step guidance and the Microsoft solutions you can use to implement your data protection controls. You can learn more about Compliance Score in [Microsoft Compliance Score](#).

### **How do I engage with Microsoft?**

Log in to the HITRUST MyCSF<sup>®</sup> tool and pre-populate your assessment for your solution hosted on Microsoft Azure with either fully inherited or shared responsibility controls for Azure. A Microsoft HITRUST Administrator will then complete their part of the assessment using their account on the MyCSF<sup>®</sup> tool.

## **Use Microsoft Compliance Manager to assess your risk**

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## **Resources**

- [HITRUST Alliance](#)
- [HITRUST CSF 9.3](#)
- [Understanding and Leveraging the CSF](#)
- [Find out more about the HITRUST Shared Responsibility Program](#)
- [Compliance on the Microsoft Trust Center](#)

# US Internal Revenue Service Publication 1075

2/5/2021 • 4 minutes to read • [Edit Online](#)

## US Internal Revenue Service Publication 1075 overview

Internal Revenue Service Publication 1075 (IRS 1075) provides guidance for US government agencies and their agents that access federal tax information (FTI) to ensure that they use policies, practices, and controls to protect its confidentiality. IRS 1075 aims to minimize the risk of loss, breach, or misuse of FTI held by external government agencies. For example, a state Department of Revenue that processes FTI in tax returns for its residents, or health services agencies that access FTI, must have programs in place to safeguard that information.

To protect FTI, IRS 1075 prescribes security and privacy controls for application, platform, and datacenter services. For instance, it prioritizes the security of datacenter activities, such as the proper handling of FTI, and the oversight of datacenter contractors to limit entry. To ensure that government agencies receiving FTI apply those controls, the IRS established the Safeguards Program, which includes periodic reviews of these agencies and their contractors.

## Microsoft and US Internal Revenue Service Publication 1075

Microsoft Azure Government and [Microsoft Office 365 U.S. Government](#) cloud services provide a contractual commitment that they have the appropriate controls in place, and the security capabilities necessary for Microsoft agency customers to meet the substantive requirements of IRS 1075.

These Microsoft cloud services for government provide a platform on which customers can build and operate their solutions, but customers must determine for themselves whether those specific solutions are operated in accordance with IRS 1075 and are, therefore, subject to IRS audit.

To help government agencies in their compliance efforts, Microsoft:

- Offers detailed guidance to help agencies understand their responsibilities and how various IRS controls map to capabilities in Azure Government and Office 365 U.S. Government. The IRS 1075 Safeguard Security Report (SSR) thoroughly documents how Microsoft services implement the applicable IRS controls, and is based on the FedRAMP packages of Azure Government and Office 365 U.S. Government. Because both IRS 1075 and FedRAMP are based on NIST 800-53, the compliance boundary for IRS 1075 is the same as the FedRAMP authorization.
- The IRS must explicitly approve the release of any IRS Safeguards document, so only government customers under NDA can review the SSR.
- Makes available audit reports and monitoring information produced by independent assessors for its cloud services.
- Provides to the IRS Azure Government Compliance Considerations and Office 365 U.S. Government Compliance Considerations, which outline how an agency can use Microsoft Cloud for Government services in a way that complies with IRS 1075. Government customers under NDA can request these documents.
- Offers customers the opportunity (at their expense) to communicate with Microsoft subject matter experts or outside auditors if needed.

## Microsoft in-scope cloud services

FedRAMP authorizations are granted at three impact levels based on NIST guidelines — low, medium, and high. These rank the impact that the loss of confidentiality, integrity, or availability could have on an organization —

low (limited effect), medium (serious adverse effect), and high (severe or catastrophic effect).

- [Azure and Azure Government](#)
- Dynamics 365 U.S. Government
- [Office 365 and Office 365 U.S. Government](#)
- Office 365 U.S. Government Defense
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Audits, reports, and certificates

Compliance with the substantive requirements of IRS 1075 is covered under the FedRAMP audit every year.

- [FedRAMP authorizations](#)
- [Azure IRS 1075 safeguard security report](#)

## Frequently asked questions

### How does Microsoft address the requirements of IRS 1075?

Microsoft regularly monitors its security, privacy, and operational controls and NIST 800-53 rev. 4 controls required by the FedRAMP baseline for Moderate Impact information systems. It provides quarterly access to this information through continuous monitoring reports. Azure Government and Office 365 U.S. Government customers can access this sensitive compliance information through the [Service Trust Portal](#).

In addition, Microsoft has committed to including IRS 1075 controls in its master control set for Azure Government and Office 365 U.S. Government, and to auditing against them annually.

### Can I review the FedRAMP packages or the System Security Plan?

Yes, if your organization meets the eligibility requirements for Azure Government and Office 365 U.S. Government. Contact your Microsoft account representative directly to review these documents. You can also refer to the FedRAMP list of compliant cloud service providers.

### Can I use the Azure or Office 365 public cloud environments and still be compliant with IRS 1075?

No. The only environments where FTI can be stored and processed are Azure Government or Office 365 U.S. Government. Government customers must meet the eligibility requirements to use these environments.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [IRS Publication 1075](#)
- [IRS Safeguards Program](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Microsoft Cloud for Government](#)
- [Compliance on the Microsoft Trust Center](#)

# ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud

2/17/2021 • 5 minutes to read • [Edit Online](#)

## ISO/IEC 27018 overview

The International Organization for Standardization (ISO) is an independent nongovernmental organization and the world's largest developer of voluntary international standards. The ISO/IEC 27000 family of standards helps organizations of every type and size keep information assets secure.

In 2014, the ISO adopted ISO/IEC 27018:2014, an addendum to ISO/IEC 27001, the first international code of practice for cloud privacy. Based on EU data-protection laws, it gives specific guidance to cloud service providers (CSPs) acting as processors of personally identifiable information (PII) on assessing risks and implementing state-of-the-art controls for protecting PII.

### Microsoft and ISO/IEC 27018

At least once a year, Microsoft Azure and Azure Germany are audited for compliance with ISO/IEC 27001 and ISO/IEC 27018 by an accredited third-party certification body, providing independent validation that applicable security controls are in place and operating effectively. As part of this compliance verification process, the auditors validate in their statement of applicability that Microsoft in-scope cloud services and commercial technical support services have incorporated ISO/IEC 27018 controls for the protection of PII in Azure. To remain compliant, Microsoft cloud services must be subject to annual third-party reviews.

By following the standards of ISO/IEC 27001 and the code of practice embodied in ISO/IEC 27018, Microsoft (the first major cloud provider to incorporate this code of practice) demonstrates that its privacy policies and procedures are robust and in line with its high standards.

- **Customers of Microsoft cloud services know where their data is stored.** Because ISO/IEC 27018 requires certified CSPs to inform customers of the countries in which their data may be stored, Microsoft cloud service customers have the visibility they need to comply with any applicable information security rules.
- **Customer data won't be used for marketing or advertising without explicit consent.** Some CSPs use customer data for their own commercial ends, including for targeted advertising. Because Microsoft has adopted ISO/IEC 27018 for its in-scope enterprise cloud services, customers can rest assured that their data will never be used for such purposes without explicit consent, and that consent cannot be a condition for use of the cloud service.
- **Microsoft customers know what's happening with their PII.** ISO/IEC 27018 requires a policy that allows for the return, transfer, and secure disposal of personal information within a reasonable period of time. If Microsoft works with other companies that need access to your customer data, Microsoft proactively discloses the identities of those sub-processors.
- **Microsoft complies only with legally binding requests for disclosure of customer data.** If Microsoft must comply with such a request (as in the case of a criminal investigation), it will always notify the customer unless it is prohibited by law from doing so.

## Microsoft in-scope cloud services

- [Azure, Azure Government, and Azure Germany](#)
- Azure DevOps Services
- Microsoft Cloud App Security

- Dynamics 365, Dynamics 365, and Dynamics 365 Germany
- Microsoft Professional Services: Premier and On Premises for Azure, Dynamics 365, Intune, and for medium business and enterprise customers of Microsoft 365 for business
- Microsoft Graph
- Microsoft Healthcare Bot
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow): cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)
- Office 365 Germany
- OMS Service Map
- PowerApps cloud service: either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service: either as a standalone service or as included in an Office 365 branded plan or suite
- Power BI Embedded
- Power Virtual Agents
- Microsoft Threat Experts
- Microsoft Stream
- Windows Defender ATP: Endpoint Detection & Response, Automatic Investigation & Remediation, Secure Score

## Audits, reports, and certificates

### Audit cycle

Microsoft cloud and commercial technical support services are audited once a year for the ISO/IEC 27018 code of practice as part of the certification process for ISO/IEC 27001.

### Audits and reports

- [Azure, Dynamics 365, and Online Services: ISO27018 Certificate](#)
- [Azure, Dynamics 365, and Online Services: ISO27018 Assessment Report](#)
- [Azure Germany: ISO27018 Code of Practice for Protecting Personal Data in the Cloud Certificate](#)

### Office 365

- [Office 365: ISO 27001, 27018, and 27017 Audit Assessment Report](#)
- [Yammer ISO 27018 Audit Assessment Report](#)

### Azure DevOps Services

- [Azure DevOps Services: ISO27018 Certificate PII 665918](#)

## Frequently asked questions

### To whom does ISO/IEC 27018 apply?

This code of practice applies to CSPs that process PII under contract for other organizations. At Microsoft, it also applies to the support of these CSPs.

### What is the difference between 'personal information controllers' and 'personal information processors'?

In the context of ISO/IEC 27018:

- 'Controllers' control the collection, holding, processing, or use of personal information; they include those who control it on another company's behalf.
- 'Processors' process information on behalf of controllers; they do not make decisions as to how to use the information or the purposes of the processing. In providing its enterprise cloud services, Microsoft (as a vendor to you) is an information processor.

#### Where can I view Microsoft compliance information for ISO/IEC 27018?

- You can review the ISO/IEC 27018 certificates from BSI for [Azure](#), [Microsoft Professional Services](#), and [Power BI](#).
- You can also review ISO/IEC 27001 certificates from BSI upon which ISO/IEC 27018 certification is based for [Dynamics 365](#), [Office 365](#), and [Azure DevOps Services](#).
- To review the BSI reports, the independent auditor that validated Microsoft compliance with ISO/IEC 27018, visit the [Service Trust Portal](#).

#### Can I use Microsoft's compliance in my organization's certification process?

Yes. If compliance with ISO/IEC 27018 is important for your business and implementations deployed on any of Microsoft in-scope enterprise cloud services, you can use Microsoft's attestation of compliance with ISO/IEC 27018 with Microsoft's certification for ISO/IEC 27001 in your compliance assessment.

However, you are responsible for engaging an assessor to evaluate your implementation for compliance, and for the controls and processes within your own organization.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [ISO/IEC 27018:2014 code of practice](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Data access policies for Microsoft enterprise cloud and technical services](#)
- [Microsoft Online Services Terms](#)
- [Microsoft Government Cloud](#)
- [Compliance on the Microsoft Trust Center](#)



# ISO 9001:2015 Quality Management Systems Standards

2/17/2021 • 2 minutes to read • [Edit Online](#)

## ISO 9001 overview

ISO 9001:2015 is an international standard that establishes the criteria for a quality management system. It is the only standard in the ISO 9000 family that results in a formal certification. The standard is based on several quality management principles, including clear focus on meeting customer requirements, strong corporate governance and leadership commitment to quality objectives, process-driven approach to meeting objectives, and focus on continuous improvement. ISO 9001:2015 helps organizations improve customer satisfaction by focusing on the consistency and quality of products and services provided to customers.

## Microsoft and ISO 9001:2015

An independent third-party auditing firm performed a rigorous examination of Microsoft Azure and several Microsoft online services for adherence to the quality management principles established by ISO 9001:2015. The available third-party certification provides independent confirmation that Azure and covered Microsoft online services meet the ISO 9001:2015 requirements.

## Microsoft in-scope cloud services

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- Dynamics 365, Dynamics 365 Government, and Dynamics 365 Germany
- Microsoft Graph
- Intune
- Microsoft Defender Advanced Threat Protection
- Microsoft Healthcare Bot
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- Power BI Embedded
- Microsoft Stream

## Audits, reports, and certificates

- [Azure, Dynamics 365, and Online Services: ISO9001 Certificate](#)
- [Azure, Dynamics 365, and Online Services: ISO9001 Assessment Report](#)
- [Azure, Dynamics 365, and Online Services: ISO9001 Statement of Applicability \(SOA\)](#)

## Frequently asked questions

To whom does the standard apply?

This standard of practice provides guidance and tools for cloud service providers and cloud service customers to ensure that cloud products and services consistently meet customers' requirements. It is structured in a format similar to ISO 27001:2013.

#### **Where can I get the ISO 9001:2015 audit reports and scope statements for Microsoft services?**

The [Service Trust Portal](#) provides independently audited compliance reports. You can use the portal to request reports so that your auditors can compare Microsoft's cloud services results with your own legal and regulatory requirements. The [FY17 Microsoft Azure ISO 9001 Assessment Report](#) and the [FY17 Microsoft Azure ISO 9001 Certificate](#) are both available.

#### **Does Microsoft run annual tests for infrastructure failures?**

Yes. The ISO 9001:2015 annual assessment includes the underlying physical infrastructure datacenter. [Review the certificate](#) for the coverage details.

#### **Where can I view Microsoft's compliance information for ISO 9001:2015?**

You can download the [ISO 9001:2015 certificate](#) for Azure and additional services that are in scope of this assessment.

## Resources

- [ISO 9001:2015—Quality management](#)
- [ISO 9001: 2015 standard](#) (requirements for purchase)
- [ISO 9000: 2015](#) (fundamentals and vocabulary for purchase)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

# International Traffic in Arms Regulations (ITAR)

11/30/2020 • 2 minutes to read • [Edit Online](#)

## ITAR overview

The US Department of State is responsible for managing the export and temporary import of defense articles (meaning any item or technical data designated under the US Munitions List, as described in Title 22 CFR 121.1) that are governed by the Arms Export Control Act (Title 22 USC 2778) and the International Traffic in Arms Regulations (ITAR) (Title 22 CFR 120–130). The Directorate for Defense Trade Controls (DDTC) is responsible for managing entities governed under these programs.

## Microsoft and ITAR

Microsoft provides certain cloud services or service features that can support customers with ITAR obligations. While there is no compliance certification for the ITAR, Microsoft operates and has designed in-scope services to be capable of supporting a customer's ITAR obligations and compliance program.

Microsoft Azure Government and Microsoft Office 365 U.S. Government for Defense provide support for customers with data subject to the ITAR through additional contractual commitments to customers regarding the location of stored data, and limitations on the ability to access such data to US persons. Microsoft provides these assurances for the infrastructure and operational components of these government cloud services, but customers are ultimately responsible for the protection and architecture of their applications within their environments.

Customers must sign additional agreements formally notifying Microsoft of their intention to store ITAR-controlled data, so that Microsoft may comply with responsibilities both to our customers and to the US government.

The ITAR has specific obligations to report violations, which can provide certain risk mitigation benefits. The Microsoft Enterprise Agreement Amendment enables Microsoft and the customer to work together in reporting such violations.

Customers seeking to host ITAR-regulated data should work with their Microsoft account and licensing teams to learn more, obtain proper agreements, and access relevant system architecture information.

## Microsoft in-scope cloud services

- [Azure Government](#)
- [Office 365 U.S. Government Defense](#)

## Frequently asked questions

**Where can I request compliance information?**

Contact your Microsoft account representative.

## Resources

- [DDTC ITAR](#)
- [ITAR Title 22 CFR 120–130](#)
- [Using Azure Government with ITAR controlled data](#)

- [Azure Government](#)
- [Office 365 U.S. Government](#)
- [Compliance on the Microsoft Trust Center](#)

# Financial Supervision Authority (KNF) Poland

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the KNF

The [Polish Financial Supervision Authority](#) ([Komisja Nadzoru Finansowego](#), KNF) is the financial regulatory authority in Poland, responsible for supervision of the financial market, which includes oversight over banking, capital markets, insurance, pension schemes, and electronic money institutions.

The KNF acts in concert with the [European Banking Authority](#) (EBA), “an independent EU authority, which works to ensure effective and consistent prudential regulation and supervision across the European banking sector.” To that end, the EBA has outlined a comprehensive approach to the use of cloud computing by financial institutions in the EU, [Recommendations on outsourcing to cloud services providers](#).

There are several requirements and guidelines that financial institutions in Poland should be aware of when moving business functions and data to the cloud:

- The Banking Act of 1997 ([Polish](#) and [English](#)) does not regulate cloud services directly but instead sets out legal requirements for outsourcing banking operations including how personal information can be processed. Cloud services could be subject to Banking Act provisions if the outsourced services are of key significance for the bank, or if outsourcing involves giving the service provider access to sensitive data that is subject to banking secrecy requirements.
- The Announcement, issued by the KNF Office in 2017, provides a detailed checklist and action plan for regulated institutions that intend to move business functions to the cloud.
- [Recommendation D](#): Management of Information Technology and ICT Environment Security at Banks defines KNF expectations for prudent IT security management by banks, particularly as to how they manage risk. The KNF makes 22 recommendations for best security practices and has issued comparable guidelines for [insurance companies](#), [investment firms](#), and [general pension companies](#).

In addition, the use of cloud services by financial institutions must comply with Poland’s Personal Data Protection Act of 1997, which is fundamental to the processing of personal data. To align with the GDPR, it was amended in late 2018 by the Act on Facilitation of Performance of Business Activity ([Polish](#)) and will take effect 1 January 2019.

## Microsoft and the KNF

To help guide financial institutions in Poland considering outsourcing business functions to the cloud, Microsoft has published [Navigating your way to the cloud: A compliance checklist for financial institutions in Poland](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When financial institutions in Poland outsource business activities to the cloud, they must address requirements of the Banking Act of 1997 and the 2017 KNF Announcement regarding the use of data processing services in the cloud, both of which fall within the broad policy framework of the European Banking Authority. In addition, financial firms using cloud services must comply with the GDPR-aligned 2018 amendment to the Personal Data Protection Act of 1997, now updated to align with the GDPR.

The Microsoft checklist helps Polish financial firms conducting due-diligence assessments of Microsoft business cloud services and includes:

- An overview of the regulatory landscape for context.

- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Compliance checklist: Poland](#): Financial firms can get help in conducting risk assessments of Microsoft business cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Use case overviews, tutorials, and other resources to build Azure solutions for financial services.
- [Privacy in Microsoft Cloud](#): Get details on Microsoft privacy principles and standards and on privacy laws specific to Poland.

## Frequently asked questions

### Is regulatory approval required?

No. However, under the Banking Act of 1997, if the service provider is based outside the European Economic Area (EEA) or if outsourced operations are to be implemented outside the EEA, banks must obtain KNF approval before entering into contracts.

### Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. Part 2 of the [Microsoft checklist](#) (page 77) contains a comprehensive list of the requirements that should be included in contracts with cloud service providers.

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Compliance on the Microsoft Trust Center](#)

# Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0 Framework

11/30/2020 • 3 minutes to read • [Edit Online](#)

## MARS-E 2.0 Framework overview

In 2012, the Center for Medicare and Medicaid Services (CMS) published the Minimum Acceptable Risk Standards for Exchanges (MARS-E) in accordance with CMS information security and privacy programs. The suite of documents, including guidance, requirements, and templates, was designed to address mandates of the Patient Protection and Affordable Care Act (ACA) and regulations of the Department of Health and Human Services that apply to the ACA. The National Institute of Standards and Technology (NIST) Special Publication 800-53 serves as the parent framework that establishes the security and compliance requirements for all systems, interfaces, and connections between ACA-mandated health exchanges and marketplaces.

Following the release of MARS-E, NIST released an update, Special Publication 800-53r4, to address growing challenges to online security, including application security; insider and advanced persistent threats; supply chain risks; and the trustworthiness, assurance, and resilience of systems of mobile and cloud computing. CMS then revised the MARS-E framework to align with the updated controls and parameters in NIST 800.53r4, publishing MARS-E 2.0 in 2015.

These updates address the confidentiality, integrity, and availability in health exchanges of protected data, which includes personally identifiable information, protected health information, and federal tax information. The MARS-E 2.0 framework aims to secure this protected data and applies to all ACA administering entities, including exchanges or marketplaces, federal, state, state Medicaid, or Children's Health Insurance Program (CHIP) agencies, and supporting contractors.

## Microsoft and MARS-E 2.0 framework

Currently, there is no formal authorization and accreditation process for MARS-E. However, Microsoft Azure platform services have undergone independent FedRAMP audits at the Moderate Impact Level and Azure Government at the High Impact Level, and are authorized according to FedRAMP standards. Although these standards do not specifically focus on MARS-E, the MARS-E control requirements and objectives are closely aligned and serve to protect the confidentiality, integrity, and availability of data on Azure.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Intune

## Audits, reports, and certificates

Microsoft business cloud services are monitored and assessed each year for the FedRAMP authorization process.

## Frequently asked questions

### To whom does the standard apply?

MARS-E applies to all Affordable Care Act administering entities, including exchanges or marketplaces, federal, state, Medicaid, and CHIP agencies administering the Basic Health Program, as well as all their contractors and

subcontractors.

### **How does Microsoft demonstrate Azure and Azure Government compliance with this standard?**

Using the formal audit reports prepared by third parties for FedRAMP authorizations, Microsoft is able to show how relevant controls noted that within these reports demonstrate Azure capabilities in meeting MARS-E security and privacy control requirements. Audited controls implemented by Microsoft serve to protect the confidentiality, integrity, and availability of data stored on the Azure platform, and correspond to the applicable regulatory requirements defined in MARS-E that have been identified as the responsibility of Microsoft.

### **What are Microsoft's responsibilities for maintaining compliance with this standard?**

Microsoft ensures that the Azure platform meets the terms defined within the governing [Online Services Terms](#) and applicable service level agreements (SLAs). These agreements define our responsibility for implementing and maintaining controls adequate to secure the Azure platform and monitor the system.

### **Can I use Microsoft's compliance in the MARS-E qualification efforts for my organization?**

Yes. Third-party audit reports to the FedRAMP standards attest to the effectiveness of the controls Microsoft has implemented to maintain the security and privacy of the Azure platform. Azure and Azure Government customers may use the audited controls described in these related reports as part of their own FedRAMP and MARS-E risk analysis and qualification efforts.

## **Resources**

- MARS-E regulatory guidance, MARS-E Document Suite, Version 2.0
  - [Volume II: Minimum acceptable risk standards for exchanges](#)
  - [Volume III: Catalog of minimum acceptable risk security and privacy controls for exchanges](#)
- [Microsoft compliance framework for online services white paper](#)
- [Microsoft cloud services terms](#)
- [Compliance on the Microsoft Trust Center](#)



# Motion Picture Association of America (MPAA)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## MPAA overview

The Motion Picture Association of America (MPAA) provides best-practices guidance and control frameworks to help major studio partners and vendors design infrastructure and solutions to ensure the security of digital film assets. The MPAA also performs content security assessments on behalf of its member companies: Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, and Warner Bros. Entertainment Inc.

## Microsoft and MPAA

In February 2016, Microsoft Azure became the first hyperscale, multitenant cloud service to successfully complete a formal assessment by independent MPAA auditors and comply with all three of the MPAA content security best practices frameworks: Common, Application, and Cloud Security Guidelines.

The MPAA assessment covers 48 security topics in the Common Guidelines, and an additional six in the Application and Cloud Security Guidelines. These are built on industry-accepted security standards such as ISO/IEC 27001 and NIST 800-53, and are aligned to best practices, such as the Cloud Security Alliance (CSA) Cloud Controls Matrix.

The formal assessment of Azure compliance means that companies who do business with major studios can use Azure to help reduce the IT costs that are normally associated with the secure creation, management, storage, and distribution of content — all while complying with MPAA requirements. Azure Media Services, Storage, Virtual Networks, and more than 30 other services provide a content workflow engine in the cloud that is more secure and scalable than traditional on-premises production processes and more effective at protecting media assets downstream.

## Microsoft in-scope cloud services

- [Azure complies with MPAA best-practices guidelines](#)

## Audits, reports, and certificates

- [Azure MPAA common guidelines](#)
- [Azure MPAA application and cloud security guidelines](#)

## Frequently asked questions

**How can I get copies of Microsoft responses to the MPAA audit?**

The [Service Trust Portal](#) provides access to Microsoft responses to the Common Guidelines and the Application and Cloud Security Guidelines. You can also review copies of the Azure ISO/IEC 27001 Audit Report and the CDSA CPS Audit Report and Statement of Applicability in the portal.

**Why is the MPAA important?**

Content security is critical for feature film development, as there are multiple points along the workflow where digital assets could be compromised or stolen. Dailies, rough cuts, and visual effects are just some of the materials exposed during a normal production cycle, and the box-office impacts of a security breach on a

blockbuster project can reach tens of millions of dollars.

MPAA guidelines provide major studio vendors and partners with a set of best practices for creating, processing, storing, and distributing digital assets. Service providers such as Azure who undergo the formal assessment can provide an additional layer of assurance that content uploaded to the cloud will be managed in accordance with established industry requirements for encryption, authentication, access control, and resiliency, among others.

### **Does my organization still need to undergo an MPAA audit, or can we use the Azure audit?**

Production facilities, visual effects houses, and other service partners should work with their executive producers and directors to understand the new security requirements, and whether a formal MPAA audit is necessary. Compliance with MPAA guidelines is voluntary, but Microsoft elected to carry out an independent assessment so that media customers can be confident in the content security and protection capabilities of Azure. However, Azure does not manage the individual cloud environments of customers, which may be subject to additional MPAA regulation that is best addressed by your own audit of your environment.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Motion Picture Association of America](#)
- [MPAA Common Guidelines](#)
- [MPAA Application and Cloud Guidelines](#)
- [CSA STAR Azure Self-Assessment](#)
- [Azure Responses to CSA CAIQ v3.0.1](#)
- [Compliance on the Microsoft Trust Center](#)

# National Bank of Belgium (NBB) and the Financial Services and Markets Authority (FSMA)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the NBB and FSMA

The primary financial services regulators in Belgium are the [National Bank of Belgium](#) (NBB) and the [Financial Services and Markets Authority](#) (FSMA).

The NBB is responsible for prudential supervision of credit institutions, insurers, stockbrokers, and other financial organizations. As the central bank of Belgium, the NBB conducts monetary policy for Belgium and contributes to the stability of its financial system. Alongside the NBB, the FSMA supervises Belgian financial markets, financial service providers including investment firms, and supplemental pensions. Its tasks include oversight of the financial information that companies disseminate and the products they offer to consumers and their compliance with the rules of business conduct.

The NBB and FSMA act in concert with the European Banking Authority (EBA), 'an independent EU authority that works to ensure effective and consistent prudential regulation and supervision across the European banking sector.' To that end, the EBA has outlined a comprehensive approach to the use of cloud computing by financial institutions in the EU, [Recommendations on outsourcing to cloud services providers](#).

There are several requirements and guidelines that financial institutions in Belgium should be aware of when moving business functions to the cloud, including:

- NBB Circular PPB 2004/5, Sound management practices in outsourcing by credit institutions and investment firms ([Dutch](#) and [French](#)), and the broadly equivalent provisions of the [FSMA Circular 05-06.2007](#) (French and Dutch) on organizational requirements for firms providing investment services.
- Circular NBB 2009-17, Financial services via the Internet: Prudential requirements ([English](#)), examines outsourcing risks and sets out the requirements for internal control and management of those risks. It also discusses compliance with the financial rules of conduct and the potential impact of cross-border transactions in the cloud.
- Circular NBB 2015-32, Additional prudential expectations regarding operational business continuity, and security of systemically important financial institutions ([Dutch](#) and [English](#)), sets out management and security processes for institutions that play a critical role in the financial system, and whose disruption could jeopardize its proper functioning.

## Microsoft and the NBB and FSMA

To help guide financial institutions in Belgium considering outsourcing business functions to the cloud, Microsoft has published [A compliance checklist for financial institutions in Belgium](#). By reviewing and completing the checklist, financial organizations can adopt Microsoft business cloud services with the confidence that they are complying with applicable regulatory requirements.

When financial organizations in Belgium outsource business functions to the cloud, they must comply with the rules and guidelines of the National Bank of Belgium (NBB) and the Financial Services and Markets Authority (FSMA) within the broad policy framework of the European Banking Authority (EBA).

The Microsoft checklist helps financial firms in Belgium that are conducting due-diligence assessments of Microsoft business cloud services. It includes:

- An overview of the regulatory landscape for context.

- A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to measure compliance against a regulatory framework and provide an internal structure for documenting compliance, and help customers conduct their own risk assessments of Microsoft business cloud services.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Office 365](#)

## How to implement

- [Compliance checklist: Belgium](#): Financial institutions can get help in conducting risk assessments of Microsoft cloud services.
- [Risk Assessment & Compliance Guide](#): Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
- [Financial use cases](#): Use case overviews, tutorials, and other resources to build Azure solutions for financial services.

## Frequently asked questions

### Is regulatory approval required?

No. However, financial institutions must notify the NBB and FSMA in the event of a disruption in an outsourcing arrangement that has the potential to materially impact the institution's business operations, reputation, or profitability, or its ability to manage risk and comply with applicable laws and regulations.

### Are there any mandatory terms that must be included in the contract with the cloud services provider?

Yes. There are specific points that financial institutions must be sure to incorporate in their cloud services contracts. Part 2 of the [Microsoft checklist](#) (page 49) maps these against the sections in the Microsoft contractual documents where they are addressed.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Microsoft Financial Services Compliance Program](#)
- [Microsoft business cloud services and financial services](#)
- [Financial services compliance in Azure](#)
- [Azure Financial Services Cloud Risk Assessment Tool](#)
- [Compliance on the Microsoft Trust Center](#)

# National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

2/5/2021 • 5 minutes to read • [Edit Online](#)

## NIST CSF overview

The National Institute of Standards and Technology (NIST) promotes and maintains measurement standards and guidance to help organizations assess risk. In response to Executive Order 13636 on strengthening the cybersecurity of federal networks and critical infrastructure, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (FICIC) in February 2014.

The main priorities of the FICIC were to establish a set of standards and practices to help organizations manage cybersecurity risk, while enabling business efficiency. The NIST Framework addresses cybersecurity risk without imposing additional regulatory requirements for both government and private sector organizations.

The FICIC references globally recognized standards including NIST SP 800-53 found in Appendix A of the NIST's [Framework for Improving Critical Infrastructure Cybersecurity](#). Each control within the FICIC framework is mapped to corresponding NIST 800-53 controls within the FedRAMP Moderate Baseline.

## Microsoft and the NIST CSF

NIST Cybersecurity Framework (CSF) is a voluntary Framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks. Microsoft Cloud services have undergone independent, third-party FedRAMP Moderate and High Baseline audits and are certified according to the FedRAMP standards. Also, through a validated assessment performed by HITRUST, a leading security and privacy standards development and accreditation organization, Office 365 is certified to the objectives specified in the NIST CSF.

Learn how to accelerate your NIST Cybersecurity Framework deployment with Compliance Score and our Azure Security and Compliance Blueprint:

- [Overview of the NIST SP 800-53 R4 blueprint sample](#)
- [Learn more about the NIST CSF assessment for Office 365 in Compliance Score](#)

## Microsoft in-scope cloud services

- [Azure Government](#)
- [Dynamics 365 for Government](#)
- [Office 365 and Office 365 U.S. Government](#)

## Audit cycle and certification

The NIST CSF certification of Office 365 is valid for two years.

- [Office 365 NIST CSF Letter of Certification](#)

## Quickly build NIST CSF solutions on Azure

The NIST Cybersecurity Framework (CSF) standard can be challenging in the cloud. Fortunately, with Azure you'll have a head start the Azure Security and Compliance NIST CSF Blueprint. This blueprint provides tools and guidance to get you started building NIST CSF-compliant solutions today.

- [Start using the Azure NIST CSF Blueprint](#)

## Perform risk assessment on Office 365 using NIST CSF in Compliance Score

Cybersecurity remains a critical management issue in the era of digital transforming. To help you implement and verify security controls for your Office 365 tenant, Microsoft provides recommended customer actions in the NIST CSF Assessment in Compliance Score.

- [Start using Compliance Score](#)

## Frequently asked questions

**Has an independent assessor validated that Azure Government, Dynamics 365, and Office 365 support NIST CSF requirements?**

Yes, a third-party assessment organization has attested that the Azure Government cloud service offering conforms to the NIST Cybersecurity Framework (CSF) risk management practices, as defined in the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, dated February 12, 2014. The NIST CSF is mapped to FedRAMP Moderate controls framework and an independent assessor has assessed Dynamics 365 against the FedRAMP Moderate baseline. Also, Office 365 obtained [the NIST CSF letter of certification](#) from HITRUST in June 2018.

**How do Microsoft Cloud Services demonstrate compliance with the framework?**

Using the formal audit reports prepared by third parties for the FedRAMP accreditation, Microsoft can show how relevant controls noted within these reports demonstrate compliance with the NIST Framework for Improving Critical Infrastructure Cybersecurity. Audited controls implemented by Microsoft serve to ensure the confidentiality, integrity, and availability of data stored, processed, and transmitted by Azure, Office 365, and Dynamics 365 that have been identified as the responsibility of Microsoft.

**What are Microsoft's responsibilities for maintaining compliance with this initiative?**

Participation in the FICIC is voluntary. However, Microsoft ensures that Azure, Office 365, and Dynamics 365 meet the terms defined within the governing Online Services Terms and applicable service level agreements. These define Microsoft's responsibility for implementing and maintaining controls adequate to secure the Azure platform and monitor the system.

**Can I use Microsoft's compliance for my organization?**

Yes. The independent third-party compliance reports to the FedRAMP standards attest to the effectiveness of the controls Microsoft has implemented to maintain the security and privacy of the Microsoft Cloud Services. Microsoft customers may use the audited controls described in these related reports as part of their own FedRAMP and NIST FICIC's risk analysis and qualification efforts.

**Which organizations are deemed by the United States Government to be critical infrastructure?**

According to the [Department of Homeland Security](#), these include organizations in the following sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear (Reactors Materials and Waste), Transportation Systems and Water (and Wastewater).

**What are the in-scope services for Office 365?**

The in-scope services of NIST CSF certification are Exchange Online Archiving, Exchange Online Protection, Exchange Online, Skype for Business, Admin Center, SharePoint Online, Project Online, OneDrive for Business,

Office Online, MyAnalytics, Microsoft Teams, Microsoft 365 Apps for enterprise in Office 365 Multi-tenant cloud and Office 365 GCC.

#### NOTE

Microsoft 365 Apps for enterprise enables access to various cloud services, such as Roaming Settings, Licensing, and OneDrive consumer cloud storage, and may enable access to additional cloud services in the future. Roaming Settings and Licensing support the standards for HITRUST. OneDrive consumer cloud storage does not, and other cloud services that are accessible through Microsoft 365 Apps for enterprise and that Microsoft may offer in the future also may not, support these standards.\*

### Why are some Office 365 services not in the scope of this certification?

Microsoft provides the most comprehensive offerings compared to other cloud service providers. To keep up with our broad compliance offerings across regions and industries, we include services in the scope of our assurance efforts based on the market demand, customer feedback, and product lifecycle. If a service is not included in the current scope of a specific compliance offering, your organization has the responsibility to assess the risks based on your compliance obligations and determine the way you process data in that service. We continuously collect feedback from customers and work with regulators and auditors to expand our compliance coverage to meet your security and compliance needs.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Microsoft Cloud Services Authorizations](#)
- [Mapping Microsoft Cyber Offerings to: NIST Cybersecurity Framework \(CSF\), CIS Controls, ISO27001:2013 and HITRUST CSF](#)
- [Framework for Improving Critical Infrastructure Cybersecurity](#)
- [Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure](#)
- [Microsoft Government Cloud](#)
- [Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

# Payment Card Industry (PCI) Data Security Standard (DSS)

2/5/2021 • 5 minutes to read • [Edit Online](#)

## PCI DSS overview

The Payment Card Industry (PCI) Data Security Standards (DSS) is a global information security standard designed to prevent fraud through increased control of credit card data. Organizations of all sizes must follow PCI DSS standards if they accept payment cards from the five major credit card brands, Visa, MasterCard, American Express, Discover, and the Japan Credit Bureau (JCB). Compliance with PCI DSS is required for any organization that stores, processes, or transmits payment and cardholder data.

## Microsoft and PCI DSS

Microsoft completed an annual PCI DSS assessment using an approved Qualified Security Assessor (QSA). The auditors reviewed Microsoft Azure, Microsoft OneDrive for Business, and Microsoft SharePoint Online environments, which include validating the infrastructure, development, operations, management, support, and in-scope services. The PCI DSS designates four levels of compliance based on transaction volume. Azure, OneDrive for Business, and SharePoint Online are certified as compliant under PCI DSS version 3.2 at Service Provider Level 1 (the highest volume of transactions, more than 6 million a year).

The assessment results in an Attestation of Compliance (AoC), which is available to customers and Report on Compliance (RoC) issued by the QSA. The effective period for compliance begins upon passing the audit and receiving the AoC from the assessor and ends one year from the date the AoC is signed.

Customers who want to develop a cardholder environment or card processing service can use these validations in many of the underlying portions, thereby reducing the associated effort and costs of getting their own PCI DSS certification.

It is important to understand that PCI DSS compliance status for Azure, OneDrive for Business, and SharePoint Online not automatically translate to PCI DSS certification for the services that customers build or host on these platforms. Customers are responsible for ensuring that they achieve compliance with PCI DSS requirements.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Microsoft Cloud App Security
- Flow cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Microsoft Graph
- Intune
- [Microsoft Defender Advanced Threat Protection](#)
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- OneDrive for Business and SharePoint Online (United States only)

## Audit, reports, and certificates



- [Azure PCI DSS Attestation of Compliance \(AoC\)](#)
- [OneDrive for Business and SharePoint Online PCI DSS Attestation of Compliance \(AoC\)](#)

## Get your PCI DSS solution running on Azure

Build and deploy your PCI DSS solution in the cloud even faster with the Azure Security and Compliance PCI DSS Blueprint. Get reference architectures, deployment guidance, control implementation mappings, automated scripts and more. [Start using the Azure PCI DSS Blueprint.](#)

## Frequently asked questions

### **Why does the Attestation of Compliance (AoC) cover page say 'June 2018'?**

The June 2018 date on the cover page is when the AoC template was published. Refer to Section 2 for the date of the assessment.

### **Why are there multiple Azure Attestations of Compliance (AoCs)?**

The Azure AoC package has AoCs corresponding to Azure Public, Germany, and Government cloud. Customers should use the AoC that corresponds with their Azure environment.

### **What is the relationship between the PA DSS and PCI DSS?**

The Payment Application Data Security Standard (PA DSS) is a set of requirements that comply with the PCI DSS, and replaces Visa's Payment Application Best Practices, and consolidates the compliance requirements of the other primary card issuers. The PA DSS helps software vendors develop third-party applications that store, process, or transmit cardholder payment data as part of a card authorization or settlement process. Retailers must use PA DSS certified applications to efficiently achieve their PCI DSS compliance. The PA DSS does not apply to Azure.

### **What is an acquirer and does Azure use one?**

An acquirer is a bank or other entity that processes payment card transactions. Azure does not offer payment card processing as a service and thus does not use an acquirer.

### **To what organizations and merchants does the PCI DSS apply?**

PCI DSS applies to any company, no matter the size, or number of transactions, that accepts, transmits, or stores cardholder data. That is, if any customer ever pays a company using a credit or debit card, then the PCI DSS requirements apply. Companies are validated at one of four levels based on the total transaction volume over a 12-month period. Level 1 is for companies that process over 6 million transactions a year; Level 2 for 1 million to 6 million transactions; Level 3 is for 20,000 to 1 million transactions; and Level 4 is for fewer than 20,000 transactions.

### **Where do I begin my organization's PCI DSS compliance efforts for a solution deployed on Azure?**

The information that the PCI Security Standards Council makes available is a good place to learn about specific compliance requirements. The council publishes the [PCI DSS Quick Reference Guide](#) for merchants and others involved in payment card processing. The guide explains how the PCI DSS can help protect a payment card transaction environment and how to apply it.

Compliance involves several factors, including assessing the systems and processes not hosted on Azure. Individual requirements vary based on which Azure services are used and how they are employed within the solution.

### **Are there plans for OneDrive for Business and SharePoint Online to be PCI DSS-compliant outside of the United States?**

Currently OneDrive for Business and SharePoint Online is PCI-DSS compliant only in the United States (US). Microsoft will evaluate the requirements and timelines for regions outside of US and provide updates when and if other regions are added to the roadmap.

### **What is in-scope for OneDrive for Business and SharePoint Online?**

Currently, only files and documents uploaded to OneDrive for Business and SharePoint Online will be compliant with PCI DSS.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [PCI Security Standards Council](#)
- [PCI Data Security Standard](#)
- [Azure PCI DSS 3.2.1 Blueprint](#)
- [PCI DSS Quick Reference Guide](#)
- [Compliance on the Microsoft Trust Center](#)

# U.S. Section 508

11/30/2020 • 2 minutes to read • [Edit Online](#)

## About U.S. Section 508

The United States Congress amended the Rehabilitation Act in 1998 and 2000 to require federal agencies to make their electronic and information technology (EIT) products, such as software, hardware, electronic content, and support documentation, accessible to people with disabilities. Section 508 of the United States Workforce Rehabilitation Act of 1973 (29 US Code §794d), as amended, mandates that federal agencies procure, maintain, and use EIT in a manner that ensures federal employees with disabilities have comparable access to, and use of, data and EIT relative to other federal employees.

Microsoft is a major software and cloud-services provider to U.S. federal and state governments. To assist government customers in making procurement decisions, Microsoft publishes Accessibility Conformance Reports describing the extent to which our products and services support the criteria of Section 508. This information can help Microsoft customers determine whether a particular product or service will meet their specific needs.

## Microsoft and U.S. Section 508

Microsoft's consideration of U.S. Section 508 in the development of products and services points to its commitment to making technology and data accessible for all customers.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Azure DevOps Services
- Dynamics 365 and Dynamics 365 U.S. Government
- Intune
- [Office 365 and Office 365 U.S. Government](#)
- [Office 365 U.S. Government Defense](#)
- Windows Server 2016

## Microsoft accessibility conformance reports

Find [conformance reports](#) for all our products and services.

## Resources

- [Microsoft accessibility page](#): Explore the ways in which Microsoft innovates so everyone has the ability to achieve more.
- [Office 365 Accessibility Center](#): Office 365 resources for people with disabilities.
- [Enterprise Disability Answer Desk](#): Dedicated support for enterprise customers with accessibility questions about our products and services or compliance.
- [DHS Trusted Tester Program](#): Get information about the U.S. Department of Homeland Security (DHS) Trusted Tester Program, in which Microsoft participates.
- [Compliance on the Microsoft Trust Center](#)

# Shared Assessments Program

11/30/2020 • 2 minutes to read • [Edit Online](#)

## About Shared Assessments

[Shared Assessments](#), managed by [The Santa Fe Group](#), is a program used by many commercial, retail, and investment banks around the world as a proxy for managing their third-party vendor risk assessment process. It publishes (and updates) instruments and a process that standardize the approach for member organizations to assess a CSP's controls for people, processes, and procedures and offers a process to validate the accuracy of the information in the CSP's report. Two tools are central to the program:

- The Standardized Information Gathering (SIG) questionnaire is used to perform an initial assessment of vendors, gathering information to determine how security risks are managed across 18 domains within a CSP's environment. With a single standard set of questions for every vendor, it streamlines the assessment of CSPs thus making comparisons more straightforward and efficient.
- The Standardized Control Assessment uses a set of objective procedures to help organizations validate a CSP's answers to the SIG through onsite testing and other verification assessments.

## Microsoft and Shared Assessments

The Shared Assessments Program is based on a wide body of US and global industry-accepted security standards, regulations, and control frameworks, including the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v3.0.1. The CCM is a controls framework covering fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a cloud service provider (CSP). These map to the 18 risk control areas (domains) that the Shared Assessments Standardized Information Gathering (SIG) questionnaire uses.

For the CSA STAR self-assessment, Microsoft submitted a report documenting Microsoft Azure and Microsoft Azure Government compliance with the CCM. (Microsoft also publishes a completed Consensus Assessments Initiative Questionnaire (CAIQ) for Azure.) Based on that self-assessment, Azure and Azure Government align with the SIG questionnaire and the Agreed Upon Procedures (AUP) v5.0.

Azure compliance is listed on the CSA STAR Registry, a free publicly accessible registry where CSPs publish their CSA-related assessments. There, Azure also maintains formal CSA STAR Certification and CSA STAR Attestation.

Because these self-assessment reports are publicly available, Azure customers gain visibility into Microsoft security practices and can compare various CSPs using the same baseline.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)

## Audits, reports, and certificates

Based on a self-assessment, Microsoft has documented Azure and Azure Government compliance with the CSA CCM framework, thus aligning it with the Shared Assessments program.

- [CSA STAR Registry](#)

## Resources

- [Azure standard response for request for information](#)
- [Microsoft and the CSA STAR Self-Assessment](#)
- [Compliance on the Microsoft Trust Center](#)

# Service Organization Controls (SOC)

2/17/2021 • 5 minutes to read • [Edit Online](#)

## SOC 1, 2, and 3 Reports overview

Increasingly, businesses outsource basic functions such as data storage and access to applications to cloud service providers (CSPs) and other service organizations. In response, the American Institute of Certified Public Accountants (AICPA) has developed the Service Organization Controls (SOC) framework, a standard for controls that safeguard the confidentiality and privacy of information stored and processed in the cloud. This aligns with the International Standard on Assurance Engagements (ISAE), the reporting standard for international service organizations.

Service audits based on the SOC framework fall into two categories — SOC 1 and SOC 2 — that apply to in-scope Microsoft cloud services.

A SOC 1 audit, intended for CPA firms that audit financial statements, evaluates the effectiveness of a CSP's internal controls that affect the financial reports of a customer using the provider's cloud services. The Statement on Standards for Attestation Engagements (SSAE 18) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) are the standards under which the audit is performed, and is the basis of the SOC 1 report.

A SOC 2 audit gauges the effectiveness of a CSP's system based on the AICPA Trust Service Principles and Criteria. An Attest Engagement under Attestation Standards (AT) Section 101 is the basis of SOC 2 and SOC 3 reports.

At the conclusion of a SOC 1 or SOC 2 audit, the service auditor renders an opinion in a SOC 1 Type 2 or SOC 2 Type 2 report, which describes the CSP's system and assesses the fairness of the CSP's description of its controls. It also evaluates whether the CSP's controls are designed appropriately, were in operation on a specified date, and were operating effectively over a specified time period.

Auditors can also create a SOC 3 report — an abbreviated version of the SOC 2 Type 2 audit report — for users who want assurance about the CSP's controls but don't need a full SOC 2 report. A SOC 3 report can be conferred only if the CSP has an unqualified audit opinion for SOC 2.

## Microsoft and SOC 1, 2, and 3 Reports

Microsoft covered cloud services are audited at least annually against the SOC reporting framework by independent third-party auditors. The audit for Microsoft cloud services covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.

Microsoft has achieved SOC 1 Type 2, SOC 2 Type 2, and SOC 3 reports. In general, the availability of SOC 1 and SOC 2 reports is restricted to customers who have signed nondisclosure agreements with Microsoft; the SOC 3 report is publicly available.

## Microsoft in-scope cloud services

### Covered services for SOC 1 and SOC 2

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- [Dynamics 365 and Dynamics 365 U.S. Government](#)
- Microsoft Graph

- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- Microsoft Stream
- Azure DevOps Services

### **Covered services for SOC 3**

- [Azure, Azure Government, and Azure Germany](#)
- Microsoft Cloud App Security
- Microsoft Graph
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](#)
- Power BI
- Microsoft Stream

## Audits, reports, and certificates

### **Audit cycle**

Microsoft cloud services are audited at least annually against SOC 1 (SSAE18, ISAE 3402), SOC 2 (AT Section 101), and SOC 3 standards.

### **Azure, Dynamics 365, Microsoft Cloud App Security, Flow, Microsoft Graph, Intune, Power BI, PowerApps, Microsoft Stream, and Microsoft Datacenters**

- [Azure + Dynamics 365 and Azure + Dynamics 365 Government SOC 1 Type 2 Report](#)
- [Azure + Dynamics 365 and Azure + Dynamics 365 Government SOC 2 Type 2 Report](#)
- [Azure + Dynamics 365 and Azure + Dynamics 365 Government SOC 3 Report](#)

### **Office 365**

- [Office 365 Core - SSAE 18 SOC 1 Report](#)
- [Office 365 Core - SSAE 18 SOC 2 Report](#)
- [Office 365 Core - SSAE 18 SOC 3 Report](#)
- [Office 365 Microservices T1-SSAE 18 SOC2 Type I Report](#)
- [Customer Lockbox SOC 1 SSAE 16 Audit Report](#)
- [Yammer SOC 2 AT 101 Type I Audit Report](#)
- [Yammer SOC 2 Type II Report](#)
- [See bridge letters and additional audit reports](#)

## Frequently asked questions

How can I get copies of the SOC reports?

With the reports, your auditors can compare Microsoft business cloud services results with your own legal and regulatory requirements.

- You can see all SOC reports through the [Service Trust Platform](#).
- Azure DevOps Service customers that can't access [Service Trust Platform](#) can email [Azure DevOps](#) for its SOC 1 and SOC 2 reports. This email is to request Azure DevOps SOC reports only.

#### How often are Azure SOC reports issued?

SOC reports for Azure, Microsoft Cloud App Security, Flow, Microsoft Graph, Intune, Power BI, PowerApps, Microsoft Stream, and Microsoft Datacenters are based on a rolling 12-month run window (audit period) with new reports issued semi-annually (period ends are March 31 and September 30). Bridge letters are issued each quarter to cover the prior three month period. For example, the January letter covers 10/1-12/31, the April letter covers 1/1-3/31, the July letter covers 4/1-6/30, and the October letter covers 7/1-9/30. Customers can [download](#) the latest reports from the Service Trust Portal.

#### Do I need to conduct my own audit of Microsoft datacenters?

No. Microsoft shares the independent audit reports and certifications with customers so that they can verify Microsoft compliance with its security commitments.

#### Can I use Microsoft's compliance in my organization's certification process?

Yes. When you migrate your applications and data to covered Microsoft cloud services, you can build on the audits and certifications that Microsoft holds. The independent reports attest to the effectiveness of controls that Microsoft has implemented to help maintain the security and privacy of your data.

#### Where do I start with my organization's own compliance effort?

The [SOC Toolkit for Service Organizations](#) is a helpful resource for understanding SOC reporting processes and promoting your organization's use of them.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Better protect your data by using Microsoft cloud services](#)
- [Service Organization Control \(SOC\) Reports](#)
- [SSAE 16 Overview](#)
- [ISAE 3402 Overview](#)
- [Microsoft Online Services Terms](#)
- [Microsoft Government Cloud](#)
- [Compliance on the Microsoft Trust Center](#)



# Spanish Royal Decree 1720/2007, Spanish Organic Law 15/1999

11/30/2020 • 2 minutes to read • [Edit Online](#)

## Spanish Royal Decree 1720/2007, Spanish Organic Law 15/1999 overview

The AEPD is the public authority that oversees compliance with Spanish Organic Law 15/1999 for the Protection of Personal Data ([Ley Orgánica 15/1999 de Protección de Datos](#), or LOPD), including the transfer of data across international boundaries. In 2014, the AEPD reviewed Microsoft's terms and conditions applicable to the EU Model Clauses-covered Microsoft Azure, Dynamics 365, and Office 365, and issued a resolution determining that those terms provided adequate safeguards for customers to move their personal data to those services.

Title VIII of Royal Decree 1720/2007 establishes stringent requirements for processing personal data, including a specific listing of basic, intermediate-level, and high-level security measures that must be implemented. Microsoft retained an independent third-party auditing firm in Spain, BDO Auditores, to assess Microsoft Azure and Office 365 for compliance with the high-level requirements and Microsoft Dynamics 365 for compliance with the intermediate-level requirements established in Royal Decree 1720/2007. Based on interviews, visits to facilities, and a review of the environmental and physical security measures and controls, the auditor determined that Microsoft Azure and Office 365 information systems, facilities, and data processing met the high-level standard with no points requiring correction.

## Microsoft and Spanish Royal Decree 1720/2007, Spanish Organic Law 15/1999

Microsoft was the first hyper-scale cloud service provider to receive, for the benefit of its customers, an authorization from the Spanish Data Protection Agency (Agencia Española de Protección de Datos, or AEPD) for its compliance with the high standards governing international data transfer under Spanish Organic Law 15/1999 ([Ley Orgánica 15/1999 de Protección de Datos](#), or LOPD). Microsoft is also the first hyper-scale cloud service provider to obtain a third-party audit certification for its online services' compliance with the security measures set forth in Title VIII of Royal Decree 1720/2007. This authorization lets customers make transfers of personal data to Microsoft Azure, Dynamics 365, and Office 365 services covered by the European Union Model Clauses.

## Microsoft in-scope cloud services

- [Microsoft Azure](#)
- [Microsoft Dynamics 365](#)
- Intune
- [Microsoft Office 365](#)

## Audits, reports, and certificates

### Microsoft Azure

- [Certification](#) (Spanish)
- [Audit report](#) (Spanish)

### Microsoft Office 365

- [Certification](#) (Spanish)
- [Audit report](#) (Spanish)

### **Microsoft Dynamics 365**

- [Audit report](#) (Spanish)
- [Audit report](#) (English)

## Frequently asked questions

### **How does meeting the high-level standard benefit Microsoft customers?**

The high-level standard applies to the processing of sensitive data such as health information. Customers who use Microsoft Azure and Office 365 can rest assured that their sensitive data is being processed in accordance with Royal Decree 1720/2007.

### **Can I use Microsoft's compliance in my organization's certification process?**

Yes. If your organization requires or is seeking an accreditation in line with the LOPD or Royal Decree 1720/2007, you can use AEPD's authorization and the security measures certification in your compliance assessment. However, you are responsible for engaging an assessor to evaluate your implementation as deployed on Microsoft Azure, Dynamics 365, or Office 365, and for the controls and processes within your own organization.

## Resources

- Spanish Data Protection Agency ([Spanish](#))
- Organic Law 15/1999 of December 13 for the Protection of Personal Data - [Spanish](#)
- [Microsoft Online Services terms](#)
- [Compliance on the Microsoft Trust Center](#)

# United Kingdom Cyber Essentials PLUS

2/5/2021 • 2 minutes to read • [Edit Online](#)

## UK Cyber Essentials PLUS overview

Cyber Essentials is a UK government-backed scheme designed to help organizations assess and mitigate risks from common cyber security threats to their IT systems. The Cyber Essentials scheme is a cyber security standard that identifies security controls for an organization to have in place within their IT systems. Cyber Essentials scheme is a requirement for all UK government suppliers handling any personal data. The Cyber Essentials badge helps an organization demonstrate the ability to:

- Identify potential risks to help organizations better protect against common cyber threats.
- Demonstrate an organization has adopted the proper security controls to protect customer data.
- Become compliant with UK government expectations for Cyber Security Essential requirements and eligible to bid for UK government contracts.

The Cyber Essentials scheme is designed for UK government suppliers to identify potential weaknesses in their IT systems and software that could exploit customer data. The methodology has defined two different levels of certification:

- Cyber Essentials is the first level and includes a self-assessment for organizations to check the most important IT security controls of their IT infrastructure. The responses are independently reviewed by an external certifying body.
- Cyber Essentials PLUS offers the same controls coverage as Cyber Essentials and also includes additional assurance by carrying out systems tests of implemented controls through an authorized third-party certifying body.

## Microsoft and UK Cyber Essentials PLUS

Microsoft Azure has attained Cyber Essentials PLUS badge and meets the requirements outlined in the [Cyber Essentials Scheme](#). Azure production systems are frequently tested and audited to provide evidence of a world-leading compliance portfolio.

The [Azure Cyber Essentials PLUS certification](#), which applies to our global operation of Azure, is available for download.

## Audits, reports, and certificates

- [Azure Cyber Essentials PLUS compliance report](#)
- [Azure Cyber Essentials PLUS certification](#)

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Cyber Essentials Scheme: Assurance framework](#)

- [Compliance on the Microsoft Trust Center](#)

# United Kingdom Government-Cloud (G-Cloud)

2/5/2021 • 4 minutes to read • [Edit Online](#)

## UK G-Cloud overview

Government Cloud (G-Cloud) is a UK government initiative to ease procurement of cloud services by government departments and promote government-wide adoption of cloud computing. G-Cloud comprises a series of framework agreements with cloud services suppliers (such as Microsoft), and a listing of their services in an online store, the Digital Marketplace. These enable public-sector organizations to compare and procure those services without having to do their own full review process. Inclusion in the Digital Marketplace requires a self-attestation of compliance, followed by a verification performed by the Government Digital Service (GDS) branch at its discretion.

The G-Cloud appointment process was streamlined in 2014 to reduce the time and cost to the UK government, and the government's security classification scheme was simplified from six to three levels: OFFICIAL, SECRET, and TOP SECRET. (G-Cloud certification levels are no longer expressed as an Impact Level, or IL; Microsoft formerly held an IL2 accreditation for Microsoft Azure, Microsoft Dynamics 365, and Microsoft Office 365.)

Instead of the central assessment of cloud services previously provided, the new process requires cloud service providers to self-certify and supply evidence in support of the 14 Cloud Security Principles of G-Cloud. This has not changed either the evidence Microsoft produces or the standards that the company adheres to.

## Microsoft and UK G-Cloud

Every year, Microsoft prepares documentation and submits evidence to attest that its in-scope enterprise cloud services comply with the principles, giving potential G-Cloud customers an overview of its risk environment. (As with previous G-Cloud accreditation, it relies on the ISO 27001 certification.) A GDS accreditor then performs several random checks on the Microsoft assertion statement, samples the evidence, and makes a determination of compliance.

The appointment of Microsoft services to the Digital Marketplace means that UK government agencies and partners can use in-scope services to store and process UK OFFICIAL government data, most government data. In addition, there are now more than 450 Microsoft partners included in G-Cloud who are resellers of Microsoft cloud services. They can directly assert the compliance of in-scope services with the 14 principles in their own applications. Customers and partners, however, will need to achieve their own compliance for any components that are not included in the attestation and determination of compliance for Microsoft cloud services.

[14 Cloud Security Controls for UK cloud using Microsoft Azure](#) provides customer strategies to move their services to Azure and help meet their UK obligations mandated by the CESG/NSCS. The whitepaper provides insight into how Azure can be used to help address the 14 controls outlined in the cloud security principals, and outlines how customers can move faster and achieve more while saving money as they adopt Microsoft Azure services.

## Microsoft in-scope cloud services

- [Azure](#)
- Microsoft Cloud App Security
- [Dynamics 365](#)
- Intune
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an

- Office 365 or Dynamics 365 branded plan or suite
- Office 365: Exchange Online, SharePoint Online, and Skype for Business Online
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Audits, reports, and certificates

To confirm that Microsoft cloud services maintain their compliance with G-Cloud agreements, the GDS accreditor may review evidence at any time, at its discretion.

### Azure

- [Azure UK G-Cloud Risk Environment](#)
- [Azure UK G Cloud Residual Risk](#)
- [Intune UK G Cloud Security Cloud Assessment Summary](#)

### Dynamics 365

- [Dynamics 365 UK G cloud Risk Environment](#)

### Intune

- [Intune UK G cloud Risk Environment](#)
- [Intune UK G cloud Residual Risk](#)
- [Azure UK G cloud Security Assessment Summary](#)

### Office 365

- [Office 365 UK G cloud Risk Environment](#)

## Accelerate your deployment of UK G-Cloud solutions on Azure

Moving your government services to the cloud is now easier than ever using the Azure Security and Compliance UK Blueprint. This blueprint provides guidance and automated scripts that get you started building compliant solutions today.

[Start using the Azure UK G-Cloud Blueprint](#)

## Frequently asked questions

### Who is eligible to use the Digital Marketplace?

All UK government departments, devolved administrations, local authorities, wider public-sector bodies, and arm's-length bodies are eligible to buy services in the marketplace. If you're uncertain of your eligibility, consult the [complete list of public-sector organizations](#).

### What is an arm's-length body?

It is an organization or agency that is funded by the UK government but acts independently of it.

### What do local datacenter locations mean for UK customers, and where are they located?

The Microsoft Cloud in the UK provides reliability and performance combined with data residency in the UK. This support provides customers with trusted cloud services that help them meet local compliance and policy requirements. In addition, replication of data in multiple datacenters across the UK gives customers geo-redundant data protection for business continuity, for both pure cloud and hybrid scenarios. We have datacenters in multiple locations across the UK.

- You can see the new Azure regions, UK West, and UK South, on the [global Azure map](#).

- For Office 365, the UK datacenters collectively comprise the new UK Office 365 region. You can see more on the [global Office 365 map](#).

### **Where are the other Microsoft EU datacenters located?**

In addition to the UK datacenters, Microsoft cloud services has data centers in multiple locations. For the most up-to-date list of all centers visit our [data location page](#).

### **How can I get copies of the auditor's reports?**

The [Service Trust Portal](#) provides independently audited compliance reports. You can use the portal to request audit reports so that your auditors can compare the Microsoft results with your own legal and regulatory requirements.

## **Resources**

- [Effective Compliance Controls to Address the UK Governments Common 14 Cloud Security Principles Using Microsoft Azure](#)
- [UK Government Cloud Strategy](#)
- [G-Cloud Security Principles](#)
- [Digital Marketplace](#)
- [Microsoft Online Services](#)
- [Compliance on the Microsoft Trust Center](#)

# Association of Banks in Singapore (ABS) Outsourced Service Provider's Audit Report (OSPAR)

2/17/2021 • 2 minutes to read • [Edit Online](#)

## ABS OSPAR overview

When financial Institutions outsource business functions, they must ensure that their service providers maintain the same level of governance, rigor, and consistency as if the financial institutions managed it themselves.

To that end, the [Association of Banks in Singapore](#) (ABS), a non-profit organization representing the interests of local and foreign banks operating in Singapore, has issued [ABS Guidelines on Control Objectives and Procedures for Outsourced Service Providers](#) (or, ABS Guidelines). The ABS Guidelines set out information security guidance for service providers who deliver services to financial institutions operating in Singapore. The guidelines specify the baseline organizational controls that service providers must implement in cloud outsourcing arrangements, particularly for material workloads. The Outsourced Service Provider's Audit Report (OSPAR) is the framework that external auditors use to validate the service provider's controls against the criteria specified in the ABS Guidelines.

## Microsoft and ABS OSPAR

An independent service auditor, performed a rigorous audit of the security capabilities of Microsoft Azure and Microsoft Dynamics 365, which include more than 120 Azure services and 10 Dynamics 365 applications, to assess their compliance with the ABS Guidelines.

The auditor attested that the security controls of Azure and Dynamics 365 were suitably designed to meet the applicable ABS controls criteria and operated effectively during the year-long testing period.

Achieving this ABS OSPAR attestation demonstrates that the set of security controls of Microsoft in-scope services meet the ABS Guidelines, putting these services on the official list, [OSPAR Audited Outsourced Service Providers](#). This, in turn, provides assurance to financial services customers with facilities in Singapore that Microsoft meets these high standards for deploying compliant financial services solutions.

## Microsoft and in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- Intune
- Microsoft Cloud App Security
- Microsoft Graph
- [Microsoft Managed Desktop](#)
- Microsoft Stream
- PowerApps cloud service: either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power Automate: either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service: either as a standalone service or as included in an Office 365 branded plan or suite
- Power Virtual Agents



# Audits, reports, and certificates

The audit is usually performed once every 12 months.

[Microsoft Azure and Dynamics 365 OSPAR Report \(2020\)](#)

## Frequently asked questions

### **What is a 'material' outsourcing arrangement and why is the definition important?**

An outsourcing arrangement is 'material' if a service failure or breach has the potential to materially affect a financial firm's business operations or ability to manage risk and comply with applicable laws and regulations; or if it involves customer information, and any unauthorized access or disclosure, loss, or theft of customer information, has a material impact on a firm's customers. The definition of 'customer information' expressly excludes securely encrypted information.

This definition is important because certain provisions of MAS Outsourcing Guidelines apply only to 'material outsourcing arrangements'. These provisions include an obligation to perform annual reviews, mandatory contractual clauses addressing audit rights, and ensuring that outsourcing outside of Singapore does not affect MAS supervisory efforts.

## Resources

### **ABS OSPAR resources**

- [ABS Guidelines for Outsourced Service Providers](#)
- [Compliance Checklist for Financial Institutions in Singapore](#)
- [Microsoft and the Monetary Authority of Singapore \(MAS\) and Association of Banks in Singapore \(ABS\)](#)

### **Other Microsoft resources for financial services**

- [Microsoft Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)

# Cloud Security Mark Gold (CS Gold Mark)

11/30/2020 • 2 minutes to read • [Edit Online](#)

## CS Gold Mark overview

The Cloud Security Mark (CS Mark) is the first security standard for cloud service providers (CSPs) in Japan, and is based on ISO/IEC 27017, the international code of practice for information security controls. This in turn is based on ISO/IEC 27002 for cloud services, which address information security in cloud computing and the implementation of cloud-related information security controls.

The CS Mark is accredited by the Japan Information Security Audit Association (JASA), a nonprofit organization established by the Ministry of the Interior and the Ministry of Economy, Trade, and Industry to strengthen information security in Japan. The CS Mark promotes the use of cloud services and provides:

- A common standard that CSPs can apply to address common customer concerns about the security and confidentiality of data in the cloud and the impact on business of using cloud services.
- Verifiable operational transparency and visibility into the risks that customers face when they use cloud services.
- Objective criteria that enterprises and government can use to choose a CSP, and clarification of the security requirements that CSPs must follow to be accredited.

JASA developed the Authorized Information Security Audit System (AISAS), which specifies the audit of approximately 1,500 controls covering such areas as organization for information, physical, and development security; the security of human resources; and business continuity, disaster recovery, and incident management. The AISAS offers CS Gold Mark accreditation that requires an independent auditor authorized by JASA to perform a stringent audit. A CS Gold Mark means that in-scope services can host important government data.

## Microsoft and CS Gold Mark

After rigorous assessments by a JASA-certified auditor, Microsoft received the CS Gold Mark for all three service classifications. Accreditations were granted for Microsoft Azure Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), and for Microsoft Office 365 Software as a Service (SaaS). Microsoft was the first global CSP to receive this accreditation across all three classifications.

## Microsoft in-scope cloud services

- [Azure](#)
- [Intune](#)
- [Office 365](#)

## Audits, reports, and certificates

Accreditation is valid for three years, with a yearly surveillance audit to be conducted.

- [CS Gold Mark for Azure and Office 365](#) (Japanese)

## Frequently asked questions

**Where do I start with my organization's own compliance effort?**

If your organization is using Azure or Office 365, you need to ensure that the CS Mark addresses your own

security requirements. If CS Mark does address your security requirements, then you can use the Microsoft accreditation and audit report as part of your own accreditation process. You are responsible for engaging an auditor to evaluate your implementation for compliance, and for the controls and processes within your own organization.

## Resources

- [CS Mark Accreditation Scheme](#) (Japanese)
- [CS Mark Standard accreditation rules](#) (Japanese)
- [CS Mark accreditation forms and templates](#) (Japanese)
- [ISO/IEC 27017: 2015](#)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

# Korea-Information Security Management System (K-ISMS)

11/30/2020 • 4 minutes to read • [Edit Online](#)

## About K-ISMS

Under Article 47 in the “Act on Promotion of Information and Communications Network Utilization and Information Protection” ([Korean](#) and [English](#)), the Korean government introduced the [Korea-Information Security Management System](#) (K-ISMS). A country-specific ISMS framework, it defines a stringent set of control requirements designed to help ensure that organizations in Korea consistently and securely protect their information assets.

To obtain the certification, a company must undergo an assessment by an independent auditor that covers both information security management and security countermeasures. It covers 104 criteria including 12 control items in 5 sectors for information security management, and 92 control items in 13 sectors for information security countermeasures. Some of these include examination of the organization’s security management responsibilities, security policies, security training, incident response, risk management, and more. A special committee examines the results of the audit and grants the certification.

The K-ISMS framework is built on successful information security strategies and policies, as well as security counter measures and threat response procedures to minimize the impact of any security breaches. These have a significant overlap with ISO/IEC 27001 control objectives but are not identical. K-ISMS is more a detailed investigation against requirements than it is a general ISO/IEC 27001 assessment.

Under the supervision of the Korean Ministry of Science and Information Technology (MSIT) ([Korean](#) and [English](#)), the Korea Internet & Security Agency (KISA) ([Korean](#) and [English](#)) is the certifying authority of the K-ISMS. Certification is valid for three years, and certified entities must pass an annual audit to maintain it.

## Microsoft and K-ISMS

Based on a rigorous evaluation by the Korea Internet & Security Agency (KISA), Microsoft Azure achieved the Korea Information Security Management System (K-ISMS) certification to host data. The certification covers Azure services that encompass compute, storage, networking, databases, and security, and the datacenter infrastructure of the Microsoft Korea Central and Korea South regions. The specifications for K-ISMS certification are based on ISO/IEC 27001, ISO/IEC 27018, and other international standards that govern the hosting of data.

Achieving this certification means that Azure customers in Korea can more easily demonstrate adherence to local legal requirements to protect key digital information assets and meet KISA compliance standards more easily. In addition, Korean organizations that have a legislated mandate to obtain their own K-ISMS certification — certain internet and information network service providers, large hospitals and schools, and so on — can more efficiently meet their own KISMS compliance requirements by building on the Azure certification.

The audit covered the measures Microsoft takes to secure data and protect its confidentiality including the:

- Certification of Microsoft business cloud services (with annual audits for compliance) to [ISO/IEC 27001:2013 Information Security Management Standards](#).
- High level of privacy protection based on Microsoft compliance with the [ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud](#).
- Layered approach in how Microsoft datacenters are designed, built, and operated to strictly control physical access to the areas where customer data is stored.

# Microsoft in-scope cloud services

- [Azure](#)
- Intune

## Audits, reports, and certificates

Azure certification is effective for three years from the certification date (19 November 2018) with an annual reassessment by KISA, the certifying body.

- [Azure K-ISMS certification](#) (Korean)

## Frequently asked questions

### Who must obtain the K-ISMS certification?

There are voluntary and compulsory subjects. Voluntary subjects, like Microsoft, apply for K-ISMS certification if they wish. However, KISA mandates certification for compulsory subjects that include:

- Internet service providers that are authorized by Article 6, Section 1 of the Telecommunication Business Act and provide information network services in Seoul and all metropolitan cities.
- Internet datacenters designated as an “integrated information and communication facilities” by Article 46 in the Act on Promotion of Information and Communications Network Utilization and Information Protection.
- Any organization that meets these conditions:
  - Hospitals categorized as a “higher general hospital” in Article 3, Section 4 of the Medical Service Act whose annual sales or tax revenue is at least USD\$ 150 million.
  - Schools, per Article 2 in the Higher Education Act, where the number of enrolled students is at least 10,000 as of December 31 of the immediately preceding year.
  - Information network service providers whose sales of information and communication services are at least USD\$ 10 million or an average of at least 1 million users per day in the previous three months; excluding, however, a financial company under subparagraph 3 of Article 2 of the Electronic Financial Transactions Act.

### How does the integration of the K-ISMS and K-PIMS impact the Microsoft certification?

In November 2018, the MSIT, Korea Communications Commission, and Ministry of the Interior and Safety merged the K-ISMS and the Korea-Personal Information Management System (K-PIMS) into a new certification system, Information Security Management System-Personal (ISMS-P).

The integration of these two systems reflects the recent trends in the integration of information security and the protection of personal information. The goal was both to strengthen the links between these systems and to reduce the compliance burden on organizations due to the considerable overlap of requirements. Instead of 104 K-ISMS controls and 82 K-PIMS controls, the new consolidated certification has 80 items related to information security and 22 items related to the protection of personal information.

Organizations can apply for the K-ISMS certification based on the 80 controls for information security, or they can apply for the ISMS-P by complying with the 22 additional requirements for personal information protection. Microsoft can apply for an audit under the new ISMS-P certification system. However, we wait until our current K-ISMS certification expires in 2021, at which point we apply for an ISMS-P audit.

## Additional resources

- [K-ISMS-certified organizations](#) (Korean)

- [K-ISMS documents and guidelines \(Korean\)](#)
- [Azure Regions](#)
- [Compliance on the Microsoft Trust Center](#)

# Ministry of Electronics and Information Technology (MeitY)

11/30/2020 • 2 minutes to read • [Edit Online](#)

## MeitY overview

The Ministry of Electronics and Information Technology (MeitY), an agency of the government of India, provides policy guidelines to all government and state public sector organizations. Its guidelines are also frequently adopted by private sector organizations in regulated industries, like financial services and telecommunications.

MeitY provides accreditation (referred to by MeitY as 'empanelment') of cloud service providers, which requires that cloud services be certified as compliant against a predefined set of standards and guidelines on security, interoperability, data portability, service level agreement, and contractual terms and conditions. Auditors accredited by MeitY verify compliance by conducting audits of cloud service providers.

Once accredited, cloud service providers are listed in a government cloud services directory where public sector organizations can compare and procure accredited cloud services. The directory is a service of the [MeghRaj Cloud Initiative](#) (or GI [Government of India] Cloud), which promotes the use of cloud computing in government, and governs the implementation of public sector IT services.

## Microsoft and Ministry of Electronics and Information Technology (MeitY)

In November 2017, Microsoft became one of the first global cloud service providers to achieve full accreditation by MeitY for its three cloud models:

- Public Cloud, for shared, multi-tenant public cloud services
- Government Virtual Private Cloud, which must be logically separate from the public and other offerings of the cloud service provider
- Government Community Cloud, for cloud services that are dedicated to government departments and physically separate from the public and other offerings of the cloud service provider

The MeitY accreditation of Microsoft was the result of a rigorous audit conducted by the Standardization Testing and Quality Certification (STQC) Directorate, a government organization that provides quality assurance services, using an evaluation framework based on the work of the MeghRaj Cloud Initiative. Through Microsoft Azure, public sector organizations can now draw on a wide range of deployment models and service offerings, including infrastructure as a service (IaaS), platform as a service (PaaS), disaster recovery, DevOps, and managed backup.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Office 365](#)

## Audits, reports, and certificates

- Microsoft Cloud accreditation under [Audit Status of Cloud Service Providers](#)

# Frequently asked questions

## Why is MeitY important?

Making government services available to citizens online is a key part of the Digital India program, which aims to 'transform India into a digitally empowered society and knowledge economy.' MeitY lists accredited cloud service providers in the government cloud services directory, which enables public sector organizations to compare and procure those services.

## Resources

- [Ministry of Electronics and Information Technology](#)
- [MeghRaj Cloud Initiative](#)
- [Accredited cloud service providers](#)
- [Compliance on the Microsoft Trust Center](#)



# Multi-Tier Cloud Security (MTCS) Standard for Singapore

2/5/2021 • 3 minutes to read • [Edit Online](#)

## MTCS overview

The Multi-Tier Cloud Security (MTCS) Standard for Singapore was prepared under the direction of the Information Technology Standards Committee (ITSC) of the Infocomm Development Authority of Singapore (IDA). The ITSC promotes and facilitates national programs to standardize IT and communications, and Singapore's participation in international standardization activities.

The purpose of the MTCS is to provide:

- A common standard that cloud service providers (CSPs) can apply to address customer concerns about the security and confidentiality of data in the cloud, and the impact on businesses of using cloud services.
- Verifiable operational transparency and visibility into risks to the customer when they use cloud services.

The MTCS builds upon recognized international standards such as ISO/IEC 27001, and covers such areas as data retention, data sovereignty, data portability, liability, availability, business continuity, disaster recovery, and incident management. It also includes a mechanism for customers to benchmark and rank the capabilities of CSPs against a set of minimum baseline security requirements.

MTCS is the first cloud security standard with different levels of security, so certified CSPs can specify which levels they offer. MTCS includes a total of 535 controls, covering basic security in Level 1, more stringent governance and tenancy controls in Level 2, and reliability and resiliency for high-impact information systems in Level 3.

## Microsoft and MTCS

After rigorous assessments conducted by the MTCS Certification Body, Microsoft cloud services received MTCS 584:2013 certification across all three service classifications — Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Microsoft was the first global CSP to receive this certification across all three classifications.

Certifications were granted at Level 3 for Microsoft Azure services (IaaS and PaaS), Microsoft Dynamics 365 services (SaaS), and Microsoft Office 365 services (SaaS). A Level 3 certification means that in-scope Microsoft cloud services can host high-impact data for regulated organizations with the strictest security requirements. It's required for certain cloud solution implementations by the Singapore government.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- Microsoft Cloud App Security
- Genomics
- Microsoft Graph
- Microsoft Healthcare Bot
- Intune
- Flow

- OMS Service Map
- PowerApps
- Power BI
- Microsoft Stream
- [Office 365](#)

## Audits, reports, and certificates

Certification is valid for three years, with a yearly surveillance audit to be conducted.

### Microsoft MTCS certification

- [Microsoft Azure and Other Online Services](#)
- [Dynamics 365](#)
- [Office 365](#)

### Microsoft MTCS cloud service provider disclosure

- [Microsoft Azure and Other Online Services](#)
- [Dynamics 365](#)
- [Intune](#)
- [Office 365](#)

## Frequently asked questions

### To whom does the standard apply?

It applies to businesses in Singapore that purchase cloud services requiring compliance with the MTCS standard.

### What are the differences between MTCS security levels?

MTCS has a total of 535 controls that cover three levels of security:

- Level 1 is low cost, with a minimum number of required baseline security controls. It is suitable for web site hosting, test and development work, simulation, and noncritical business applications.
- Level 2 addresses the needs of most organizations that are concerned about data security, with a set of more stringent controls targeted at security risks and threats to data. Level 2 is applicable for most cloud usage, including mission-critical business applications.
- Level 3 is designed for regulated organizations with specific requirements and those willing to pay for stricter security requirements. Level 3 adds a set of security controls to supplement those in Levels 1 and 2. They address security risks and threats in high-impact information systems using cloud services, such as hosting applications with sensitive information and in regulated systems.

### Where do I start with my organization's own compliance effort?

The [MTCS Certification Scheme](#) provides guidance on audit controls and security requirements.

### Can I use Microsoft's compliance in my organization's certification process?

Yes. If you have a requirement to certify your services built on these Microsoft cloud services, you can use the MTCS certification to reduce the impact of auditing your IT infrastructure, if it relies on them. However, you are responsible for engaging an assessor to evaluate your implementation for compliance, and for the controls and processes within your own organization.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your

organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the **assessment templates** page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [MTCS Certification Scheme](#)
- [Azure compliance in the context of Singapore security and privacy requirements](#)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

# My Number Act (Japan)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## About the My Number Act

The Japanese government enacted the My Number Act ([Japanese](#) and [English](#)), which took effect in January 2016. It assigned a unique 12-digit number, called My Number, or the Social Benefits and Tax Number or Individual Number, to every resident of Japan, whether Japanese or foreign. Giving each person one number for all purposes (like the US Social Security number) was designed to simplify and make more efficient taxation and the implementation of social benefits such as the national pension, medical insurance, and unemployment.

The Personal Information Protection Commission (PPC), which acts as the centralized data protection authority, was established by the Act on the Protection of Personal Information ([Japanese](#) and [English](#)). In the PPC's role of supervising and monitoring compliance with the My Number Act, it has issued [My Number Guidelines](#) ([Japanese](#)) to ensure that organizations properly handle and adequately protect personal data, including My Number data, as required by law.

## Microsoft and the My Number Act

To help our Japanese customers protect the privacy of personal data, Microsoft contractually commits through the [Microsoft Online Services Terms](#) that our in-scope business cloud services have implemented the technical and organizational security safeguards that help our customers comply with the My Number Act. This support means that customers in Japan can deploy Microsoft business cloud services with the confidence that they can comply with Japanese legislative requirements.

The [Q&A](#) ([Japanese](#)) published by the Personal Information Protection Commission (PPC) sets forth guidelines for the appropriate handling and protection of personal information. It provides that a third party is not construed as handling personal data if the third party stipulates in its agreement that (a) it does not do so, and (b) it establishes a proper access control system. The My Number Act specifies obligations when data is transferred to a third party, but section [Q3-12](#) ([Japanese](#)) of the PPC Q&A explains that these requirements do not apply if the third party does not 'handle', that is, have standing access to personal data.

Microsoft business cloud services address those requirements in the [Microsoft Online Services Terms](#), which stipulate that the ownership of and responsibility for customer data that contains My Number data lie with our customers, not Microsoft. The customer, therefore, must have appropriate controls in place to protect My Number data contained in customer data.

Because Microsoft does not have standing access to My Number data stored in its cloud services, an 'outsourcing' contract for handling My Number data is not required. If a customer wants Microsoft to have access to customer data that contains My Number data, the customer must create an additional outsourcing contract with Microsoft for every case before making such a request.

The terms also state that Microsoft commits to use customer data only to provide services to the customer—not for any advertising or similar commercial purposes, and that Microsoft has robust access control systems in place.

Regarding security concerns, Microsoft business cloud services meet the [Cloud Security Mark \(Gold\)](#) standard, the first Japanese security accreditation for cloud service providers.

Therefore, Microsoft business cloud services support My Number Act requirements and do not create any additional obligations under the act for customers, such as consent from an individual owner of personal data.

# Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- Intune
- [Office 365](#)

## How to implement

- [Microsoft Security Policy](#): How Microsoft handles the security of personal and organizational information in its cloud services.
- [Privacy in Office 365](#): How Microsoft builds strong privacy protections into Office 365.
- [Admin Access in Office 365](#): How Microsoft manages administrative access to customer data.
- [Audits & Reports in Office 365](#): Explore the features customers can use to track user and administrative activity within their tenant.
- [Data Retention in Office 365](#): Understand the data handling policy for how long customer data is retained after being deleted.

## Frequently asked questions

### **Who is ultimately responsible for protecting personal data under the My Number Act?**

[Section Q3-13](#) (Japanese) of the PPC Q&A states that because the ownership of personal data lies with Microsoft customers, they are required to take appropriate security measures, such as controlling administrator passwords, to protect personal information and My Number data.

## Resources

- [Azure Compliance and the Japan Security and Privacy Requirements](#)
- [Privacy at Microsoft](#)
- [Microsoft Privacy Statement](#)
- [Privacy considerations in the cloud](#)
- [Compliance on the Microsoft Trust Center](#)

# Australian Prudential Regulation Authority (APRA)

2/5/2021 • 5 minutes to read • [Edit Online](#)

## APRA overview

The [Australian Prudential Regulation Authority](#) (APRA) oversees banks, credit unions, insurance companies, and other financial services institutions in Australia. Recognizing the momentum towards cloud computing, APRA has called on regulated entities to implement a thoughtful cloud-adoption strategy with effective governance, thorough risk assessment, and regular assurance processes. Regulated institutions must comply with the [APRA Prudential Standard CPS 231 Outsourcing](#) when outsourcing a material business activity — any activity that has the potential, if disrupted, to have a significant impact on the financial institution's business operations or ability to manage its risks effectively. Based on its review of outsourcing arrangements involving cloud computing services submitted to APRA, APRA published specific, detailed guidance in its information paper, [Outsourcing involving cloud computing services](#) to help regulated entities assess cloud providers and services more effectively and guide them through the regulatory issues of outsourcing to the cloud. When outsourcing, including to a cloud service, regulated institutions must also review and consider their ongoing compliance with [APRA Prudential Standard CPS 234 Information Security](#).

## Microsoft and APRA

For financial institutions in Australia that are assessing cloud providers and their services, Microsoft has published:

- [Microsoft response to the APRA Information Paper on Cloud](#)
- [Microsoft cloud services: a compliance checklist for financial institutions in Australia](#)
- [Microsoft cloud services: compliance with APRA Prudential Standard CPS 234](#)

Together they demonstrate how financial firms can move data and workloads to Microsoft Azure with the confidence that they are complying with Australian Prudential Regulation Authority (APRA) regulations and guidance.

To learn about the benefits of APRA-compliant financial services on Azure, read the [Regtech meets Fintech: Perpetual and Microsoft transform the finance sector](#) article.

## Microsoft response to the APRA Information Paper on Cloud

This Microsoft paper provides detailed guidance for financial services with a detailed response to each issue raised in the APRA Information Paper [Outsourcing involving cloud computing services](#). The APRA guidelines identify three risk categories into which cloud usage typically falls — low, heightened, and extreme inherent risk — and highlight key issues that regulated entities must consider as part of their risk assessment.

The Microsoft response focuses on the two highest risk categories. While cloud services are not prohibited by any risk category, APRA expects you to undertake a commensurately higher level of diligence, and you should expect an increasing level of APRA scrutiny, as you move up the risk categories. APRA lists a range of factors that typically indicate high or extreme inherent risk for cloud outsourcing. Microsoft addresses each of these factors in depth, providing information and tools to help you assess and manage the risk of moving your data and workloads to Azure.

Microsoft also addresses each APRA risk management consideration: strategy, governance, solution selection process, APRA access and ability to act, transition approach, risk assessments and security, ongoing oversight, business disruption, and audit and assurance. Point by point, we give advice and offer tools to help you respond

to each issue when deploying Azure.

Get practical support for moving data and workloads to Azure in compliance with APRA regulations: [Download the Microsoft response to the APRA Information Paper on Cloud](#).

## Microsoft response to the APRA CPS 234 on Information Security

APRA [Prudential Standard CPS 234 Information Security](#) requires regulated institutions to:

- clearly define information-security related roles and responsibilities;
- maintain an information security capability commensurate with the size and extent of threats to their information assets;
- implement controls to protect information assets and undertake regular testing and assurance of the effectiveness of controls; and
- promptly notify APRA of material information security incidents.

CPS 234 closely mirrors the core Microsoft security framework: protect, detect, and respond.

[Microsoft cloud services: compliance with APRA Prudential Standard CPS 234 Information Security](#) sets out each of the relevant CPS 234 regulatory obligations, and maps against it the Microsoft cloud service controls, capabilities, functions, contract commitments, and supporting information to help your APRA-regulated entity comply with its regulatory obligations under CPS 234.

## Navigating your way to the cloud: A compliance checklist for financial institutions in Australia

This Microsoft checklist introduces APRA regulatory requirements that financial firms must address when moving to the cloud. It maps Azure against not only the [Prudential Standard CPS 231 Outsourcing](#), but other relevant APRA standards, such as for business continuity and risk management. Completing this checklist helps your financial service institutions adopt Azure with the confidence that it meets the relevant APRA requirements.

By relying on our comprehensive approach to risk assurance in the cloud, we are confident that Australian financial services organizations can move to Microsoft cloud services in a manner that is not only consistent with APRA guidance, but can provide customers with a more advanced security risk management profile than on-premises or other hosted solutions.

Get practical support for moving data and workloads to Azure in compliance with APRA regulations: [Download Microsoft cloud services: a compliance checklist for financial institutions in Australia](#).

## Microsoft in-scope cloud services

- [Azure](#)
- [Office 365](#)
- [Dynamics 365](#)

## Frequently asked questions

**Do financial institutions need APRA approval before outsourcing material business activities?**

No. However, most regulated financial organizations must notify APRA after entering into agreements to outsource material business activities within Australia or consult with APRA before outsourcing those activities outside of Australia.

In addition, if the cloud services are deemed to carry 'heightened or extreme inherent risk' as described in the [APRA Information Paper on Clouds](#), the financial institution is encouraged (but not required) to consult with

APRA, regardless of whether the service is provided within or outside of Australia.

### Are transfers of data outside of Australia permitted?

Yes. General privacy legislation (which applies across all sectors, not just to financial institutions) permits transfers outside of Australia under certain conditions. Microsoft agrees to contractual terms in line with Australian Privacy Principles so that transfers of data outside of Australia are permitted when you use Microsoft cloud services. However, many of our Australian financial services customers take advantage of the cloud services available from our Australian datacenters, for which we make specific contractual commitments to store categories of data at rest in the Australian geography. These commitments are outlined further in the [compliance checklist](#).

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Australian Prudential Regulation Authority](#)
- [APRA Information Paper Outsourcing involving cloud computing services](#)
- [Prudential Standard CPS 231 Outsourcing](#)
- [Prudential Standard CPS 234 Information Security](#)
- [Microsoft response to the APRA Information Paper on the Cloud](#)
- [Microsoft cloud services: a compliance checklist for financial institutions in Australia](#)
- [Microsoft cloud services: compliance with APRA Prudential Standard CPS 234](#)
- [Microsoft Australia: Cloud in Financial Services](#)
- [Microsoft Financial Services Compliance Program](#)
- [Financial services compliance in Azure](#)
- [Microsoft business cloud services and financial services](#)
- [Compliance on the Microsoft Trust Center](#)



# Australian Government Information Security Registered Assessor Program (IRAP)

2/17/2021 • 4 minutes to read • [Edit Online](#)

The Information Security Registered Assessor Program (IRAP) provides a comprehensive process for the independent assessment of a system's security against Australian government policies and guidelines. The IRAP goal is to maximize the security of Australian federal, state, and local government data by focusing on the information and communications technology infrastructure that stores, processes, and communicates it.

## IRAP overview

The Information Security Registered Assessors Program (IRAP) is governed and administered by the Australian Cyber Security Centre (ACSC). IRAP provides the framework to endorse individuals from the private and public sectors to provide cyber security assessment services to the Australian government. Endorsed IRAP assessors can provide an independent assessment of ICT security, suggest mitigations and highlight residual risks. IRAP provides a comprehensive process for the independent assessment of a system's security against Australian government policies and guidelines. The IRAP goal is to maximize the security of Australian federal, state, and local government data by focusing on the information and communications technology infrastructure that stores, processes, and communicates it.

- In 2014, Azure was launched as the first IRAP-assessed cloud service in Australia, hosted from datacenters in Melbourne and Sydney. These two datacenters give Australian customers control over where their customer data is stored, while also providing enhanced data durability in there are disasters through backups at both locations.
- In early 2015, Office 365 became the first cloud productivity service to complete this assessment.
- In April 2015, the ASD announced the CCSL certification of both Azure and Office 365, and in November 2015, of Dynamics 365.
- In June 2017, ASD announced the recertification of Microsoft Azure and Office 365 for a greatly expanded set of services.
- In April 2018, the ACSC announced the certification of Azure and Office 365 at the PROTECTED classification. Microsoft is the first and only public cloud provider to achieve this level of certification.
- In September 2019, Microsoft's updated IRAP assessment scope expanded to include 113 services at the PROTECTED classification.
- In December 2020, Microsoft released two incremental IRAP assessments for Azure and Office 365. These reports utilized the new guidance post the cessation of the Certified Cloud Services List (CCSL). The reports contain both an assessment of Microsoft as a Cloud Service Provider (CSP) and other services that are incremental to the 2019 reports across Azure, Dynamics, and Office 365.

## Microsoft and IRAP

In December 2020, Microsoft completed two incremental Azure & Dynamics and Office 365 assessments. These assessments added more services assessed to the classification level of PROTECTED. Moreover, these assessments were conducted under the new, post CCSL Cloud Security Guidance as outlined in the [Anatomy of a Cloud Assessment and Authorisation guidance](#) from the ACSC.

For each assessment, Microsoft engaged an ACSC-accredited IRAP assessor who examined the security controls and processes used by Microsoft's IT operations team, physical datacenters, intrusion detection, cryptography, cross-domain and network security, access control, and information security risk management of in-scope

services. The IRAP assessments found that the Microsoft system architecture is based on sound security principles, and that the applicable Australian Government Information Security Manual (ISM) controls are in place and fully effective within our assessed services.

The risk management framework used by the ISM draws from [National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-37 Rev. 2](#), 'Risk Management Framework for Information Systems and Organizations: A System Life-Cycle Approach for Security and Privacy.' Within this risk management framework, the identification of risks and selection of security controls can be undertaken using various risk management standards, such as [International Organization for Standardization \(ISO\) 31000:2018, Risk management - Guidelines](#). Broadly, the risk management framework used by the ISM has six steps:

- Define the system
- Select security controls
- Implement security controls
- Assess security controls
- Authorize the system
- Monitor the system

As always, additional compensating controls can be implemented on a risk-managed basis by individual agencies prior to agency authorization and subsequent use of these cloud services.

The IRAP assessment of Microsoft's services and cloud operations helps provide assurance to public sector customers in government and their partners that Microsoft has appropriate and effective security controls in place for the processing, storage, and transmission of data classified up to and including the level of PROTECTED. This assessment includes most government, healthcare, and education data in Australia.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft Managed Desktop](#)
- [Office 365](#)

## Frequently asked questions

### To whom does the IRAP apply?

IRAP applies to all Australian federal, state, and local government agencies that use cloud services. New Zealand government agencies require compliance with a standard similar to the Australian Government ISM, so they may also use the IRAP assessments.

### Can I use Microsoft's compliance in my organization's risk assessment and approval process?

Yes. If your organization requires or is seeking an approval to operate in line with the ISM, you can use the IRAP security assessments of Azure, Dynamics 365, Microsoft Managed Desktop, and Office 365 in your risk assessment. You are, however, responsible for engaging an assessor to evaluate your implementation as deployed on Microsoft's platforms, and for the controls and processes within your own organization.

### Where do I start with my organization's own risk assessment and approval to operate?

It is recommended that you read the [Cloud Security Assessments](#) guidance from the ACSC.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium

template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Australian Government ISM](#)
- [Australia page of the Microsoft Service Trust Portal \(STP\)](#)
- [Australian Cyber Security Centre \(ACSC\)](#)

# New Zealand Government Cloud Computing Security and Privacy Considerations

12/1/2020 • 2 minutes to read • [Edit Online](#)

## New Zealand Government Cloud Computing Security and Privacy overview

In October 2015, the New Zealand Government endorsed a revised all-government ICT strategy that reaffirmed its 'cloud first' policy on using information technology across the public sector. The revised strategy retains the 'Cloud Computing Risk and Assurance Framework' that was developed and implemented under the authority of the NZ Government Chief Information Officer (GCIO).

The government expects all New Zealand State Service agencies to work within this framework when assessing and adopting cloud services. 'Requirements for Cloud Computing' outlines what agencies must do when adopting cloud services along with an overview of the history of the government's cloud policy.

To assist NZ government agencies in conducting consistent and robust due diligence on potential cloud solutions, the GCIO has published 'Cloud Computing: Information Security and Privacy Considerations' (the 'Cloud Computing ISPC'). This document contains more than 100 questions focused on data sovereignty, privacy, security, governance, confidentiality, data integrity, availability, and incident response and management. 'Cloud Computing IPSC' does not define a NZ government standard against which cloud service providers must demonstrate formal compliance. Many of the questions set out in the document do, however, point toward the importance of understanding how cloud service providers comply with a wide array of relevant standards.

### Microsoft and New Zealand Government Cloud Computing Security and Privacy Considerations

To help agencies undertake their analysis and evaluation of Microsoft enterprise cloud services, Microsoft New Zealand has produced documents showing how its enterprise cloud services address the questions set out in the 'Cloud Computing ISPC' by linking them to the standards against which Microsoft cloud services are certified. These certifications are central to how Microsoft assures both public and private sector customers that its cloud services are designed, built, and operated to effectively mitigate privacy and security risks and address data sovereignty concerns.

Learn how to accelerate your NZ CC Framework deployment with our Azure Security and Compliance Blueprint: [Download Azure response to the NZ CC Framework](#)

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- [Dynamics 365](#)
- Intune
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- [Office 365](#)
- Exchange Online, SharePoint Online, and Microsoft Teams. Microsoft NZ has worked with the GCIO team to develop a reference architecture for integrating Exchange Online and SEEMail.

## Frequently asked questions

To whom does the framework apply?

Organizations that fall under the GCIO mandate, the public and non-public service departments, the 20 district health boards, and 7 Crown entities, must adhere to the framework when they are deciding on the use of a cloud service.

**Can my agency use Microsoft's responses to this framework in the certification process of our ICT systems?**

If your agency is required to undertake certification and accreditation of its ICT system under the [New Zealand Information Security Manual](#), then you can use these responses as part of your analysis.

## Resources

- [Security requirements for offshore hosted Office productivity services: conformance guide for Office 365](#)
- [Microsoft Azure compliance in the context of New Zealand security and privacy requirements](#)
- [NZ Government ICT Strategy 2015](#)
- [NZ Government requirements for cloud computing](#)
- [Cloud Computing: Information Security and Privacy Considerations \(ISPC\)](#)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

## Microsoft responses to 'Cloud Computing IPSC'

- [Azure](#)
- [Dynamics 365](#)
- [Intune](#)
- [Office 365](#)
- [Power BI](#)

# Baseline Informatiebeveiliging Rijksdienst standard (BIR 2012)

11/30/2020 • 3 minutes to read • [Edit Online](#)

## BIR 2012 overview

Organizations operating in the Netherlands government sector must demonstrate compliance with the Baseline Informatiebeveiliging Rijksdienst standard (BIR 2012). The BIR 2012 provides a standard framework based on ISO 27001 and ISO 27002. When using Microsoft Azure or Office 365, part of the BIR 2012 controls for these cloud services are managed by Microsoft in line with the shared responsibility model in cloud computing. Organizations that need to comply with BIR 2012 are therefore required to determine if the underlying Microsoft services they are using are compliant with BIR 2012.

The BIR coverage report provides guidance where the BIR standards are covered by existing ISO 27001 certifications that are available for Microsoft cloud services. Where there are additional BIR controls that are not covered by ISO 27001, references are made to other independent attestations, audit documentation, or contractual statements.

## Microsoft and BIR 2012

While Microsoft is not subject to BIR 2012 compliance, customers from the government sector seeking to use cloud services can use Microsoft's existing certifications to determine their compliance with this standard. Azure and Office 365 undergo various periodic independent certifications and attestations, some of which are closely related to BIR 2012.

[Download the Microsoft Cloud: Azure and Office 365 BIR-2012 Baseline Coverage User Guide](#)

## Microsoft in-scope cloud services

- [Azure](#)
- [Intune](#)
- [Office 365](#)

## Audits, reports, and certificates

- [Azure and Office 365 BIR-2012 Baseline Coverage](#)
- [Azure and Office 365 BIR-2012 Baseline Coverage User Guide \(Dutch\)](#)

## Frequently asked questions

### Is Microsoft BIR 2012 certified?

The responsibility for BIR compliance is applicable to the government sector. It requires the organization to implement an information security management system and to address risk with appropriate technical and organizational measures. For Microsoft in its role as cloud service provider, BIR compliance is not the objective, nor is it technically feasible. When a customer implements or uses Microsoft cloud services, those services may be in scope of a BIR evaluation. However, the organization must add its own (additional) controls, choices, and processes, which are part of the overall BIR evaluation. The objective of the report is to demonstrate that a government agency can adopt Microsoft cloud services in a manner that is compliant with BIR 2012.

## Is a customer that uses Microsoft cloud services compliant with BIR 2012?

Demonstrating BIR compliance is the responsibility of the customer. When using a cloud services vendor, customers typically demand assurances from the vendor, and add their own (additional) technology and organizational decisions, choices, and processes. This effort results in an overall assessment by the customer on its BIR compliance, which can be submitted for review or certification to a third-party auditor. The BIR coverage report provides insight into what BIR controls are covered by Microsoft cloud services, but as such does not cover end-to-end compliance.

## The report does not show 100% coverage. Is BIR 2012 compliance not feasible?

Microsoft cloud services provide many controls that help organizations within the Netherlands with their BIR compliance needs. However, an organization needs to complement those vendor assurances with their own implementation choices, additional technology controls, and administrative processes. The report shows already over 91% direct coverage of the full list of applicable controls. For the remaining controls, Microsoft provides guidance in the report on how compliance with those controls can be demonstrated.

## Is the BIR coverage report a legal binding document?

No. It is a supporting tool for the customer's internal BIR assurance process and helps to establish confidence and trust that BIR compliance is feasible. The report has a descriptive status and includes a legal disclaimer.

## Can we share this report?

The report is provided to customers under a non-disclosure agreement, on the basis that it is for customer information only and that it will not be copied or disclosed via other channels than the Microsoft [Service Trust Platform](#). Customers can share the report with their own internal or external auditor as part of their compliance or assurance processes.

## Resources

- [ISO-IEC 27001](#)
- [Security prescription national 2013 \(BVR\)](#)
- [Prescription information security national 2007 \(VIR\)](#)
- [Baseline Information Security \(BIR\)](#)
- [Compliance on the Microsoft Trust Center](#)

# Cloud Computing Compliance Controls Catalog (C5)

2/5/2021 • 3 minutes to read • [Edit Online](#)

## C5 overview

In 2016, the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, or BSI) created the Cloud Computing Compliance Controls Catalog (C5). C5 is an audited standard that establishes a mandatory minimum baseline for cloud security and the adoption of public cloud solutions by German government agencies and organizations that work with government. C5 is also being increasingly adopted by the private sector.

The purpose of the C5 catalog of requirements is to provide a consistent security framework for certifying cloud service providers and to give customers assurance that their data will be managed securely.

C5 is based on internationally recognized IT security standards like ISO/IEC 27001:2013, the Cloud Security Alliance Cloud Controls Matrix 3.0.1, and BSI's own IT-Grundschutz Catalogues. The catalog consists of 114 requirements across 17 domains, for example, the organization of information security and physical security, with security requirements basic to all cloud service providers, and other requirements for processing highly confidential data and situations requiring high availability.

The BSI also puts emphasis on transparency. As part of an audit, the cloud provider must include a detailed system description and disclose environmental parameters like jurisdiction and data processing location, provision of services, and other certifications issued to the cloud services, and information about the cloud provider's disclosure obligations to public authorities. This helps potential cloud customers decide whether the cloud services meet their essential requirements such as compliance with legal requirements like data protection, company policies, or the ability to address the threat of industrial espionage.

## Microsoft and C5

Microsoft cloud services are audited at least annually against SOC 2 (AT Section 101) standards. According to BSI, a C5 audit can be combined with a SOC 2 audit to reuse parts of the system description and audit results for overlapping controls. Microsoft Azure, Azure Government, and Azure Germany maintain a combined report (C5, SOC 2 Type 2, CSA STAR Attestation) based on the audit assessment performed by an independent auditor, which demonstrates proof of compliance with C5.

## Microsoft in-scope cloud services

- [Azure, Azure Government, and Azure Germany](#)
- Office 365 Germany

## Audits, reports, and certificates

- [Azure, Azure Government, and Azure Germany SOC 2 Type II Report.pdf](#)

## Frequently asked questions

**Can I use Microsoft compliance with C5 to help my organization get its own C5 attestation?**

Yes. You may use the attestation of Microsoft cloud services as the foundation for any program or initiative that



requires C5. However, you need to achieve your own C5 attestation for components outside or built on top of these services.

### What's the difference between C5 and the IT-Grundschutz Catalogues?

IT-Grundschutz supplies the specific methodology to help organizations identify and implement security measures for IT systems and is one of the elements upon which the C5 standards are built. C5 provides a set of audit standards for cloud service providers but leaves the details of implementation up to the cloud service provider.

### What is Microsoft Cloud Germany?

Microsoft Cloud Germany is physically based in Germany, adhering to the requirement of German privacy law, which limits the transfer of personal data to other countries and offers protection against access by authorities from other jurisdictions who could violate domestic laws. Azure Germany delivers Azure services from German datacenters with data residency in Germany, and it delivers strict data access and control measures provided through a unique data trustee model governed under German law.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Cloud Computing Compliance Controls Catalogue \(C5\)](#) ([English](#)) ([German](#))
- [Security Recommendations for Cloud Computing Providers](#) ([English](#)) ([German](#))
- [Compliance Reports: C5- und SOC-Testate Azure Deutschland](#)
- [IT-Grundschutz Compliance Workbook](#) for Microsoft Azure Germany
- [Compliance on the Microsoft Trust Center](#)

# United Kingdom Cyber Essentials PLUS

2/5/2021 • 2 minutes to read • [Edit Online](#)

## UK Cyber Essentials PLUS overview

Cyber Essentials is a UK government-backed scheme designed to help organizations assess and mitigate risks from common cyber security threats to their IT systems. The Cyber Essentials scheme is a cyber security standard that identifies security controls for an organization to have in place within their IT systems. Cyber Essentials scheme is a requirement for all UK government suppliers handling any personal data. The Cyber Essentials badge helps an organization demonstrate the ability to:

- Identify potential risks to help organizations better protect against common cyber threats.
- Demonstrate an organization has adopted the proper security controls to protect customer data.
- Become compliant with UK government expectations for Cyber Security Essential requirements and eligible to bid for UK government contracts.

The Cyber Essentials scheme is designed for UK government suppliers to identify potential weaknesses in their IT systems and software that could exploit customer data. The methodology has defined two different levels of certification:

- Cyber Essentials is the first level and includes a self-assessment for organizations to check the most important IT security controls of their IT infrastructure. The responses are independently reviewed by an external certifying body.
- Cyber Essentials PLUS offers the same controls coverage as Cyber Essentials and also includes additional assurance by carrying out systems tests of implemented controls through an authorized third-party certifying body.

## Microsoft and UK Cyber Essentials PLUS

Microsoft Azure has attained Cyber Essentials PLUS badge and meets the requirements outlined in the [Cyber Essentials Scheme](#). Azure production systems are frequently tested and audited to provide evidence of a world-leading compliance portfolio.

The [Azure Cyber Essentials PLUS certification](#), which applies to our global operation of Azure, is available for download.

## Audits, reports, and certificates

- [Azure Cyber Essentials PLUS compliance report](#)
- [Azure Cyber Essentials PLUS certification](#)

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Cyber Essentials Scheme: Assurance framework](#)

- [Compliance on the Microsoft Trust Center](#)

# European Standards EN 301 549

11/30/2020 • 2 minutes to read • [Edit Online](#)

## About EN 301 549

Accessibility requirements suitable for information and communications technologies (ICT) products and services are set forth in EN 301 549, which is a set of standards for ICT products and services including websites, software, and digital devices. EN 301 549 was published in 2014 by the European Telecommunications Standards Institute (ETSI) in response to a request from the European Commission, and it was most recently updated in November 2019 to version 3.1.1. EN 301 549 3.1.1 incorporates the [WCAG](#) standards for web accessibility.

Microsoft is a major software and cloud-services provider to European states. To assist government customers in making procurement decisions, Microsoft publishes Accessibility Conformance Reports (ACRs) describing the extent to which our products and services support the criteria of EN 301 549. The information in the ACRs can help Microsoft customers determine whether a product or service will meet their specific needs.

## Microsoft and EN 301 549

Microsoft's consideration of EN 301 549 in the development of products and services points to its commitment to accessibility for all customers.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Azure DevOps Services
- Dynamics 365 and Dynamics 365 U.S. Government
- Intune
- [Office 365 and Office 365 U.S. Government](#)
- Office 365 U.S. Government Defense
- Windows Server 2016

## Microsoft accessibility conformance reports

Find [conformance reports](#) for all our products and services.

## Resources

- [Microsoft accessibility site](#): Get information on using accessibility features and explore how Microsoft innovates to help everyone achieve more.
- [Office 365 Accessibility Center](#): Office 365 resources for people with disabilities.
- [Enterprise Disability Answer Desk](#): Dedicated support for enterprise customers with accessibility questions about our products and services or compliance.
- [Compliance on the Microsoft Trust Center](#)

# Spain Esquema Nacional de Seguridad (ENS) High-Level Security Measures

11/30/2020 • 3 minutes to read • [Edit Online](#)

## Spain ENS overview

In 2007, the Spanish government enacted Law 11/2007, which established a legal framework to give citizens electronic access to government and public services. This law is the basis for Esquema Nacional de Seguridad (National Security Framework), which is governed by Royal Decree (RD) 3/2010. The goal of the framework is to build trust in the provision of electronic services, and ensure the access, integrity, availability, authenticity, confidentiality, traceability, and preservation of data, information, and services.

The framework applies to all public organizations and government agencies in Spain that purchase cloud services, as well as to providers of information and communications technologies (ICT). It guides these agencies and companies in implementing effective controls for security in the cloud and on premises, in compliance with Spanish and EU security and privacy standards.

The framework establishes core policies and mandatory requirements that both government agencies and their service providers must meet. It defines a set of specific security controls, many of which align directly with ISO/IEC 27001, relating to availability, authenticity, integrity, confidentiality, and traceability. The sensitivity of the information, low, intermediate, or high, determines the security measures that must be applied to protect it.

Each government agency is required to adopt a risk-management approach to security, whereby they identify and assess risks, and then apply security controls appropriate to those risks. Service providers, too, must comply with the stringent framework requirements to help ensure that their procedures, technical capacities, and operations are secure and enable agencies to comply with the regulations.

The framework prescribes an accreditation process that is voluntary for systems handling information of low sensitivity, but mandatory for systems handling information at an intermediate or high level of sensitivity. An audit is performed by an accredited independent auditor. The report is then reviewed in a process of certification before risk-management controls are accepted in the final step of accreditation.

## Microsoft and Spain ENS high-level security measures

Microsoft Azure and Microsoft Office 365 have gone through a rigorous assessment by BDO, an independent auditor, which issued an official statement of their compliance. BDO reports that the security measures in both services, and their information systems and data processing facilities, comply at the high level with RD 3/2010 without requiring any corrective measures. Microsoft was the first hyperscale cloud service provider to receive this certification in Spain.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- [Office 365](#)

## Audits, reports, and certificates

The certification is valid for two years, with an annual surveillance audit.

**Azure**

- [Azure National Security Framework ENS certificate](#)
- [Azure Spanish National Security Framework \(ENS\) Audit Report](#)
- [Azure Audit Report ENS \(Spanish\)](#)
- [Azure National Security Framework Certificate ENS \(Spanish\)](#)

#### **Office 365**

- [Office 365 National Security Framework ENS Certificate](#)
- [Office 365 Spanish National Security Framework \(ENS\) Audit Report](#)
- [Office 365 Audit Report ENS \(Spanish\)](#)
- [Office 365 National Security Framework Certificate ENS \(Spanish\)](#)

## Frequently asked questions

### **How can I get copies of the audit reports and certifications?**

The [Service Trust Portal](#) provides the audit reports and certifications in both Spanish and English. Your auditors can use them to compare Microsoft cloud services results with your own legal and regulatory requirements.

### **Where do I start with my organization's own compliance effort?**

If your organization is using Azure or Office 365, you can use ENS Microsoft audit reports and accreditation as part of your own accreditation process. However, you are responsible for engaging an auditor to evaluate your implementation for compliance, and for ensuring that the controls and processes within your own organization align with the framework.

## Resources

- [Esquema Nacional de Seguridad of Spain \(Spanish and English\)](#)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

# ENISA Information Assurance Framework

11/30/2020 • 2 minutes to read • [Edit Online](#)

## About the ENISA Information Assurance Framework

The [European Network and Information Security Agency](#) (ENISA) is a center of network and information expertise. It works closely with EU member states and the private sector to provide advice and recommendations on good cybersecurity practices. ENISA also supports the development and implementation of EU policy and law relating to national information security.

The [Information Assurance Framework](#) (IAF) is a set of assurance criteria that organizations can review with cloud service providers to ensure that they sufficiently protect customer data. The IAF is intended to help organizations assess the risk of adopting cloud services, better compare the offers from different cloud services, and reduce the assurance burden on cloud service providers.

## Microsoft and the ENISA IAF

The ENISA Information Assurance Framework is based on the broad classes of controls from ISO/IEC 27001, the international information security management standard, and the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v3.0.1. The CCM is a controls framework covering fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a cloud service provider (CSP).

For the CSA STAR self-assessment, Microsoft submitted a report documenting Microsoft Azure compliance with the CSA CCM. (Microsoft also publishes a completed Consensus Assessments Initiative Questionnaire (CAIQ) for Azure.) That self-assessment of compliance aligns it with the ENISA IAF.

Azure compliance is listed on the CSA STAR Registry, a free publicly accessible registry where CSPs publish their CSA-related assessments. There, Azure also maintains a formal CSA STAR Certification and CSA STAR Attestation.

Because these self-assessment reports are publicly available, Azure customers gain visibility into Microsoft security practices and can compare various CSPs using the same baseline.

## Microsoft in-scope cloud services

- [Azure](#)

## Audits, reports, and certificates

Microsoft attests to Azure compliance with the CSA CCM framework based on self-assessment, aligning services with the ENISA IAF.

- [CSA STAR Registry](#)

## Resources

- [Azure standard response for request for information](#)
- [Microsoft and the CSA STAR Self-Assessment](#)

- Microsoft and ISO/IEC 27001



# European Union Model Clauses

11/30/2020 • 4 minutes to read • [Edit Online](#)

## European Union Model Clauses overview

European Union (EU) data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA), which includes all EU countries and Iceland, Liechtenstein, and Norway. The EU Model Clauses are standardized contractual clauses used in agreements between service providers (such as Microsoft) and their customers to ensure that any personal data leaving the EEA will be transferred in compliance with EU data-protection law and meet the requirements of the EU Data Protection Directive 95/46/EC.

On a practical level, compliance with EU data protection laws also means that customers need fewer approvals from individual authorities to transfer personal data outside of the EU, since most EU member states do not require additional authorization if the transfer is based on an agreement that complies with the Model Clauses.

## Microsoft and European Union Model Clauses

Microsoft has invested in the operational processes necessary to meet the exacting requirements of the Model Clauses for the transfer of personal data to processors. Microsoft offers customers Model Clauses, referred to as Standard Contractual Clauses, that make specific guarantees around transfers of personal data for in-scope Microsoft services. This ensures that Microsoft customers can freely move data through the Microsoft cloud from the EEA to the rest of the world.

However, Microsoft enterprise customers, who are the controllers of the personal data, carry the primary obligation to protect that data. This means that EEA enterprise customers have a strong interest in ensuring that their service provider abides by EU data protection laws, or the customer can face liability — and even blockage of its ability to use a service.

Microsoft provided its Standard Contractual Clauses to the EU's Article 29 Working Party for review and approval. The Article 29 Working Party includes representatives from the European Data Protection Supervisor, the European Commission, and each of the 28 EU data protection authorities (DPAs).

The group determined that implementation of the provisions in Microsoft agreements was in line with their stringent requirements. (Microsoft was the first cloud service provider to receive a letter of endorsement and approval from the group.) Approval covered the engagements reflected in Model Clauses 2010/87/EU but not in the appendices, which describe the transfers of data and the security measures implemented by the data importer. The appendices may be analyzed separately by the DPA.

## Microsoft in-scope cloud services

- [Azure and Azure Government](#)
- Microsoft Cloud App Security
- Microsoft Professional Services: Premier and On Premises for Azure, Dynamics 365, Intune, and for Medium Business and Enterprise customers of Microsoft 365 for business
- [Dynamics 365](#)
- Intune: Cloud service portion of the Intune Add-on Product and Mobile Device Management for Office 365
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- [Office 365](#)

- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite
- Azure DevOps Services
- Windows Defender Advanced Threat Protection for the following cloud service portions: Endpoint Detection & Response, Automatic Investigation & Remediation, Secure Score.

## Audits, reports, and certificates

Microsoft continually assesses the EU standards, and updates its services as needed.

## Frequently asked questions

### What is the EU Data Protection Directive 95/46/EC?

This directive sets the baseline for handling personal data in the EU. It provides the regulatory framework under which Microsoft transfers personal data out of the EU. Under this directive and our contractual agreements, Microsoft acts as the data processor of customer data. The customer acts as the data controller, with final ownership and responsibility for ensuring that the data can be legally provided to Microsoft for processing outside of the EEA.

### Why is compliance with the Model Clauses important?

A service provider that commits contractually to the Model Clauses gives its customers assurance that personal data will be transferred and processed in compliance with EU data protection law. Use of the Model Clauses also means that customers need to get fewer approvals from individual data-protection authorities to transfer personal data outside the EU.

### Where can I see compliance information for Microsoft services?

Compliance is a contractual commitment. Microsoft Standard Contractual Clauses are available to all cloud customers in the [Online Services Terms](#); for other services, see your existing agreement with Microsoft.

### What is a 'sub-processor'?

A sub-processor is someone who processes personal data following the data controller's instructions, and the terms of the EU Model Clauses and the subcontract. Microsoft customers—independent software vendors (ISVs), in particular — are sometimes themselves data processors. In those instances, Microsoft is the sub-processor.

### Where do I start with my own organization's compliance efforts?

You can enter an agreement such, as the [Online Services Terms](#), or explore amending your existing agreement to incorporate the Standard Contractual Clauses.

## Resources

- [EU Standards Organization](#)
- [EU Model Clauses](#)
- [EU Data Protection Directive](#)
- [European Data Protection Board](#)
- [EU Model Clauses FAQ for Dynamics 365 and Office 365](#)
- [Microsoft and the EU-U.S. Privacy Shield](#)
- [Microsoft Common Controls Hub Compliance Framework](#)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

# EU-US and Swiss-US Privacy Shield Frameworks

2/5/2021 • 4 minutes to read • [Edit Online](#)

## About the EU-U.S. and Swiss-U.S. Privacy Shield frameworks

According to the Privacy Shield Program, “the [EU-U.S. and Swiss-U.S. Privacy Shield Frameworks](#) were designed by the US Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States.” The International Trade Administration within the Department of Commerce administers the Privacy Shield Program in the United States.

The transfer of personal data outside of the EU and Switzerland is governed by EU and Swiss law, which generally prohibit personal data from being transferred to countries outside the EEA unless “adequate” levels of protection are ensured. The Privacy Shield Frameworks and the Standard Contractual Clauses (or [EU Model Clauses](#)) are two mechanisms designed to provide this level of data protection.

The 23 [Privacy Shield Principles](#) define a set of requirements that govern the use and handling of personal data transferred from the EU as well as access and dispute resolution mechanisms that participating companies must provide to EU citizens. Companies must let individuals know how their data is processed, limit the purposes for which it is used, protect data for as long as it is held, and ensure accountability for data transferred to third parties. Requirements also include providing free and accessible dispute resolution and transparency related to government requests for personal data.

## Microsoft and the EU-U.S. and Swiss-U.S. Privacy Shield frameworks

To join the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks — an action that is voluntary — US-based companies must publicly commit to complying with framework requirements and self-certify their compliance to the US Department of Commerce. Once they publicly commit and self-certify, that commitment becomes enforceable under US law.

Microsoft has publicly committed to the [Privacy Shield Principles](#) and has self-certified its compliance with its requirements. Our participation applies to all personal data processed by Microsoft that is transferred to the United States from the European Union, European Economic Area (EEA), and Switzerland. In addition, customers of Microsoft business cloud services benefit from compliance with the Standard Contractual Clauses (also known as [EU Model Clauses](#)) under the [Microsoft Online Services Terms](#), unless the customer has opted out of those clauses.

Microsoft cooperates with EU and Swiss national data protection authorities (DPAs) and complies with their advice for resolving any disputes that arise under the Privacy Shield. We will also meet Privacy Shield obligations for transparency about government requests for access to personal information. Our [Law Enforcement Requests Report](#) and [U.S. National Security Orders Report](#) make this information publicly available twice a year.

## Microsoft in-scope cloud services

- [Azure and Azure DevOps](#)
- [Dynamics 365 MT & GCC](#)
- Intune
- [Microsoft 365](#)

- Power BI cloud service as a standalone service or as included in an Office 365 branded plan or suite
- Professional Services
- Windows 10 and Windows Server

## Audits, reports, and certificates

Microsoft has certified to the US Department of Commerce that it adheres to the Privacy Shield Principles and submitted its self-certification to the EU-U.S. and Swiss-U.S. Privacy Shield. It is listed by the Privacy Shield Framework as an [Active Participant](#).

## How to implement

Privacy in the Microsoft Cloud — Get details on Microsoft privacy principles and standards and our approach to regulatory compliance.

- [Learn more](#)

Data protection in Azure — Azure provides customers with strong data security, both by default and as customer options.

- [Learn more](#)

## Frequently asked questions

### **What data is transferred from the EU or Switzerland to the United States under the Microsoft Privacy Shield agreement?**

As specified in our Online Services Terms, personal data that Microsoft processes on the customer's behalf may be transferred to, stored, and processed in the United States or any other country in which Microsoft or its affiliates or subcontractors maintain facilities. Any such transfers from the EU, however, must meet the requirements of EU law.

When personal data is transferred from the EU to the United States by:

- Online services other than the core online services (as defined in the Online Services Terms), the transfer is subject to Microsoft commitments under the Microsoft Privacy Shield Agreement.
- The core online services, the transfer is subject to Microsoft commitments under the Standard Contractual Clauses.

### **How is Microsoft accountable for EU personal data transferred to a third party?**

Microsoft accountability for personal data that it receives under the Privacy Shield and later transfers to a third party is described in the Privacy Shield Principles. In particular, Microsoft remains responsible and liable if third-party agents that it engages to process the personal data do so in a manner inconsistent with the Principles. Microsoft is, however, not liable if it proves that it is not responsible for the event giving rise to the damage.

### **Is the transfer of data under the EU-U.S. and Swiss-U.S. Privacy Shield compliant with the GDPR?**

Privacy Shield is not a GDPR compliance mechanism, but rather a framework that enables participating companies to meet the EU requirements for transferring personal data outside of the EU.

### **How does Microsoft handle complaints under the EU-U.S. and Swiss-U.S. Privacy Shield?**

If you have a complaint that is Privacy Shield-related, please let us know using the [How to Contact Us](#) section of the [Microsoft Privacy Statement](#). For any complaints that you cannot resolve with Microsoft directly, we cooperate with EU DPAs and will comply with the advice they provide. Contact us to be directed to the relevant DPA contacts. As further explained in the [Privacy Shield Principles](#), you can take advantage of a binding arbitration option to address complaints unresolved by other means.

## Resources

- [EU Data Protection Directive](#)
- [Privacy Shield Frequently Asked Questions](#)
- [Microsoft and the EU Model Clauses](#)
- [Privacy at Microsoft](#)
- [Privacy considerations in the cloud](#)
- [Compliance on the Microsoft Trust Center](#)

# United Kingdom Government-Cloud (G-Cloud)

2/5/2021 • 4 minutes to read • [Edit Online](#)

## UK G-Cloud overview

Government Cloud (G-Cloud) is a UK government initiative to ease procurement of cloud services by government departments and promote government-wide adoption of cloud computing. G-Cloud comprises a series of framework agreements with cloud services suppliers (such as Microsoft), and a listing of their services in an online store, the Digital Marketplace. These enable public-sector organizations to compare and procure those services without having to do their own full review process. Inclusion in the Digital Marketplace requires a self-attestation of compliance, followed by a verification performed by the Government Digital Service (GDS) branch at its discretion.

The G-Cloud appointment process was streamlined in 2014 to reduce the time and cost to the UK government, and the government's security classification scheme was simplified from six to three levels: OFFICIAL, SECRET, and TOP SECRET. (G-Cloud certification levels are no longer expressed as an Impact Level, or IL; Microsoft formerly held an IL2 accreditation for Microsoft Azure, Microsoft Dynamics 365, and Microsoft Office 365.)

Instead of the central assessment of cloud services previously provided, the new process requires cloud service providers to self-certify and supply evidence in support of the 14 Cloud Security Principles of G-Cloud. This has not changed either the evidence Microsoft produces or the standards that the company adheres to.

## Microsoft and UK G-Cloud

Every year, Microsoft prepares documentation and submits evidence to attest that its in-scope enterprise cloud services comply with the principles, giving potential G-Cloud customers an overview of its risk environment. (As with previous G-Cloud accreditation, it relies on the ISO 27001 certification.) A GDS accreditor then performs several random checks on the Microsoft assertion statement, samples the evidence, and makes a determination of compliance.

The appointment of Microsoft services to the Digital Marketplace means that UK government agencies and partners can use in-scope services to store and process UK OFFICIAL government data, most government data. In addition, there are now more than 450 Microsoft partners included in G-Cloud who are resellers of Microsoft cloud services. They can directly assert the compliance of in-scope services with the 14 principles in their own applications. Customers and partners, however, will need to achieve their own compliance for any components that are not included in the attestation and determination of compliance for Microsoft cloud services.

[14 Cloud Security Controls for UK cloud using Microsoft Azure](#) provides customer strategies to move their services to Azure and help meet their UK obligations mandated by the CESG/NSCS. The whitepaper provides insight into how Azure can be used to help address the 14 controls outlined in the cloud security principals, and outlines how customers can move faster and achieve more while saving money as they adopt Microsoft Azure services.

## Microsoft in-scope cloud services

- [Azure](#)
- Microsoft Cloud App Security
- [Dynamics 365](#)
- Intune
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an

Office 365 or Dynamics 365 branded plan or suite

- Office 365: Exchange Online, SharePoint Online, and Skype for Business Online
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

## Audits, reports, and certificates

To confirm that Microsoft cloud services maintain their compliance with G-Cloud agreements, the GDS accreditor may review evidence at any time, at its discretion.

### Azure

- [Azure UK G-Cloud Risk Environment](#)
- [Azure UK G Cloud Residual Risk](#)
- [Intune UK G Cloud Security Cloud Assessment Summary](#)

### Dynamics 365

- [Dynamics 365 UK G cloud Risk Environment](#)

### Intune

- [Intune UK G cloud Risk Environment](#)
- [Intune UK G cloud Residual Risk](#)
- [Azure UK G cloud Security Assessment Summary](#)

### Office 365

- [Office 365 UK G cloud Risk Environment](#)

## Accelerate your deployment of UK G-Cloud solutions on Azure

Moving your government services to the cloud is now easier than ever using the Azure Security and Compliance UK Blueprint. This blueprint provides guidance and automated scripts that get you started building compliant solutions today.

[Start using the Azure UK G-Cloud Blueprint](#)

## Frequently asked questions

### Who is eligible to use the Digital Marketplace?

All UK government departments, devolved administrations, local authorities, wider public-sector bodies, and arm's-length bodies are eligible to buy services in the marketplace. If you're uncertain of your eligibility, consult the [complete list of public-sector organizations](#).

### What is an arm's-length body?

It is an organization or agency that is funded by the UK government but acts independently of it.

### What do local datacenter locations mean for UK customers, and where are they located?

The Microsoft Cloud in the UK provides reliability and performance combined with data residency in the UK. This support provides customers with trusted cloud services that help them meet local compliance and policy requirements. In addition, replication of data in multiple datacenters across the UK gives customers geo-redundant data protection for business continuity, for both pure cloud and hybrid scenarios. We have datacenters in multiple locations across the UK.

- You can see the new Azure regions, UK West, and UK South, on the [global Azure map](#).

- For Office 365, the UK datacenters collectively comprise the new UK Office 365 region. You can see more on the [global Office 365 map](#).

### **Where are the other Microsoft EU datacenters located?**

In addition to the UK datacenters, Microsoft cloud services has data centers in multiple locations. For the most up-to-date list of all centers visit our [data location page](#).

### **How can I get copies of the auditor's reports?**

The [Service Trust Portal](#) provides independently audited compliance reports. You can use the portal to request audit reports so that your auditors can compare the Microsoft results with your own legal and regulatory requirements.

## **Resources**

- [Effective Compliance Controls to Address the UK Governments Common 14 Cloud Security Principles Using Microsoft Azure](#)
- [UK Government Cloud Strategy](#)
- [G-Cloud Security Principles](#)
- [Digital Marketplace](#)
- [Microsoft Online Services](#)
- [Compliance on the Microsoft Trust Center](#)



# IT-Grundschutz Compliance workbook

11/30/2020 • 2 minutes to read • [Edit Online](#)

## IT-Grundschutz Compliance workbook overview

To help organizations identify and implement measures to help secure IT systems, the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, or BSI) created a baseline set of standards for protecting information technology (in German, IT-Grundschutz). These BSI standards consist of:

- An information security management system (ISMS) based on ISO/IEC 27001 standards (BSI-Standard 100-1)
- The IT-Grundschutz methodology, which describes how to set up and operate an ISMS (BSI Standard 100-2)
- A risk analysis method (BSI Standard 100-3)
- The IT-Grundschutz Catalogues, a standard set of potential threats and safeguards against them for typical business environments

## Microsoft and IT-Grundschutz Compliance workbook

To help our clients achieve their IT-Grundschutz certification, Microsoft Germany has published the [IT-Grundschutz Compliance workbook](#) for solutions and workloads deployed on Azure Germany. Developed by HiSolutions AG, an independent consulting, and auditing firm in Germany, the workbook is based on the most recent version of the [IT-Grundschutz Catalogues v.15](#) (2015), which includes modules covering internet and cloud usage, such as M 1.17 Cloud Usage.

This workbook can help Microsoft Cloud Germany customers implement the IT-Grundschutz methodology within the scope of their existing or planned ISO 27001 certification. It describes how to apply the IT-Grundschutz methodology to applications in the cloud and outlines how to implement all audit-relevant safeguards from the IT-Grundschutz module, M 1.17 Cloud Usage.

## Audits, reports, and certificates

[Microsoft IT-Grundschutz Compliance workbook](#)

## Microsoft in-scope cloud services

- [Azure Germany](#)
- Intune

## Frequently asked questions

**Can I use the Microsoft IT-Grundschutz Compliance workbook to help my organization comply with IT-Grundschutz?**

Yes. The purpose of the workbook is to help Microsoft Cloud Germany customers use Microsoft Cloud Germany services to implement the IT-Grundschutz methodology within the scope of their existing or planned ISO 27001 certification based on IT-Grundschutz.

**What's the difference between IT-Grundschutz Catalogues and C5?**

The Cloud Computing Compliance Controls Catalog (C5) is an audited standard from BSI that establishes a mandatory minimum baseline for cloud security and the adoption of public cloud solutions by German

government agencies and organizations that work with government. The IT-Grundschutz Catalogues supplies the specific methodology to help organizations identify and implement security measures for IT systems and is one of the elements upon which the C5 standards are built.

### **What is Microsoft Cloud Germany?**

Microsoft Cloud Germany is physically based in Germany and adheres to the requirement of German privacy law, which strictly limits the transfer of personal data to other countries, including protection against access by authorities from other jurisdictions who could violate domestic laws. It offers Azure Germany, our public cloud computing platform, and all its services.

## **Resources**

- [IT-Grundschutz](#)
- [IT-Grundschutz Catalogues v.15 \(2015\)](#)
- [BSI Standards](#)
- [Azure Germany IT-Grundschutz Compliance workbook](#)
- [ISO/IEC 27001:2013 Information Security Management Systems background](#)
- [Compliance on the Microsoft Trust Center](#)

# Spanish Royal Decree 1720/2007, Spanish Organic Law 15/1999

11/30/2020 • 2 minutes to read • [Edit Online](#)

## Spanish Royal Decree 1720/2007, Spanish Organic Law 15/1999 overview

The AEPD is the public authority that oversees compliance with Spanish Organic Law 15/1999 for the Protection of Personal Data ([Ley Orgánica 15/1999 de Protección de Datos](#), or LOPD), including the transfer of data across international boundaries. In 2014, the AEPD reviewed Microsoft's terms and conditions applicable to the EU Model Clauses-covered Microsoft Azure, Dynamics 365, and Office 365, and issued a resolution determining that those terms provided adequate safeguards for customers to move their personal data to those services.

Title VIII of Royal Decree 1720/2007 establishes stringent requirements for processing personal data, including a specific listing of basic, intermediate-level, and high-level security measures that must be implemented. Microsoft retained an independent third-party auditing firm in Spain, BDO Auditores, to assess Microsoft Azure and Office 365 for compliance with the high-level requirements and Microsoft Dynamics 365 for compliance with the intermediate-level requirements established in Royal Decree 1720/2007. Based on interviews, visits to facilities, and a review of the environmental and physical security measures and controls, the auditor determined that Microsoft Azure and Office 365 information systems, facilities, and data processing met the high-level standard with no points requiring correction.

## Microsoft and Spanish Royal Decree 1720/2007, Spanish Organic Law 15/1999

Microsoft was the first hyper-scale cloud service provider to receive, for the benefit of its customers, an authorization from the Spanish Data Protection Agency (Agencia Española de Protección de Datos, or AEPD) for its compliance with the high standards governing international data transfer under Spanish Organic Law 15/1999 ([Ley Orgánica 15/1999 de Protección de Datos](#), or LOPD). Microsoft is also the first hyper-scale cloud service provider to obtain a third-party audit certification for its online services' compliance with the security measures set forth in Title VIII of Royal Decree 1720/2007. This authorization lets customers make transfers of personal data to Microsoft Azure, Dynamics 365, and Office 365 services covered by the European Union Model Clauses.

## Microsoft in-scope cloud services

- [Microsoft Azure](#)
- [Microsoft Dynamics 365](#)
- Intune
- [Microsoft Office 365](#)

## Audits, reports, and certificates

### Microsoft Azure

- [Certification](#) (Spanish)
- [Audit report](#) (Spanish)

### Microsoft Office 365

- [Certification](#) (Spanish)
- [Audit report](#) (Spanish)

### **Microsoft Dynamics 365**

- [Audit report](#) (Spanish)
- [Audit report](#) (English)

## Frequently asked questions

### **How does meeting the high-level standard benefit Microsoft customers?**

The high-level standard applies to the processing of sensitive data such as health information. Customers who use Microsoft Azure and Office 365 can rest assured that their sensitive data is being processed in accordance with Royal Decree 1720/2007.

### **Can I use Microsoft's compliance in my organization's certification process?**

Yes. If your organization requires or is seeking an accreditation in line with the LOPD or Royal Decree 1720/2007, you can use AEPD's authorization and the security measures certification in your compliance assessment. However, you are responsible for engaging an assessor to evaluate your implementation as deployed on Microsoft Azure, Dynamics 365, or Office 365, and for the controls and processes within your own organization.

## Resources

- Spanish Data Protection Agency ([Spanish](#))
- Organic Law 15/1999 of December 13 for the Protection of Personal Data - [Spanish](#)
- [Microsoft Online Services terms](#)
- [Compliance on the Microsoft Trust Center](#)

# Police-Assured Secure Facilities (PASF) United Kingdom

11/30/2020 • 2 minutes to read • [Edit Online](#)

## About PASF

The National Policing Information Risk Management Team (NPIRMT) of the UK Home Office (the ministry responsible for security, immigration, and law and order) is charged with ensuring that the storage of and access to police information meet its standards. Through the [National Policing Information Risk Management Policy](#), it sets the central standards and controls for law enforcement agencies across the UK that are assessing the risk of moving police information systems to the cloud. The policy requires that all national police services in the UK that store and process protectively marked or other sensitive law enforcement information take an extra step in their risk assessment: a physical inspection of the datacenter where their data will be stored. The successful assessment of a datacenter determines that it is PASF.

To assist local police services with their due-diligence review, the NPIRMT performed a PASF audit of Azure datacenters and has determined that they are compliant. Local police services can use this NPIRMT assessment to support their own review. Using the NPIRMT policy guidelines, the senior information risk owner for each police service is responsible for assessing the suitability of an individual datacenter in the context of their particular application, which they then submit to the NPIRMT for approval.

## Microsoft and PASF

The UK National Policing Information Risk Management Team (NPIRMT) completed a comprehensive security assessment of the physical infrastructure of Microsoft Azure datacenters in the UK and concluded that they are in compliance with NPIRMT requirements without any remedial actions. This successful physical audit means that Microsoft business cloud services can now support police forces across the UK who require Police-Assured Secure Facilities (PASF) to process and store their data in the cloud.

Microsoft takes a holistic defense-in-depth approach to security. Our UK datacenters (like all Microsoft datacenters) are certified to comply with the [most comprehensive portfolio](#) of internationally recognized standards of any cloud service provider and consistently meet those requirements. This compliance includes certification for our implementation of the [ISO/IEC 27001 Information Security Management Standards](#) and the [ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud](#).

These certifications are backed by the measures that we take to protect the physical security of our datacenters. We adopt a layered approach that starts with how we design, build, and operate datacenters to strictly control physical access to the areas where customer data is stored. Datacenters managed by Microsoft have extensive levels of protection with access approval required at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. This structure reduces the risk of unauthorized users gaining physical access to data and datacenter resources.

## Microsoft in-scope cloud services

- [Azure](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## Audits, reports, and certificates

The NPIRMT audits one Azure datacenter each year, annually cycling through the four Microsoft datacenters in the UK. The NPIRMT assessment that Microsoft datacenters are PASF is available through the Home Office for law enforcement customers who are conducting their own risk assessment of Azure and other Microsoft cloud services.

## How to implement

- [Azure UK Official Blueprint](#): Helps UK customers accelerate IaaS and PaaS deployments of compliant workloads in Azure.

## Frequently asked questions

**Can police departments in the UK use the Azure PASF assessment as part of their own risk assessments?**

Yes. Law enforcement can use the NPIRMT assessment of Azure to support their own local risk assessment before a move to the cloud.

## Resources

- [National Policing Accreditation Policy](#)
- [Azure facilities, premises, and physical security](#)
- [Microsoft and ISO/IEC 27001:2013 ISM Standards](#)
- [Microsoft Online Services Terms](#)
- [Compliance on the Microsoft Trust Center](#)

# Russian Personal Data Localization Requirements

2/5/2021 • 3 minutes to read • [Edit Online](#)

As of September 1, 2015, organizations that are considered personal data operators must ensure that, when collecting personal data, Russian citizens' personal data recording, systematization, accumulation, storage, clarification (updating, changing), and extraction are performed through the databases located in Russia ('personal data localization requirement').<sup>1</sup>

Microsoft services available to organizations (including but not limited to educational institutions) (hereinafter referred to as 'customer'), including those enabling personal data processing such as Microsoft Azure, Microsoft 365, Dynamics 365, and Power Platform, are provided from data processing centers located outside of Russia (for more information visit the [Microsoft Trust Center](#)).

Based on the type and content of information processed by customer information systems, such systems, including those using Microsoft cloud products, may be deemed a personal data information system ('PDIS', 'ISPD'). In cases where the customer would like to use Microsoft services in a system that qualifies as PDIS through its architecture and types of information processed, Microsoft invites its customers to consider, amongst other things, available solutions specified below. All the scenarios provided are available for customers as an additional option to standard business offerings.

It should be noted that it is the customer as personal data operator of PDIS who is in charge of compliance and shall analyze and assess applicable legal requirements for personal data localization, and at its own discretion, independently determine sufficient measures to ensure that personal data processing in PDIS complies with the Russian personal data law.<sup>2</sup>

## Subscribing to Microsoft services

### Microsoft ID Management

Microsoft invites customers to consider subscribing to Microsoft services; Microsoft Azure, Microsoft 365, Dynamics 365, and Power Platform—via a Microsoft Cloud Solution Provider (CSP) partner. For more information, see this [list of CSP partners](#).

### Managing User Identity and Access for Microsoft services

For Microsoft services such as Microsoft Azure, Microsoft 365, Dynamics 365, and Power Platform, user verification and access management are performed through [Azure Active Directory \(Azure Active Directory\)](#). In cases where a Microsoft customer uses a local identification management system for Microsoft cloud services (such as the Windows Server Active Directory (AD) or any other ID management system), the customer has an opportunity to swiftly integrate such system with the Azure Active Directory (Azure Active Directory) through Azure AD Connect. For more information, see the [Azure AD Connect](#). Microsoft customers may also consider using applications and solutions of third-party vendors for managing their users and integrating their local identification system with the Azure AD.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Questions and support

For technical and billing questions, refer to the Microsoft Support resources below. For additional questions or clarifications, contact the Microsoft [privacy team](#).

### **Microsoft Azure**

- **Website:** [Microsoft Azure support](#)
- **Toll Free:** 8 800 200 8001
- **Local Call:** 495 916 7171
- **Online support:** Submit queries via the [Azure portal](#)

### **Microsoft 365**

- **Toll Free:** 8 10 800 2548 1044
- **Local Call:** 499 922 8623
- **Online support:** Submit queries via the [Admin Center](#)

### **Dynamics 365**

- **Toll Free:** 8 10 800 2548 1044
- **Local Call:** 499 922 8623
- **Online support:** Submit queries via the [Dynamics Support portal](#)

### **Power Platform**

- **Toll Free:** 8 10 800 2548 1044
- **Local Call:** 499 922 8623
- **Online support:** Submit queries via the [Power Platform Support](#)

#### **NOTE**

<sup>1</sup> Federal Law No. 242-FZ (edition dated 12.31.2014) 'On entering amendments into certain legislative acts of the Russian Federation about clarifying the procedure for personal data processing in information and telecommunication networks' dated 07.21.2014

<sup>2</sup> Federal Law No. 152-FZ on Personal data as of 07.27. 2006



# California Consumer Privacy Act (CCPA)

2/5/2021 • 4 minutes to read • [Edit Online](#)

## CCPA overview

The California Consumer Privacy Act (CCPA) is the first comprehensive privacy law in the United States. It provides a variety of privacy rights to California consumers. Businesses regulated by the CCPA will have a number of obligations to those consumers, including disclosures, General Data Protection Regulation (GDPR)-like consumer data subject rights (DSRs), an 'opt-out' for certain data transfers, and an 'opt-in' requirement for minors.

The CCPA only applies to companies doing business in California which satisfy one or more of the following: (1) have a gross annual revenue of more than \$25 million, or (2) derive more than 50% of their annual income from the sale of California consumer personal information, or (3) buy, sell or share the personal information of more than 50,000 California consumers annually.

The CCPA goes into effect on January 1, 2020. However, enforcement by the California Attorney General (AG) will start on July 1, 2020.

The California AG will enforce the CCPA and will have power to issue non-compliance fines. The CCPA also provides a private right of action which is limited to data breaches. Under the private right of action, damages can come in between \$100 and \$750 per incident per consumer. The California AG also can enforce the CCPA in its entirety with the ability to levy a civil penalty of not more than \$2,500 per violation or \$7,500 per intentional violation.

## Microsoft and the CCPA

For commercial customers doing business in California, Microsoft will be acting as a 'service provider' with respect to our Online Services and Professional Services offering. The terms of the Online Services Terms (OST) and the Microsoft Professional Services Data Protection Addendum (MSDPA) already meet the requirements for Service Providers under the CCPA and are generally sufficient to permit customers to continue to transfer data to our Online Services. As such, no additional contractual changes are required for customers to be able to rely on Microsoft as a Service Provider under the CCPA.

As set out in the OST, Microsoft complies with all laws and regulations applicable to its provision of the Online Services, which would include the CCPA.

## Microsoft in-scope cloud services

- [Azure](#)
- Azure Dev Ops
- [Dynamics 365](#)
- Intune
- [Office 365](#)
- Support and Professional Services
- Visual Studio

## How you can prepare for your CCPA compliance when using Microsoft Products and Services

Here are a few steps you could take to get ready for the CCPA:

- Start leveraging the GDPR assessment in [Compliance Manager](#) as part of your CCPA privacy program.
- Establish a process to efficiently respond to Data Subject Access Requests (DSARs) using the Data Subject Requests tool.
- Set up label and policies to discover, classify & label, and protect sensitive data with Microsoft Information Protection.
- Use email encryption capabilities to further control sensitive information.

## Frequently asked questions

### How will the CCPA affect my company?

Many of the CCPA's rights afforded to Californians are similar to the rights the GDPR provides, including the disclosure and data subject right (DSR) requests, such as access, deletion, and portability. As such, customer can look to our already existing GDPR solutions to help them with their CCPA compliance.

To begin your CCPA journey you should focus on Discovery of information, determining how personal information is shared, governing how it is used, how it is protected and having a formal data breach response program in place.

### What are the differences between GDPR and CCPA?

There are many differences. It's easier to focus on the similarities, including:

- Transparency/disclosure obligations,
- Consumer rights to access, delete, and receive a copy of data,
- Definition of 'service providers' that is similar to how GDPR defines 'processors' with a similar contractual obligation, and
- Definition of 'businesses' that encompasses the GDPR definition of 'controllers'.

The biggest difference in CCPA is the core requirement to enable an opt-out from sales of data to third parties (with 'sale' broadly defined to include sharing of data for valuable consideration).

### What rights must companies enable under the CCPA?

The CCPA requires regulated businesses that collect, transfer, and sell personal information to, among other things:

- Provide disclosures to consumers, prior to collection, regarding the categories and purposes of collection.
- Provide more detailed disclosures in a privacy policy regarding the sources, business purposes, and categories of personal information that is collected, including how those categories are sold or transferred to other entities.
- Enable DSR rights of access, deletion, and portability for the specific pieces of personal information that has been collected by you.
- Enable a control that will permit consumers to opt out of the sale of the consumer's data. However, transfers to exempt entities, such as service providers, will be permitted.
- For minors, under 16, enable an opt-in process so that no sale of the minor's personal information can occur without actively opting-in to the sale.
- Ensure that consumers are not discriminated against for exercising any of their rights under CCPA.

### How does the CCPA apply to children?

- CCPA introduces parental consent obligations consistent with The Children's Online Privacy Protection Act (COPPA) for children under the age of 13.
- For children between 13 and 16 years old, CCPA imposes a new obligation to obtain opt-in consent from the

child.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

### Resources

- [5 tips to help you prepare for the new California Consumer Privacy Act](#)
- [Getting Started with CCPA Guide](#)
- [Data Subject Requests and the GDPR](#)
- [California Consumer Privacy Act \(CCPA\) FAQ](#)
- [Compliance on the Microsoft Trust Center](#)

# Canadian Privacy Laws

2/5/2021 • 4 minutes to read • [Edit Online](#)

## About Canadian Privacy Laws

Canadian privacy laws were established to protect the privacy of individuals and give them the right to access information gathered about them. The [Office of the Privacy Commissioner of Canada](#) (OPCC) oversees compliance with these laws.

The [Privacy Act](#) regulates how federal government organizations collect, use, and disclose personally identifiable information including that of federal employees. The [Personal Information Protection and Electronic Documents Act](#) (PIPEDA) governs the same for the business activities of commercial for-profit enterprises and for the employees of federally regulated businesses like banks, airlines, and telecommunications companies.

PIPEDA is founded on 10 [fair information principles](#) that businesses must follow if they are to comply with it. For example, the basic principle of consent gives rise to the PIPEDA requirement that organizations must obtain an individual's permission to collect or use their personal information. Individuals have the right both to access that personal information and challenge its accuracy (grounded in the principle of 'individual access'). The principle of 'identifying purposes' leads to the rule that personal information can be used only for the purposes agreed upon.

In general, PIPEDA applies to commercial activities in all provinces and territories, except those operating entirely within provinces with their own privacy laws that have been declared 'substantially similar' to the federal law. For example, British Columbia, Alberta, and Quebec have private sector privacy legislation deemed substantively similar to PIPEDA, and as a result the provincial laws are followed there in place of the federal legislation.

## Microsoft and Canadian privacy laws

Microsoft Azure and Microsoft Intune are built with established ISO/IEC security standards in mind, and Microsoft maintains technical and organizational measures to protect customer data. These measures comply with the requirements set forth in such established security standards as [ISO/IEC 27001](#) and ISO/IEC 27002, and the code of practice for cloud privacy, [ISO/IEC 27018](#). Microsoft has assessed its practices in risk, security, and incident management; access control; data integrity protection; and other areas relative to the recommendations from the Office of the Privacy Commissioner of Canada, and has determined that in-scope Azure and Intune services can meet those recommendations. This support means that Azure and Intune can help customers meet the requirements of Canadian privacy laws.

To support public- and private-sector organizations that are concerned about data sovereignty, Microsoft has established two datacenters in Canada in Toronto and Quebec City. These datacenters add in-country data residency, failover, and disaster recovery for core customer data at rest as defined in the [Microsoft Online Services Terms](#).

To assist Canadian customers who are considering outsourcing business functions to the cloud, Microsoft has published [Navigating your way to the cloud: A compliance checklist for financial institutions in Canada](#). This document provides an overview of the regulatory landscape, including privacy regulations, and a detailed listing of how Microsoft business cloud services can help organizations meet contractual requirements for material outsourcing arrangements.

## Microsoft in-scope cloud services

- [Azure](#)
- [Intune](#)

## How to implement

- [Privacy at Microsoft](#): Get details on Microsoft privacy principles and standards and on privacy laws specific to Canada.
- [Compliance checklist for Canada](#): Learn more about Azure and Intune functionalities that can help meet Canadian privacy laws.
- [Azure data protection](#): Azure provides customers with strong data security, both by default and as customer options.

## Frequently asked questions

### Can customers using Azure and Intune comply with PIPEDA and other Canadian privacy laws?

Microsoft agrees in its [Online Services Terms](#) that it complies with laws and regulations that apply to its provision of Microsoft Online Services. However, organizations that use Microsoft business cloud services always remain accountable for adherence to Canadian privacy legislation, the laws are clear that organizations are ultimately responsible for ensuring that any sensitive data they gather is fairly handled and adequately protected.

As a result, privacy is a shared responsibility between Microsoft as a cloud service provider and the customer using cloud services. At a high level, this requirement means that customers must ensure that their solutions implemented within Microsoft environments address the 10 principles codified in PIPEDA. For example, getting the consent of individuals to collect their data and safeguarding it with adequate security measures.

### What third-party audits validate the security control environment of Azure and Intune?

Azure and Intune are built on such established security standards as [ISO/IEC 27001](#) and the [SOC framework](#). Their compliance with these standards is confirmed by third-party auditors who provide independent validation that security controls are in place and operating effectively.

Each audit results in the generation of an audit report, which Microsoft makes available either on the [Microsoft Service Trust Portal](#) or at another location. Microsoft provides audit reports to customers who request them, subject to non-disclosure and distribution limitations of Microsoft and the auditor.

### Will customers know the physical location where their data is stored?

Canadian customers of Microsoft business cloud services will [know where their customer data is stored](#). Furthermore, no matter where customer data is located, Microsoft does not control or limit the locations from which customers or their end users may access their data.

PIPEDA doesn't require Canadian businesses to keep personal information in Canada. However, depending on the province where organizations do business, or their industry, they could be required to keep certain types of data within Canadian borders. To help address these types of requirements, Microsoft has established two datacenters in Canada that support Azure and Intune—in Toronto and Quebec City, and verifies that each datacenter meets stringent security requirements.

## Resources

- [Summary of privacy laws in Canada](#) (OPCC)
- [Privacy at Microsoft](#)
- [Microsoft Privacy Statement](#)
- [Privacy considerations in the cloud](#)

- [Compliance on the Microsoft Trust Center](#)

# Personal Data Protection Act (PDPA) Argentina

2/5/2021 • 2 minutes to read • [Edit Online](#)

## About the PDPA

In agreement with the Argentine National Constitution, the [Personal Data Protection Act 25.326](#) (PDPA) ([Ley de Protección de los Datos Personales](#)) was executed in 2000 to help protect the privacy of personal data, and to give individuals access to any information stored in public and private databases and registries. The Argentine Agency of Access to Public Information ([Agencia de Acceso a la Información Pública](#), AAIP) within the Chief of Ministries' Cabinet is responsible for enforcing this law.

The PDPA aligns with the European legislative model for protecting data privacy, and Argentina was the first country in Latin America to achieve an 'adequacy' qualification for data transfers from the EU.

In 2016, the AAIP issued a new regulation, [Provision 60-E/2016](#) (Spanish), governing cross-border transfers of personal data. Under the rule, it approved model forms (partly based on the data transfer model in the EU) for such transfers to data controllers and data processors.

## Microsoft and the PDPA

Microsoft contractually commits through the [Microsoft Online Services Terms](#) that our in-scope business cloud services have implemented technical and organizational security safeguards that can help our customers comply with the Argentine Personal Data Protection Act (PDPA) 25.326. Microsoft also makes a data-transfer agreement available to help with compliance with Provision 60-E/2016, which regulates the cross-border transfer of personal data. This means that Microsoft customers can use Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 in a manner that complies with the PDPA in Argentina.

The technical and organizational security measures implemented in the business cloud services would also support other rules in the PDPA such as the prohibition of any secondary use of a data subject's personal data and the prohibition against the transfer of personal data to countries that do not offer an adequate level of protection.

The Microsoft data-transfer agreement is an amendment (Amendment ID M314) to the data processing terms in our Online Services Terms. It adds important commitments, including that Microsoft notifies the customer of any legally binding request to disclose personal data; will submit its data processing facilities to audit at the customer's request either by the customer or an independent third party; and will get prior written consent for the use of subcontractors.

## Microsoft in-scope cloud services

- [Azure & Azure DevOps](#)
- [Dynamics 365](#)
- [Microsoft 365](#)

## How to implement

- [Privacy in Microsoft Cloud Services](#): Get details on Microsoft privacy principles and standards and on privacy laws specific to Argentina.
- [Azure data protection](#): Azure offers customers strong data security, both by default and as customer options.

# Frequently asked questions

## How has the GDPR changed the Personal Data Protection Act?

In late 2018, Argentina has not yet enacted GDPR-related regulations, but it has drafted a new data protection bill — already submitted to Congress by the Executive Power and under revision by the House of Representatives — to bring its data protection law into alignment with the GDPR. It addresses such differences as the definition of data subjects and concerns over the cross-border transfer of personal information.

## Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager offers a premium template for building an assessment for this regulation. Find the template in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Resources

- [Privacy at Microsoft](#)
- [Microsoft Privacy Statement](#)
- [Privacy Considerations in the Cloud](#)
- [Compliance on the Microsoft Trust Center](#)



# General Data Protection Regulation Summary

2/18/2021 • 21 minutes to read • [Edit Online](#)

The General Data Protection Regulation (GDPR) introduces new rules for organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents no matter where you or your enterprise are located. This document guides you to information to help you honor rights and fulfill obligations under the GDPR when using Microsoft products and services. A [Recommended action plan for GDPR](#) and [Accountability Readiness Checklists](#) provide additional resources for assessing and implementing GDPR compliance.

## Terminology

Helpful definitions for GDPR terms used in this document:

- **Data Controller (Controller):** A legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Personal data and data subject:** Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly.
- **Processor:** A natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller.
- **Customer Data:** Data produced and stored in the day-to-day operations of running your business.

## What is the GDPR?

The GDPR gives rights to people to manage personal data collected by an organization. These rights can be exercised through a Data Subject Request (DSR). The organization is required to provide timely information regarding DSRs and data breaches, and perform Data Protection Impact Assessments (DPIAs).

Several points should be considered when implementing or assessing GDPR requirements:

- Developing or evaluating your GDPR-compliance data privacy policy.
- Assessing the data security of your organization.
- Who is your data controller?
- What data security processes may you have to perform?

The [Recommended action plan for GDPR](#) and [Accountability Readiness Checklists](#) may prompt additional thinking points.

The following tasks are involved to meet GDPR standards. Follow the links in the list for details regarding your implementation.

- **Data subject requests (DSR).** A formal request by a data subject to a controller to take an action (change, restrict, access) regarding their personal data.
- **Breach notification.** Under GDPR, a personal data breach is 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.'
- **Data protection impact assessment (DPIA).** Data controllers are required under GDPR to prepare a DPIA for data operations that are 'likely to result in a high risk to the rights and freedoms of natural persons.'

As mentioned above, the Recommended action plan for GDPR and Accountability Readiness Checklists provide a guide to implementing or assessing GDPR conformance using Microsoft products and services.

# Use Microsoft Compliance Manager to assess your risk

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager has a pre-built assessment for this regulation for Enterprise E5 customers. Find the template for building the assessment in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

## Data Subject Request (DSR)

The GDPR grants individuals (or data subjects) certain rights in connection with the processing of their personal data, including the right to correct inaccurate data, erase data or restrict its processing, receive their data and fulfill a request to transmit their data to another controller. The controller is responsible for providing a timely, GDPR consistent reply. For technical details, refer to [Data Subject Requests](#).

### DSR FAQs

#### What actions will be required to complete a DSR?

DSRs involve six activities: Discovery, Access, Rectification, Restriction, Export, and Deletion.

#### What are your data sources?

A large fraction of an organization's data is generated in [Office applications](#) such as Excel and Outlook. You may also find data relevant to a DSR in [Insights](#) generated by Microsoft products and services, and [system-generated logs](#).

#### What kinds of data need to be searched?

Personal data may be found in customer data, insights generated by Microsoft products and services, and system-generated logs.

#### How will personal data be searched?

Searching for personal data may vary across Microsoft products and services. Search tools include [Content Search](#), or [in-app search](#) capacity. Administrators may access [system-generated logs](#) associated with a user's activity.

#### In what formats should personal data be made available?

The GDPR 'right of data portability' allows a data subject to request a copy of personal data in a 'structured, commonly used, machine-readable format', and to request that your organization transmit these files to another data controller.

#### What does the GDPR require and what are my responsibilities as the controller?

As controller, the GDPR requires you to be able to:

- Give data subjects a copy of their personal data, together with an explanation of the categories of their data that are being processed, the purposes of that processing, and the categories of third parties to whom their data may be disclosed.
- Help every individual exercise their right to correct inaccurate personal data, erase data or restrict its processing, receive their data in a readable form, and where applicable, fulfill a request to transmit their data to another controller.

#### What does the GDPR require and what are the responsibilities of Microsoft as processor?

We must implement the appropriate technical and organizational measures to assist you in responding to requests from data subjects exercising their rights as discussed above.

## Where can I find GDPR-related information for on-premises servers?

You can find a series of GDPR-related articles here. Produced by Microsoft, they provide recommended approaches for on-premises workload for SharePoint Server, Exchange Server, Project Server, Office Web Apps Server, Office Online Server, and on-premises file shares.

## How does Microsoft enable you to respond to data subject requests?

Online Services offers a host of capabilities to enable you, as a controller, to respond to a data subject's request. Microsoft enterprise online services and administrative controls help you act on personal data responsive to data subject rights requests, allowing you to discover, access, rectify, restrict, delete, and export personal data that resides in the controller-managed data stored in Microsoft's cloud. Online Services also provides data in machine-readable form should you need it.

# Data Protection Impact Assessment

Under GDPR, data controllers are required to prepare a [Data Protection Impact Assessment](#) (DPIA) for processing operations that are 'likely to result in a high risk to the rights and freedoms of natural persons.' There is nothing inherent in Microsoft products and services that need the creation of a DPIA. Rather, it depends on the details of your Microsoft configuration. A list of details that must be considered in Office can be found in [Contents of DPIA](#)

## DPIA FAQs

### When should you conduct a DPIA?

Controllers are required to perform a DPIA addressing risks to personal data security or as a result of a data breach. Specific examples of risk factors in Office are addressed in [Determining Whether a DPIA is Needed](#).

### What is required to complete a DPIA?

The GDPR mandates that a DPIA includes:

- Assessment of the necessity, and proportionality of data processing in relation to the DPIA's purpose.
- An assessment of the risks to the rights and freedoms of data subjects.
- Intended measures to address the risks, safeguards, security measures, and mechanisms to ensure the protection of personal data and demonstrate compliance with the GDPR.

### What are my responsibilities as a Controller?

Under the GDPR, as a controller you are required to undertake DPIAs prior to data processing that is likely to result in a high risk to the rights and freedoms of individuals—in particular, processing using new technologies. The GDPR provides the following non-exhaustive list of cases in which DPIAs must be carried out:

- Automated processing for the purposes of profiling and similar activities that has legal effects or similarly significantly affects data subjects;
- Processing on a large scale of special categories of personal data—data revealing racial or ethnic origin, political opinion, and the like—or of data relating to criminal convictions and offenses;
- Systematic monitoring of a publicly accessible area on a large scale.

The GDPR also requires that you must consult with your Data Protection Authority (DPA) before you begin any processing if you cannot identify sufficient processes to minimize high risks to data subjects.

### What are the responsibilities of Microsoft?

Microsoft practices privacy by design and privacy by default in its engineering and business functions. As part of these efforts, Microsoft performs comprehensive privacy reviews on data processing operations that have the potential to cause impacts to the rights and freedoms of data subjects. Privacy teams embedded in the service

groups review the design and implementation of services to ensure that personal data is processed in a respectful manner that accords with international law, user expectations, and our express commitments.

These privacy reviews tend to be granular — a particular service may receive dozens or hundreds of reviews. Microsoft rolls up these granular privacy reviews into Data Protection Impact Assessments (DPIAs) that cover major groupings of processing, which the Microsoft EU Data Protection Officer (DPO) then reviews. The DPO assesses the risks related to the data processing to ensure that sufficient mitigations are in place. If the DPO finds unmitigated risks, changes are recommended back to the engineering group. DPIAs will be reviewed and updated as data protection risks change.

Microsoft, as a processor, has a duty to assist controllers in ensuring compliance with the DPIA requirements laid out in the GDPR. To support our customers, relevant sections of Microsoft's DPIAs are abstracted and will be provided through this section in future updates with the intent of allowing controllers relying on Microsoft services to leverage the abstracts in order to create their own DPIAs.

## Breach Notification

The GDPR mandates notification requirements for data controllers and processors for a breach of personal data. As a data processor, Microsoft ensures that customers are able to meet the GDPR's breach notification requirements. Data controllers are responsible for assessing risks to data privacy and determining whether a breach requires notification of a customer's DPA. Microsoft provides the information needed to make that assessment. More information about how Microsoft detects and responds to a breach of personal data in [Data Breach Notification Under the GDPR](#).

### **Breach notification FAQs**

#### **What constitutes a breach of personal data under the GDPR?**

Personal data means any information related to an individual that can be used to identify them directly or indirectly. A personal data breach is 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.'

#### **What are your responsibilities as the controller?**

If a breach of personal data that is likely to result in a high risk to the rights and freedoms of individuals (such as discrimination, identity theft, fraud, financial loss, or damage to their reputation) occurs, the GDPR requires you to:

- Notify the appropriate Data Protection Authority (DPA) within 72 hours of becoming aware of it—for example, after Microsoft notifies you. If you don't notify the DPA within that time period, you'll need to explain why to the DPA. This notice to the DPA is required even where there is a risk to individuals that is not likely to result in a high risk.
- Notify the data subjects of the breach without undue delay.
- Document the breach including a description of the nature of the breach—such as how many people were impacted, the number of data records affected, the consequences of the breach, and any remedial action your organization is proposing or took.

#### **What are the responsibilities of Microsoft as the processor?**

After we become aware of a personal data breach, the GDPR requires us to notify you without undue delay. Where Microsoft is a processor our obligations reflect both GDPR requirements and our standard, worldwide contractual provisions. We consider that all confirmed personal data breaches are in scope; there is no risk of harm threshold. We will notify our customers whether the data breach was suffered by Microsoft directly or by any of our sub-processors. We have processes in place to quickly identify and contact security incident personnel you've identified in your organization. In addition, all sub-processors are contractually obliged to report their own breaches to Microsoft, and provide guarantees to that effect.

## How will Microsoft detect a data breach?

All our services and personnel follow internal incident management procedures to ensure that we take proper precautions to avoid data breaches in the first place. However, in addition, Online Services have specific security controls in place across our platforms to detect data breaches in the rare event that they occur.

## How will Microsoft respond to a data breach?

To support you for a breach of personal data Microsoft has: - Security personnel trained on the specific procedures to follow. - Has policies, procedures, and controls in place to ensure that Microsoft maintains detailed records. This response includes documentation that captures the facts of the incident, its effects, and remedial action, as well as tracking and storing information in our incident management systems.

## How will Microsoft notify me in the event of a data breach?

Microsoft has policies and procedures in place to notify you promptly. To satisfy your notice requirements to the DPA, we will provide a description of the process we used to determine if a breach of personal data has occurred, a description of the nature of the breach and a description of the measures we took to mitigate the breach.

# Accountability Readiness Checklists for the GDPR

These [checklists](#) provide a convenient way to access information you may need to support the GDPR using Microsoft products. You can manage checklist items with [Microsoft Compliance Manager](#) by referencing the Control ID and Control Title under Customer Managed Controls in the GDPR tile.

## GDPR FAQs

### Does Microsoft make commitments to its customers with regard to the GDPR?

Yes. The GDPR requires controllers (such as organizations using Microsoft's enterprise online services) only use processors (such as Microsoft) that provide sufficient guarantees to meet key requirements of the GDPR. Microsoft has taken the proactive step of providing these commitments to all Volume Licensing customers as part of their agreements.

### How does Microsoft help me comply?

Microsoft provides tools and documentation to support your GDPR accountability. This includes support for Data Subject Rights, performing your own Data Protection Impact Assessments, and working together to resolve personal data breaches.

### What commitments are in the GDPR Terms?

Microsoft's GDPR Terms reflect the commitments required of processors in Article 28. Article 28 requires that processors commit to:

- Only use subprocessors with the consent of the controller and remain liable for subprocessors.
- Process personal data only on instructions from the controller, including with regard to transfers.
- Ensure that persons who process personal data are committed to confidentiality.
- Implement appropriate technical and organizational measures to ensure a level of personal data security appropriate to the risk.
- Assist controllers in their obligations to respond to data subjects' requests to exercise their GDPR rights.
- Meet the breach notification and assistance requirements.
- Assist controllers with data protection impact assessments and consultation with supervisory authorities.
- Delete or return personal data at the end of provision of services.
- Support the controller with evidence of compliance with the GDPR.

## Under what basis does Microsoft facilitate the transfer of personal data outside of the EU?

Microsoft has long used the Standard Contractual Clauses (also known as the Model Clauses) as a basis for transfer of data for its enterprise online services. The Standard Contractual Clauses are standard terms provided by the European Commission that can be used to transfer data outside the European Economic Area in a compliant manner. Microsoft has incorporated the Standard Contractual Clauses into all of our Volume Licensing agreements via the [Online Services Terms](#). For personal data from the European Economic Area, Switzerland, and the United Kingdom, Microsoft will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. In addition to Microsoft's commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft continues to abide by the terms of the [Privacy Shield framework](#) but will no longer rely on it as a basis for the transfer of personal data from the EU/EEA to the United States.

## What are the other Microsoft compliance offerings?

As a global company with customers in nearly every country in the world, Microsoft has a robust compliance portfolio to assist our customers. To view a complete list of our compliance offerings including FedRamp, HIPAA/HITECH, ISO 27001, ISO 27002, ISO 27018, NIST 800-171, UK G-Cloud, and many others visit our [compliance offering topics](#).

## How will GDPR affect my company?

The GDPR imposes a wide range of requirements on organizations that collect or process personal data, including a requirement to comply with six key principles:

- *Transparency, fairness, and lawfulness* in the handling and use of personal data. You will need to be clear with individuals about how you are using personal data and will also need a "lawful basis" to process that data.
- Limiting the processing of personal data to *specified, explicit, and legitimate purposes*. You will not be able to reuse or disclose personal data for purposes that are not "compatible" with the purpose for which the data was originally collected.
- *Minimizing the collection and storage of personal data* to that which is adequate and relevant for the intended purpose.
- Ensuring the *accuracy of personal data* and enabling it to be *erased or rectified*. You will need to take steps to ensure that the personal data you hold is accurate and can be corrected if errors occur.
- *Limiting the storage of personal data*. You will need to ensure that you retain personal data only for as long as necessary to achieve the purposes for which the data was collected.
- Ensuring *security, integrity, and confidentiality of personal data*. Your organization must take steps to keep personal data secure through technical and organizational security measures.

You will need to understand what your organization's specific obligations are to the GDPR are and how you will meet them, though Microsoft is here to help you on your GDPR journey.

## What rights must companies enable under GDPR?

The GDPR provides EU residents with control over their personal data through a set of 'data subject rights'. This includes the right to:

- Access information about how personal data is used.
- Access personal data held by an organization.
- Have incorrect personal data deleted or corrected.
- Have personal data rectified and erased in certain circumstances (sometimes referred to as the "right to be forgotten").
- Restrict or object to automated processing of personal data.
- Receive a copy of personal data.

## **What are Processors and Controllers?**

A controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. A processor is a natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller.

## **Does the GDPR apply to Processors and Controllers?**

Yes, the GDPR applies to both controllers and processors. Controllers must only use processors that take measures to meet the requirements of the GDPR. Under the GDPR, processors face additional duties and liability for noncompliance, or acting outside of instructions provided by the controller, as compared to the Data Protection Directive. Processor duties include, but are not limited to:

- Processing data only as instructed by the controller.
- Using appropriate technical and organizational measures to protect personal data.
- Assisting the controller with data subject requests.
- Ensuring subprocessors it engages meet these requirements.

## **How much can companies be fined for noncompliance?**

Companies can be fined up to €20m or 4% of annual global turnover, whichever is greater, for failure to meet certain GDPR requirements. Additional individual remedies could increase your risk if you fail to adhere to GDPR requirements.

## **Does my business need to appoint a Data Protection Officer (DPO)?**

It depends on several factors identified within the regulation. Article 37 of the GDPR states that controllers and processors shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offenses referred to in Article 10.

## **How much will it cost to meet compliance with the GDPR?**

Meeting compliance with the GDPR will cost time and money for most organizations, though it may be a smoother transition for those who are operating in a well-architected cloud services model and have an effective data governance program in place.

## **How do I know if the data that my organization is processing is covered by the GDPR?**

The GDPR regulates the collection, storage, use, and sharing of 'personal data'. Personal data is defined broadly under the GDPR as any data that relates to an identified or identifiable natural person.

Personal data can include, but is not limited to, online identifiers (for example, IP addresses), employee information, sales databases, customer services data, customer feedback forms, location data, biometric data, CCTV footage, loyalty scheme records, health, and financial information and much more. It can even include information that does not appear to be personal—such as a photo of a landscape without people—where that information is linked by an account number or unique code to an identifiable individual. And even personal data that has been pseudonymized can be personal data if the pseudonym can be linked to a particular individual.

Processing of certain "special" categories of personal data, such as personal data that reveals a person's racial or ethnic origin, or concerns their health or sexual orientation, is subject to more stringent rules than the processing of "ordinary" personal data. This evaluation of personal data is highly fact-specific, so we recommend engaging an expert to evaluate your specific circumstances.

**My organization is only processing data on behalf of others. Does it still need to comply with the**

## GDPR?

Yes. Although the rules differ somewhat, the GDPR applies to organizations that collect and process data for their own purposes ('controllers') as well as to organizations that process data on behalf of others ('processors'). This requirement is a shift from the existing Data Protection Directive, which applies to controllers.

### What specifically is deemed personal data?

Personal data is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. Personal data can include:

- Name
- Home address
- Work address
- Telephone number
- Mobile number
- Email address
- Passport number
- National ID card
- Social Security Number (or equivalent)
- Driver's license
- Physical, physiological, or genetic information
- Medical information
- Cultural identity
- Bank details / account numbers
- Tax file number
- Work address
- Credit/Debit card numbers
- Social media posts
- IP address (EU region)
- Location / GPS data
- Cookies

### Am I allowed to transfer data outside of the EU?

Yes, however the GDPR strictly regulates transfers of personal data of European residents to destinations outside the European Economic Area. You may need to set up a specific legal mechanism, such as a contract, or adhere to a certification mechanism in order to enable these transfers. Microsoft details the mechanisms we use in the Online Services Terms.

### I have data retention requirements through compliance. Do these requirements override the right to erasure?

Where there are legitimate grounds for continued processing and data retention, such as 'for compliance with a legal obligation, which requires processing by Union or Member State law to which the controller is subject' (Article 17(3)(b)), the GDPR recognizes that organizations may be required to retain data. You should, however, make sure you engage your legal counsel to ensure that the grounds for retention are weighed against the rights and freedoms of the data subjects, their expectations at the time the data was collected, etc.

### Does the GDPR deal with encryption?

Encryption is identified in the GDPR as a protective measure that renders personal data unintelligible when it is affected by a breach. Therefore, whether or not encryption is used may impact requirements for notification of a personal data breach. The GDPR also points to encryption as an appropriate technical or organizational measure



in some cases, depending on the risk. Encryption is also a requirement through the Payment Card Industry Data Security Standard and part of the strict compliance guidelines specific to the financial services industry. Microsoft products and services such as Azure, Dynamics 365, Enterprise Mobility + Security, Office Microsoft 365, SQL Server/Azure SQL Database, and Windows 10 offer robust encryption for data in transit and data at rest.

### **How does the GDPR change an organization's response to personal data breaches?**

The GDPR will change data protection requirements and make stricter obligations for processors and controllers regarding notice of personal data breaches. Under the new regulation, the processor must notify the data controller of a personal data breach, after having become aware of it, without undue delay. Once aware of a personal data breach, the controller must notify the relevant data protection authority within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, controllers will also need to notify impacted individuals without undue delay. Additional guidance on this topic is being developed by the EU's Article 29 Working Party.

Microsoft products and services—such as Azure, Dynamics 365, Enterprise Mobility + Security, Microsoft Office 365, and Windows 10—have solutions available today to help you detect and assess security threats and breaches and meet the GDPR's breach notification obligations.

## **Additional resources**

- [Address your needs around GDPR with one of our global partners offering Microsoft-based solutions](#)
- [Know how Microsoft manages your data, where it's located, who can access it and the terms, and more.](#)
- [How Microsoft Detects and Responds to a Breach of Personal Data, and Notifies You Under the GDPR](#)
- [Assess your GDPR readiness today](#)

# Microsoft 365 GDPR action plan — Top priorities for your first 30 days, 90 days, and beyond

2/5/2021 • 6 minutes to read • [Edit Online](#)

This article includes a prioritized action plan you can follow as you work to meet the requirements of the General Data Protection Regulation (GDPR). This action plan was developed in partnership with Protiviti, a Microsoft partner specializing in regulatory compliance.

The GDPR introduces new rules for companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents. The GDPR applies no matter where you or your enterprise are located.

## Action plan outcomes

These recommendations are provided across three phases in a logical order with the following outcomes:

PHASE	OUTCOMES
30 days	<p><b>Understand your GDPR requirements and consider engaging with a Microsoft GDPR Advisory Partner.</b></p> <ul style="list-style-type: none"><li>* Benchmark your readiness and get recommendations for next steps.</li><li>* Work with a Microsoft GDPR Advisory Partner to establish internal guidelines for responding to Data Subject Requests (DSRs), perform a GDPR compliance gap analysis for your organization and establish a roadmap to compliance.</li></ul> <p><b>Start discovering the types of personal data you are storing and where it resides to comply with DSRs.</b></p> <ul style="list-style-type: none"><li>* Use Content search and eDiscovery in the security and compliance centers to discover personal data across the organization.</li><li>* When working with vast quantities of content, use Advanced eDiscovery, powered by machine learning technologies, to perform more efficient, and accurate content searches.</li></ul>

PHASE	OUTCOMES
90 days	<p><b>Start implementing compliance requirements using Microsoft 365 data governance and compliance capabilities.</b></p> <ul style="list-style-type: none"> <li>* Assess and manage your compliance risks by using Microsoft Compliance Manager.</li> <li>* Help users identify and classify personal data, as defined by the GDPR.</li> </ul> <p><b>Use Microsoft 365 security capabilities to prevent data breaches and implement protections for personal data.</b></p> <ul style="list-style-type: none"> <li>* Protect administrator and end-user accounts.</li> <li>* Protect against malicious code and implement data breach prevention and response.</li> <li>* Use audit logging to monitor for potentially malicious activity and to enable forensic analysis of data breaches.</li> <li>* Use Data Loss Prevention (DLP) policies to identify and protect sensitive data.</li> <li>* Prevent the most common attack vectors including phishing emails and Office documents containing malicious links and attachments.</li> </ul>
Beyond 90 days	<p><b>Use Microsoft 365 advanced data governance tools and information protection to implement ongoing governance programs for personal data.</b></p> <ul style="list-style-type: none"> <li>* Automatically identify personal information in documents and emails.</li> <li>* Protect personal data stored on devices across the organization, and ensure that compliant corporate devices are used to access sensitive data.</li> <li>* Ensure that sensitive personal information is stored and accessed according to corporate policies.</li> <li>* Implement data retention policies to help ensure that you are only retaining personal data for as long as necessary.</li> </ul> <p><b>Monitor ongoing compliance across Microsoft 365 and other Cloud applications. Consider addressing data residency requirements for EU personal data.</b></p> <ul style="list-style-type: none"> <li>* Monitor usage of cloud applications and implement advanced alerting policies for your organization.</li> <li>* Address data residency requirements as one global organization.</li> </ul>

## 30 days — Powerful quick wins

These tasks are quick and powerful with low impact to users.

AREA	TASKS

AREA	TASKS
<p><b>Understand your GDPR requirements and consider engaging with a Microsoft GDPR Advisory Partner.</b></p>	<ul style="list-style-type: none"> <li>* Use the <a href="#">Microsoft GDPR Assessment Tool</a> to privately benchmark your readiness and get recommendations for next steps.</li> <li>* Assess and manage your compliance risks by using <a href="#">Microsoft Compliance Manager</a> in the <a href="#">Microsoft 365 compliance center</a> to conduct a GDPR Assessment of your organization.</li> <li>* Work with your <a href="#">Microsoft GDPR Advisory Partner</a> to establish internal guidelines to respond to Data Subject Requests (DSRs) and exclusions from DSRs.</li> <li>* Work with your Microsoft GDPR Advisory partner to perform a gap analysis in GDPR compliance for your organization, and develop a roadmap that charts your journey to GDPR compliance.</li> <li>* Learn how to use the <a href="#">GDPR Dashboard and Data Subject Request capability</a> in the Microsoft 365 compliance center.</li> </ul>
<p><b>Start discovering the types of personal data you are storing and where it resides to comply with DSRs.</b></p>	<ul style="list-style-type: none"> <li>* Use <a href="#">Content Search</a> and <a href="#">eDiscovery cases</a> to easily search across mailboxes, public folders, Microsoft 365 Groups, Microsoft Teams, SharePoint Online sites, One Drive for Business sites and Skype for Business conversations. Learn how to use <a href="#">sensitive information types</a> to find personal data of EU citizens</li> <li>* When working with vast quantities of content, identify documents that are relevant to a particular subject (for example, a compliance investigation) quickly and with better precision than traditional keyword searches with <a href="#">Advanced eDiscovery (classic)</a>, powered by machine learning technologies.</li> <li>* Preview search results, get keyword statistics for one or more searches, bulk-edit content searches, and <a href="#">export the results</a> using the Security &amp; Compliance Center.</li> </ul>

## 90 days — Enhanced protections

These tasks take a bit more time to plan and implement but greatly increase your security posture.

AREA	TASKS
<p><b>Start implementing compliance requirements using Microsoft 365 data governance and compliance capabilities.</b></p>	<ul style="list-style-type: none"> <li>* Manage your GDPR Compliance with <a href="#">Microsoft Compliance Manager</a> within the <a href="#">Microsoft 365 compliance center</a>.</li> <li>* Help users identify and classify personal data, as defined by the GDPR, with a classification schema and associated Office 365 Labels for Exchange email, SharePoint sites, OneDrive for Business sites and Microsoft 365 Groups. See <a href="#">Office 365 Information Protection for GDPR</a>.</li> </ul>

AREA	TASKS
<p><b>Use Microsoft 365 security capabilities to prevent data breaches and implement protections for personal data.</b></p>	<ul style="list-style-type: none"> <li>* Improve authentication for administrators and end users in the Microsoft Cloud by enabling <a href="#">multi-factor authentication</a> for all user accounts and <a href="#">modern authentication</a> for all apps. For recommended policy configuration, see <a href="#">Identity and device access configurations</a>.</li> <li>* Deploy <a href="#">Windows Defender Advanced Threat Protection (ATP)</a> to all desktops for protection against malicious code, data breach prevention, and responses.</li> <li>* Enable <a href="#">audit logging</a> and <a href="#">mailbox auditing</a> for all Exchange mailboxes to monitor for potentially malicious activity and to enable forensic analysis of data breaches.</li> <li>* Configure, test, and deploy <a href="#">Office 365 Data Loss Prevention (DLP) policies</a> to identify, monitor and <a href="#">automatically protect</a> over 80 common sensitive data types within documents and emails, including financial, medical, and personally identifiable information.</li> <li>* Implement <a href="#">Office 365 Advanced Threat Protection (ATP)</a> to help prevent the most common attack vectors including phishing emails and Office documents containing malicious links and attachments.</li> </ul>

## Beyond 90 Days — Ongoing Security, Data Governance, and Reporting

Secure personal data at rest and in transit, detect and respond to data breaches, and facilitate regular testing of security measures. These configurations are important security measures that build on previous work.

AREA	TASKS
<p><b>Use Microsoft 365 advanced data governance tools and information protection to implement ongoing governance programs for personal data.</b></p>	<ul style="list-style-type: none"> <li>* Use <a href="#">Office 365 Advanced Data Governance</a> to identify personal information in documents and emails by automatically applying Office 365 Labels.</li> <li>* Protect personal data stored on devices across the organization by deploying Microsoft Intune.</li> <li>* Implement <a href="#">AAD Conditional Access policies</a> with Microsoft Intune to ensure that sensitive personal information is stored and accessed according to corporate policies. For recommended policy configuration, see <a href="#">Identity and device access configurations</a></li> <li>* Implement data retention policies with Office 365 Labels, Advanced Data Governance, and Retention Policies to retain personal data for as long as necessary in your jurisdiction.</li> </ul>
<p><b>Monitor ongoing compliance across Microsoft 365 and other Cloud applications. Consider addressing data residency requirements for EU personal data.</b></p>	<ul style="list-style-type: none"> <li>* Use <a href="#">Office 365 Alert Policies</a>, <a href="#">data loss prevention reports</a> and <a href="#">Microsoft Cloud App Security</a> to monitor usage of cloud applications and implement advanced alerting policies based on heuristics and user activity.</li> <li>* Address organizational, regional, and local data residency requirements while configured as one global organization using Microsoft's multi-geo capabilities for <a href="#">Exchange Online mailboxes</a>, <a href="#">OneDrive for Business sites</a> and <a href="#">SharePoint Online sites</a>.</li> </ul>

### Learn more

- [Guide to the General Data Protection Regulation \(GDPR\)](#) by the Information Commissioner's Office
- [General Data Protection Regulation \(GDPR\) FAQs for small organizations](#) by the Information Commissioner's

Office

- [Microsoft.com/GDPR](https://www.microsoft.com/GDPR)
- [Microsoft Trust Center](#)

# Information protection for GDPR with Microsoft 365 capabilities

2/5/2021 • 2 minutes to read • [Edit Online](#)

Microsoft 365 provides a rich set of capabilities to help you achieve compliance with the General Data Protection Regulation (GDPR). This article summarizes recommended capabilities with links to more information.

For more information about how Microsoft can help you with the GDPR, see [Get Started: Support for GDPR Accountability](#) in the Service Trust Portal.

## Information protection

Office 365 provides a rich set of data governance capabilities. For help with finding, classifying, protecting, and monitoring personal data, see [Office 365 Information Protection for GDPR](#).

For help with on-premises servers, including file shares, SharePoint Server, Exchange Server, Skype for Business Server, Project Server, and Office Online Server, see [GDPR for on-premises Office servers](#).

## Identity and access management

Azure Active Directory and other Microsoft 365 capabilities provide a rich set of capabilities to protect access to your data from identities and devices:

- Multi-factor authentication (MFA)
- Conditional access
- Privileged identity management
- Mobile device management
- Mobile application management
- Hardware protection for credentials

Microsoft provides a recommended configuration you can use as a starting point:

- [Identity and device access configurations](#): Recommended policy configurations to achieve three tiers of protection (baseline, sensitive, highly regulated). This guidance includes recommended policies for Exchange Online and SharePoint Online (including OneDrive for Business).
- [Security guidance for political campaigns, nonprofits, and other agile organizations](#): This includes the same set of policies but provides more guidance for BYOD environments and for B2B accounts.

## Threat Protection

Threat protection is built across Microsoft 365 services. Here are a few resources to get you started:

- [Office 365 security roadmap: Top priorities for the first 30 days, 90 days, and beyond](#). This roadmap includes recommendations for implementing capabilities.
- [Protect against threats in Office 365](#). Learn about protection actions you can take in the Microsoft 365 security center.
- [Windows Threat Protection](#). Learn more about Windows Defender Advanced Threat Protection and other capabilities in Windows 10.

Learn more

[Microsoft Trust Center](#)



# Microsoft's data protection officer

1/26/2021 • 2 minutes to read • [Edit Online](#)

Microsoft has designated a European Union Data Protection Officer (DPO) to be an independent advisor for Microsoft's engineering and business groups and to help ensure that all proposed processing of personal data meets EU legal requirements and Microsoft's corporate standards. The role was designed to meet the GDPR criteria set out in Articles 37-39.

## Qualifications

The DPO role requires successful candidates to have at least seven years of professional data protection experience, or a mix of 10 years of data protection, security, and enterprise risk management experience in order to be considered for the position. In addition, candidates must have demonstrated expertise in international data protection law and practices.

## Nature of the role

The DPO is involved, properly and in a timely manner, in all key issues, which relate to the protection of personal data. This action is effectuated, in part, by the DPO's role in reviewing and advising on all Data Protection Impact Assessments (DPIAs) generated by Microsoft. As the DPIA program is designed to capture all personal data processing at Microsoft, the DPO will have cross-company visibility into, and the opportunity to inform and advise Microsoft of its obligations pursuant to the GDPR regarding Microsoft's personal data processing. This same mechanism also allows the DPO to monitor Microsoft's compliance with applicable data protection regulations, including the GDPR, and Microsoft's internal policies and controls.

## Position of the Data Protection Officer

The European Union DPO reports directly to Microsoft's Chief Privacy Officer, a senior executive within Microsoft's Corporate and Legal Affairs division. The DPO role has autonomy to perform the functions in an independent, unbiased manner. Through the Chief Privacy Officer's organization, the DPO has access to training and customer response resources as necessary to perform the DPO functions. The DPO is bound by confidentiality concerning their tasks by using a non-disclosure agreement.

## Contact

Data subjects may contact the data protection officer by filling out the webform at <https://aka.ms/privacyresponse>. The DPO can also be reached by post at:

Microsoft EU Data Protection Officer  
One Microsoft Place  
South County Business Park  
Leopardstown  
Dublin 18  
D18 P521  
Ireland  
Telephone: +353 (1) 706-3117

The contact details for the Data Protection Officer have been communicated to Microsoft's Supervisory Authority.

## Learn more

- [Microsoft Trust Center](#)

# Support your GDPR program with Accountability Readiness Checklists

2/5/2021 • 5 minutes to read • [Edit Online](#)

The General Data Protection Regulation (GDPR) introduces new rules for organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents no matter where you or your enterprise are located. Additional details are in the [GDPR Summary](#) topic.

## Accountability Readiness Checklists

Accountability readiness checklists are provided to conveniently access information you may need to support the GDPR when using Microsoft products and services. The checklist lists potential obligations you may have under the GDPR, and points you to information that you can use to support your organizations' compliance.

There is a specific guide for four Microsoft product and services families:

- [Office 365](#)
- [Dynamics 365](#)
- [Azure](#)
- [Microsoft Support and Professional Services](#)

You can manage the items in this checklist with [Compliance Manager](#) by referencing the Control ID and Control Title under Customer Managed Controls in the GDPR tile.

The checklists include the four basic categories of considerations for a privacy program supporting GDPR listed below, along with example requirements.

1. Conditions for Data Collection and Processing:
  - When is consent obtained?
  - Identify and document purpose
  - Privacy impact assessment
2. Data Subject Rights
  - Determining information for PII principals (data subjects)
  - Providing mechanism to modify or withdraw consent
3. Privacy by Design and Default
  - Limit Collection
  - Comply with identification levels
  - Temporary files
4. Data Protection and Security
  - Understanding the organization and its context
  - Planning
  - Information Security Policies

## Customer agreements

- **Online service terms:** You can find Microsoft contractual commitments with regard to the GDPR in the

[Online Services Terms](#).

- **Microsoft product terms:** Microsoft extends the [GDPR Terms commitments](#) to all Volume Licensing customers.
- **Data protection addendum:** Microsoft services [extends the commitments](#) to Microsoft Consulting Services customers and others.

## GDPR compliance controls

- **Use Compliance Manager:** Review and incorporate controls Microsoft uses to support obligations in the GDPR with [Compliance Manager](#).
- **GDPR control mapping:** Access a [comprehensive mapping](#) of Microsoft controls to GDPR obligations.

## Records of Processing for Processors

Due to the scale and breadth of the online services we provide as processors to our controller customers, we expect customers to identify the services they seek the records of processing for and retrieve the relevant logs in the online tools we provide. One example is for the records of processing for Azure in which customers would be requested to identify which types of processing activity they seek the records of.

### Azure logs

Typically, customers would be interested in the Activity logs and potentially the Diagnostic logs:

- **Activity logs:** [Activity logs](#) provide insight into operations performed on resources in a subscription. Activity logs can help determine an operation's initiator, time of occurrence, and status.
- **Diagnostic logs:** [Diagnostic logs](#) are all logs emitted by every resource. These logs include Windows event system logs, Azure storage logs, Key Vault audit logs, and Application Gateway access and firewall logs.
- **Log archiving:** All diagnostic logs write to a centralized and encrypted Azure storage account for archival. The retention is user-configurable, up to 730 days, to meet organization-specific retention requirements. These logs connect to Azure Monitor logs for processing, storing, and dashboard reporting.

### Other logs

Additionally, the following monitoring solutions are installed as a part of this architecture. It is the customer's responsibility to configure these solutions to align with FedRAMP security controls:

- **AD Assessment:** The Active Directory Health Check solution assesses the risk and health of server environments on a regular interval and provides a prioritized list of recommendations specific to the deployed server infrastructure.
- **Anti-malware Assessment:** The Anti-malware solution reports on malware, threats, and protection status.
- **Azure Automation:** The Azure Automation solution stores, runs, and manages runbooks.
- **Security and Audit:** The Security and Audit dashboard provides a high-level insight into the security state of resources by providing metrics on security domains, notable issues, detections, threat intelligence, and common security queries.
- **SQL Assessment:** The SQL Health Check solution assesses the risk and health of server environments on a regular interval and provides customers with a prioritized list of recommendations specific to the deployed server infrastructure.
- **Update Management:** The Update Management solution allows customer management of operating system security updates, including a status of available updates and the process of installing required updates.
- **Agent Health:** The Agent Health solution reports how many agents are deployed and their geographic distribution, as well as how many agents that are unresponsive and the number of agents that are submitting operational data.
- **Azure Activity Logs:** The Activity Log Analytics solution assists with analysis of the Azure activity logs across all Azure subscriptions for a customer.

- [Change Tracking](#): The Change Tracking solution allows customers to easily identify changes in the environment.

For information on the technical and security measures for Azure, controller customers should visit the [Azure Security Documentation](#). As Microsoft doesn't know if Customer Data is Personal Data or not, Azure processes all Customer Data as if it were Personal Data so a customer would likely consider all of the material relevant.

### **Processor information**

Another product our customer might need records of processing information for processors is Office 365. To view information related to Office 365, see the [Search the audit log in the Security & Compliance Center](#) article.

You can also view the information for Dynamics 365 using the Security & Compliance center. In order to view the Security & Compliance center page, ensure that you have the correct license. Learn more about licensing with the [Security & Compliance Center service description](#) article. To search for Dynamics 365 events, visit the Unified Audit Log in the [Security & Compliance center](#).

### **Professional services information**

As for Professional Services, the Professional Services Support Data is provided by the customer to the support engineer by the customer's representative. This may take place when a customer submits a Service Request either through the online product portal, Services Hub or via phone.

The information is stored in our CRM systems and only used for the following purposes:

- Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.
- Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents); and
- Ongoing improvement (maintaining the Professional Services, including installing the latest updates, and making improvements to the reliability, efficacy, quality, and security).

Due to the scale of our support operations, Microsoft operates product group-based CRM system. Records of processing will be contained within those systems. A history of processing is reflected in the records maintained within our CRM systems. In most instances the Service Request History is available on the portals or Service Hub. For any specific details that are not available on the portals or any other inquiries about processing of your data, contact your Technical Account Manager or contact [Microsoft Technical Support](#).

## Learn more

- [Microsoft Trust Center](#)

# Azure and Dynamics 365 accountability readiness checklist for the GDPR

2/9/2021 • 2 minutes to read • [Edit Online](#)

To support the General Data Protection Regulation (GDPR) when using Microsoft Azure and Dynamics 365, use the set of privacy and security controls for personal data processors:

- [ISO/IEC 27701](#) for privacy management requirements
- [ISO/IEC 27001](#) for security techniques requirements

Microsoft Azure and Dynamics 365 services are [certified](#) to [ISO 27701 \(PIMS\)](#).

# Microsoft Support and Professional Services accountability readiness checklist for the GDPR

2/5/2021 • 27 minutes to read • [Edit Online](#)

## 1. Introduction

This accountability readiness checklist provides a convenient way to access information you may need to support GDPR when using Microsoft Professional Services and Support Services. The checklist is organized using the titles and reference number (in parentheses for each checklist topic) of a set of privacy and security controls for personal data processors drawn from:

- [ISO/IEC 27701](#) for privacy management requirements.
- [ISO/IEC 27001](#) for security techniques requirements.

This control structure is also used to organize the presentation of the internal controls that Microsoft Professional Services implements to support GDPR, which you can download from the [Service Trust Portal](#).

## 2. Conditions for collection and processing

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Identify and document purpose (7.2.1)</i>	The customer should document the purpose for which personal data is processed.	A description of the processing Microsoft performs for you, and the purposes of that processing, that can be included in your accountability documentation. - Microsoft Professional Services Data Protection Addendum [1]	(5)(1)(b), (32)(4)
<i>Identify lawful basis (7.2.2)</i>	The customer should understand any requirements related to the lawful basis of processing, such as whether consent must first be given.	A description of processing personal data by Microsoft services for inclusion in your accountability documentation. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]	(5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (10), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Determine when consent is to be obtained (7.2.3)</i>	The customer should understand legal or regulatory requirements for obtaining consent from individuals prior to processing personal data (when it is required, if the type of processing is excluded from the requirement, etc.), including how consent is collected.	Microsoft Professional Services does not provide direct support for gaining user consent.	(6)(1)(a), (8)(1), (8)(2)
<i>Obtain and record consent (7.2.4)</i>	When it is determined to be required, the customer should appropriately obtain consent. The customer should also be aware of any requirements for how a request for consent is presented and collected.	Microsoft Professional Services does not provide direct support for gaining user consent.	(7)(1), (7)(2), (9)(2)(a)
<i>Privacy impact assessment (7.2.5)</i>	The customer should be aware of requirements for completing privacy impact assessments (when they should be performed, categories of data that might necessitate one, timing of completing the assessment).	Microsoft Professional Services provides guidance as to when and how to determine when to perform a DPIA, and an overview of the DPIA program at Microsoft including the involvement of the DPO, which is provided in the Service Trust Portal <a href="#">Data Protection Impact Assessments (DPIAs) page</a> . For support for your DPIAs see: - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]	Article (35)
<i>Contracts with PII Processors (7.2.6)</i>	The customer should ensure that their contracts with processors include requirements for aiding with any relevant legal or regulatory obligations related to processing and protecting personal data.	The Microsoft contracts that require us to aid with your obligations under the GDPR, including support for the data subject's rights. - Microsoft Professional Services Data Protection Addendum [1]	(5)(2), (28)(3)(e), (28)(9)



CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Records related to processing PII (7.2.7)</i>	The customer should maintain all necessary and required records related to processing personal data (for example, purpose, security measures, etc.). Where some of these records must be provided by a sub-processor, the customer should ensure that they can obtain such records.	Microsoft Professional Services maintains records necessary to demonstrate compliance and support for accountability under the GDPR. See the Microsoft Professional Services Security Documentation [2]	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(g), (30)(1)(f), (30)(3), (30)(4), (30)(5)

### 3. Rights of data subjects

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Determining PII principals' rights and enabling exercise (7.3.1)</i>	The customer should understand requirements around the rights of individuals related to the processing of their personal data. These rights may include things such as access, correction, and erasure. Where the customer uses a third-party system, they should determine which (if any) parts of the system provide tools related to enabling individuals to exercise their rights (for example, to access their data). Where the system provides such capabilities, the customer should utilize them as necessary.	The capabilities Microsoft provides to help you support data subject rights. <ul style="list-style-type: none"> <li>- Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]</li> <li>- Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11]</li> </ul>	(12)(2)
<i>Determining information for PII principals (data subjects) (7.3.2)</i>	The customer should understand requirements for the types of information about processing of personal data that is to be available to be provided to the individual. This may include things such as: <ul style="list-style-type: none"> <li>• Contact details about the controller or its representative;</li> <li>• Information about the processing (purposes, international transfer, and related safeguards, retention period, etc.);</li> <li>• Information on how the principal may access and/or amend their personal data;</li> </ul>	Information about Microsoft services that you can include in the data you provide to data subjects. <ul style="list-style-type: none"> <li>- Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]</li> <li>- Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]</li> </ul>	(11)(2), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(3), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)

CATEGORY	requesting erasure or restriction of processing; CONSIDERATION receiving a copy of their	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
	<p>personal data, and portability of their personal data</p> <ul style="list-style-type: none"> <li>• How and from where the personal data was obtained (if not obtained from the principal directly)</li> <li>• Information about the right to lodge a complaint and to whom;</li> <li>• Information regarding corrections to personal data;</li> <li>• Notification that the organization is no longer in position to identify the data subject (PII principal), in cases where the processing no longer requires the identification of the data subject;</li> <li>• Transfers and/or disclosures of personal data;</li> <li>• Existence of automated decision making based solely on automated processing of personal data;</li> <li>• Information regarding the frequency with which information to the data subject is updated and provided (for example 'just in time' notification, organization defined frequency, etc.)</li> </ul> <p>Where the customer uses third-party systems or processors, they should determine which (if any) of this information may need to be provided by them and ensure that they can obtain the required information from the third party.</p>		
<p><i>Providing information to PII principals (7.3.3)</i></p>	<p>The customer should comply with any requirements around how/when/in what form the required information is to be given to an individual related to the processing of their personal data. In cases where a third party may provide required information, the customer should ensure that it is within the parameters required by the GDPR.</p>	<p>Templated information about Microsoft Professional Services that you can include in the data you provide to data subjects.</p> <ul style="list-style-type: none"> <li>- Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]</li> <li>- Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]</li> </ul>	<p>(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)</p>

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<p><i>Provide mechanism to modify or withdraw consent (7.3.4)</i></p>	<p>The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.</p>	<p>Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects when requesting consent. - Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]</p>	<p>(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)</p>
<p><i>Provide mechanism to object to processing (7.3.5)</i></p>	<p>The customer should understand requirements around rights of data subjects. Where an individual has a right to object to processing, the customer should inform them, and have a way for the individual to register their objection.</p>	<p>Information about Microsoft services relating to object to processing that you can include in the data you provide to data subjects. - Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]</p>	<p>(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)</p>
<p><i>Sharing the exercising of PII principals' rights (7.3.6)</i></p>	<p>The customer should understand requirements for notifying third-parties with whom personal data has been shared of instances of data modification based on the exercise of individual rights (for example, an individual requesting erasure or modification, etc.)</p>	<p>Information about capabilities in Microsoft services that allow you to discover personal data that you have shared with third parties. - Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]</p>	<p>(19)</p>
<p><i>Correction or erasure (7.3.7)</i></p>	<p>The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.</p>	<p>Information about Microsoft services relating to their ability to access, correct, or erase personal data that you can include in the data you provide to data subjects. - Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]</p>	

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Providing copy of PII processed (7.3.8)</i>	The customer should understand requirements around providing a copy of the personal data being processed to the individual. These may include requirements around the format of the copy (that is, that it is machine readable), transferring the copy, etc. Where the customer uses a third-party system that provides the functionality to provide copies, they should utilize this functionality as necessary.	Information about capabilities in Microsoft services to allow you to obtain a copy of their personal data that you can include in the data you provide to data subjects.- Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
<i>Request management (7.3.9)</i>	The customer should understand requirements for accepting and responding to legitimate requests from individuals related to the processing of their personal data. Where the customer uses a third-party system, they should understand whether that system provides the capabilities for such handling of requests. If so, the customer should utilize such mechanisms to handle requests, as necessary.	Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects as you manage data subject requests.- Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]	(12)(3), (12)(4), (12)(5), (12)(6), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h)
<i>Automated decision making (7.3.10)</i>	The customer should understand requirements around automated personal data processing and where decisions are made by such automation. These may include providing information about the processing to an individual, objecting to such processing, or to obtain human intervention. Where such features are provided by a third-party system, the customer should ensure that the third party provides any required information or support.	Information about any capabilities in Microsoft services for that might support automated decision making that you can use in your accountability documentation, and templated information for data subjects about those capabilities. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)

## 4. Privacy by design and default

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Limit collection (7.4.1)</i>	The customer should understand requirements around limits on collection of personal data (for example, that the collection should be limited to what is needed for the specified purpose).	A description of the data collected by Microsoft services. - Microsoft Professional Services Data Protection Addendum [1] - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]]	(5)(1)(b), (5)(1)(c)
<i>Limit processing (7.4.2)</i>	The customer is responsible for limiting the processing of personal data so that it is limited to what is adequate for the identified purpose.	A description of the data collected by Microsoft services. - Microsoft Professional Services Data Protection Addendum [1] - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]	(25)(2)
<i>Define and document PII minimization and de-identification objectives (7.4.3)</i>	The customer should understand requirements around de-identification of personal data, which may include, when it should be used, the extent to which it should de-identify, and instances when it cannot be used.	Customer is responsible for de-identification before transferring data to Microsoft. Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)
<i>Comply with identification levels (7.4.4)</i>	The customer should use and comply with de-identification objectives and methods set by their organization.	Customer is responsible for de-identification before transferring data to Microsoft. Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)
<i>PII de-identification and deletion (7.4.5)</i>	The customer should understand requirements around the retention of personal data past its use for the identified purposes. Where provided tooling by the system, the customer should utilize those tools to erase or delete as necessary.	Capabilities provided by Microsoft Services to support your data retention policies. - Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]	(5)(1)(c),(5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Temporary files (7.4.6)</i>	The customer should be aware of temporary files that may be sent to Microsoft that could lead to non-compliance with policies around processing of personal data (for example, personal data might be retained in a temporary file longer than required or allowed).	A description of capabilities provided by the service to identify personal data to support your temporary file policies. - Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]	(5)(1)(c)
<i>Retention (7.4.7)</i>	The customer should determine how long personal data should be retained, taking into consideration the identified purposes.	Information about the retention of personal data by Microsoft services that you can include in documentation provided to data subjects. - Microsoft Professional Services Data Protection Addendum [1]	(13)(2)(a), (14)(2)(a)
<i>Disposal (7.4.8)</i>	The customer should utilize any deletion or disposal mechanisms provided by the system to delete personal data.	Capabilities provided by Microsoft Services to support your data deletion policies. - Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]	(5)(1)(f)
<i>Collection procedures (7.4.9)</i>	The customer should be aware of requirements around the accuracy of personal data (for example, accuracy upon collection, keeping data up-to-date, etc.) and utilize any mechanisms provided by the system for such.	How Microsoft services support the accuracy of personal data, and any capabilities they provide to support your data accuracy policy. - Microsoft Professional Services Data Subject Requests for the GDPR and CCPA [7]	(5)(1)(d)
<i>Transmission controls (7.4.10)</i>	The customer should understand requirements around safeguarding the transmission of personal data, including who has access to transmission mechanisms, records of transmission, etc.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]	(15)(2), (30)(1)(e), (5)(1)(f)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Identify basis for PII transfer (7.5.1)</i>	The customer should be aware of requirements for transferring personal data (PII) to a different geographic location and document what measures are in place to meet such requirements.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]	Articles (44), (45), (46), (47), (48), and (49)
<i>Countries and organizations to which PII might be transferred (7.5.2)</i>	The customer should understand and be able to provide to the individual, the countries to which personal data is or may be transferred. Where a third-party/processor may perform this transfer, the customer should obtain this information from the processor.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]	(30)(1)(e)
<i>Records of transfers of PII (personal data) (7.5.3)</i>	The customer should maintain all necessary and required records related to transfers of personal data. Where a third-party/processor performs the transfer, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]	(30)(1)(e)
<i>Records of PII disclosure to third parties (7.5.4)</i>	The customer should understand requirements around recording to whom personal data has been disclosed. This may include disclosures to law enforcement, etc. Where a third-party/processor discloses the data, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	Documentation provided about the categories of recipients of disclosures of personal data including available records of disclosure. - Who can access your data and on what terms [6]	(30)(1)(d)
<i>Joint controller (7.5.5)</i>	The customer should determine whether they are a joint controller with any other organization, and appropriately document and allocate responsibilities.	Microsoft is not a joint controller of personal information provided as part of Support and Consulting Data.	(26)(1), (26)(2), (26)(3)

## 5. Data protection & security

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Understanding the organization and its context (5.2.1)</i>	Customers should determine their role in processing personal data (for example, controller, processor, co-controller) to identify the appropriate requirements (regulatory, etc.) for processing personal data.	How Microsoft considers each service as either a processor or controller when processing personal data. - Microsoft Professional Services Data Protection Addendum [1]	(24)(3), (28)(10), (28)(5), (28)(6), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
<i>Understanding the needs and expectations of interested parties (5.2.2)</i>	Customers should identify parties that may have a role or interest in their processing of personal data (for example, regulators, auditors, data subjects, contracted personal data processors), and be aware of requirements to engage such parties where required.	How Microsoft incorporates the views of all stakeholders in consideration of the risks involved in the processing of personal data. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]	(35)(9), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
<i>Determining the scope of the information security management system (5.2.3, 5.2.4)</i>	As part of any overall security or privacy program that a customer may have, they should include the processing of personal data and requirements relating to it.	How Microsoft services include the processing of personal data in information security management and privacy programs. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11] - ISO 27001 Audit Report [10]	(32)(2)
<i>Planning (5.3)</i>	Customers should consider the handling of personal data as part of any risk assessment they complete and apply controls as they deem necessary to mitigate risk related to personal data they control.	How Microsoft services consider the risks specific to the processing of personal data as part of their overall security and privacy program. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11]	(32)(1)(b), (32)(2)



CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Information Security Policies (6.2)</i>	The customer should augment any existing information security policies to include protection of personal data, including policies necessary for compliance with any applicable legislation.	Microsoft policies for information security and any specific measures for the protection of personal information. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11] - ISO 27001 Audit Report [10]	24(2)
<i>Organization of Information Security Customer consideration (6.3)</i>	The customer should, within their organization, define responsibilities for security and protection of personal data. This may include establishing specific roles to oversee privacy-related matters, including a DPO. Appropriate training and management support should be provided to support these roles.	Microsoft has published information on the Microsoft Data Protection Officer, the nature of their duties, reporting structure and contact information. - Microsoft DPO Information [13]	(37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
<i>Human Resource Security (6.4)</i>	The customer should determine and assign responsibility for providing relevant training related to protecting personal data.	An overview of the role of Microsoft's Data Protection Officer, the nature of his duties, reporting structure and contact information. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11] - Training and Awareness Program Description [3]	(39)(1)(b)
<i>Classification of Information (6.5.1)</i>	The customer should explicitly consider personal data as part of a data classification scheme.	How Microsoft considers personal data in data classification, tagging and tracking information. - Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments [9]	(39)(1)(b)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Management of removable media (6.5.2)</i>	The customer should determine internal policies for the use of removeable media as it relates to the protection of personal data (for example, encrypting devices).	How Microsoft services protect the security of personal information on any removeable media. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11] - Microsoft Professional Services Control Set [4]	(32)(1)(a), (5)(1)(f)
<i>Physical media transfer (6.5.3)</i>	The customer should determine internal policies for protecting personal data when transferring physical media (for example, encryption).	How Microsoft services protect personal data during any transfer of physical media. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11] - Microsoft Professional Services Control Set [4]	(32)(1)(a), (5)(1)(f)
<i>User access management (6.6.1)</i>	The customer should be aware of which responsibilities they have for access control within the service they are using, and manage those responsibilities appropriately, using the tools available.	The tools provided by Microsoft services to help you enforce access control. - Microsoft Professional Services Security Documentation [2]	(5)(1)(f)
<i>User registration and de-registration (6.6.2)</i>	The customer should manage user registration and de-registration within the service they utilize, using the tools available to them.	The tools provided by Microsoft services to help you enforce access control. - Microsoft Professional Services Security Documentation [2]	(5)(1)(f)
<i>User access provisioning (6.6.3)</i>	The customer should manage user profiles, especially for authorized access to personal data, within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, and the registration and de-registration of users. - Microsoft Professional Services Security Documentation [2]	(5)(1)(f)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Management of privileged access (6.6.4)</i>	The customer should manage user ID's to facilitate tracking of access (especially to personal data), within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, and the registration and de-registration of users. - Microsoft Professional Services Security Documentation [2]	(5)(1)(f)
<i>Secure log on procedures (6.6.5)</i>	The customer should utilize provided mechanisms in the service to ensure secure log on capabilities for their users where necessary.	How Microsoft services support internal access control policies related to personal data. - Who can access your data and on what terms [6]	(5)(1)(f)
<i>Cryptography (6.7)</i>	The customer should determine which data may need to be encrypted, and whether the service they are utilizing offers this capability. The customer should utilize encryption as needed, using the tools available to them.	How Microsoft services support encryption and pseudonymization to reduce the risk of processing personal data. - Microsoft Professional Services Security Documentation [2]	(32)(1)(a)
<i>Secure disposal or reuse of equipment (6.8.1)</i>	Where the customer uses cloud computing services (PaaS, SaaS, IaaS) they should understand how the cloud provider ensures that personal data is erased from storage space prior to that space being assigned to another customer.	How Microsoft Professional Services ensures that personal data is erased from storage equipment before that equipment is transferred or reused, when utilizing Microsoft Azure cloud computing services during professional services. - Microsoft Professional Services Security Documentation [2]	(5)(1)(f)
<i>Clear desk and clear screen policy (6.8.2)</i>	The customer should consider risks around hardcopy material that displays personal data, and potentially restrict the creation of such material. Where the system in use provides the capability to restrict this (for example, settings to prevent printing or copying/pasting of sensitive data), the customer should consider the need to utilize those capabilities.	What Microsoft implements to manage hardcopy. - Microsoft maintains these controls internally, see Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11] - Microsoft Professional Services GDPR Control Set [4]	(5)(1)(f)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Separation of development, testing, and operational environments (6.9.1)</i>	The customer should consider the implications of using personal data in development and testing environments within their organization.	How Microsoft ensures that personal data is protected in development and test environments. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11] - Microsoft Professional Services Control Set [4]	(5)(1)(f)
<i>Information backup (6.9.2)</i>	The customer should ensure that they use system provided capabilities to create redundancies in their data and test as necessary.	How Microsoft ensures the availability of data that may include personal data, how accuracy of restored data is ensured, and the tools and procedures Microsoft services provide to allow you to back up and restore data. - Microsoft Enterprise Business Continuity Management Documentation [5]	(32)(1)(c), (5)(1)(f)
<i>Event logging (6.9.3)</i>	The customer should understand the capabilities for logging provided by the system and utilize such capabilities to ensure that they can log actions related to personal data that they deem necessary.	The data Microsoft service records for you, including user activities, exceptions, faults and information security events, and how you can access those logs for use as part of your record keeping. - Microsoft Professional Services Security Documentation [2] - Microsoft Professional Services Control Set [4]	(5)(1)(f)
<i>Protection of log information (6.9.4)</i>	The customer should consider requirements for protecting log information that may contain personal data or that may contain records related to personal data processing. Where the system in use provides capabilities to protect logs, the customer should utilize these capabilities where necessary.	How Microsoft protects logs that may contain personal data. - Microsoft Professional Services Security Documentation [2] - Microsoft Professional Services Control Set [4]	(5)(1)(f)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<p><i>Information transfer policies and procedures (6.10.)</i></p>	<p>The customer should have procedures for cases where personal data may be transferred on physical media (such as a hard drive being moved between servers or facilities). These may include logs, authorizations, and tracking. Where a third-party or other processor may be transferring physical media, the customer should ensure that that organization has procedures in place to ensure security of the personal data.</p>	<p>How Microsoft services transfer physical media that may contain personal data, including the circumstances when transfer might occur, and the protective measures taken to protect the data.</p> <ul style="list-style-type: none"> <li>- Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11]</li> <li>- Microsoft Professional Services Control Set [4]</li> </ul>	<p>(5)(1)(f)</p>
<p><i>Confidentiality or non-disclosure agreements (6.10.2)</i></p>	<p>The customer should determine the need for confidentiality agreements or the equivalent for individuals with access to or responsibilities related to personal data.</p>	<p>How Microsoft services ensure that individuals with authorized access to personal data have committed themselves to confidentiality.</p> <ul style="list-style-type: none"> <li>- Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11]</li> <li>- Microsoft Professional Services Control Set [4]</li> </ul>	<p>(5)(1)(f), (28)(3)(b), (38)(5)</p>
<p><i>Securing application services on public networks (6.11.1)</i></p>	<p>The customer should understand requirements for encryption of personal data, especially when sent over public networks. Where the system provides mechanisms to encrypt data, the customer should utilize those mechanisms where necessary.</p>	<p>Descriptions of the measures Microsoft services take to protect data in transit, including encryption of the data, and how Microsoft services protect data that may contain personal data as it passes through public data networks, including any encryption measures.</p> <ul style="list-style-type: none"> <li>- Microsoft Professional Services Security Documentation [2]</li> </ul>	<p>(5)(1)(f), (32)(1)(a)</p>

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Secure system engineering principles (6.11.2)</i>	The customer should understand how systems are designed and engineered to consider protection of personal data. Where a customer uses a system engineered by a third party, it is their responsibility to ensure that such protections have been considered.	How Microsoft services include personal data protection principles as a mandatory part of our secure design/engineering principles. - Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability [11] - <a href="#">What is the Security Development Lifecycle?</a>	(25)(1)
<i>Supplier Relationships (6.12)</i>	The customer should ensure that any information security and personal data protection requirements and that are the responsibility of a third party are addressed in contractual information or other agreements. The agreements should also address the instructions for processing.	How Microsoft services address security and data protection in our agreements with our suppliers and how we ensure that those agreements are effectively implemented. - Who can access your data and on what terms [6]	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
<i>Management of information security incidents and improvements (6.13.1)</i>	The customer should have processes for determining when a personal data breach has occurred.	How Microsoft services determine if a security incident is a breach of personal data, and how we communicate the breach to you. - Microsoft Professional Services and Breach Notification Under the GDPR [8]	(33)(2)
<i>Responsibilities and procedures (during information security incidents) (6.13.2)</i>	The customer should understand and document their responsibilities during a data breach or security incident involving personal data. Responsibilities may include notifying required parties, communications with processors or other third-parties, and responsibilities within the customer's organization.	How to notify Microsoft services if you detect a security incident or breach of personal data. - Microsoft Professional Services and Breach Notification Under the GDPR [8]	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<p><i>Response to information security incidents (6.13.3)</i></p>	<p>The customer should have processes for determining when a personal data breach has occurred.</p>	<p>Description of the information Microsoft services provides to help you decide if a breach of personal data has occurred. - Microsoft Professional Services and Breach Notification Under the GDPR [8]</p>	<p>(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)</p>
<p><i>Protection of records (6.15.1)</i></p>	<p>The customer should understand the requirements for records related to personal data processing that need to be maintained.</p>	<p>How Microsoft services store records relating to the processing of personal data. - Microsoft Professional Services Security Documentation [2]</p>	<p>(5)(2), (24)(2)</p>
<p><i>Independent review of information security (6.15.2)</i></p>	<p>The customer should be aware of requirements for assessments of the security of personal data processing. This may include internal or external audits, or other measures for assessing the security of processing. Where the customer is dependent on another organization or third party for all or part of the processing, they should collect information about such assessments performed by them.</p>	<p>How Microsoft services test and assesses the effectiveness of technical and organizational measures to ensure the security of processing, including any audits by third parties. - Microsoft Professional Services Data Protection Addendum [1]</p>	<p>(32)(1)(d), (32)(2)</p>

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Technical compliance review (6.15.3)</i>	The customer should understand requirements for testing and evaluating the security of processing personal data. This may include technical tests such as penetration testing. Where the customer uses a third-party system or processor, they should understand what responsibilities they have for securing and testing the security (for example, managing configurations to secure data and then testing those configuration settings). Where the third party is responsible for all or part of the security of processing, the customer should understand what testing or evaluation the third party performs to ensure the security of the processing.	How Microsoft services are tested security based on identified risks, including tests by third parties, and the types of technical tests. - For a listing of external certifications, see Microsoft Trust Center Compliance offerings [12] - For more information about vulnerability testing your applications, see Microsoft Professional Services Security Documentation [2]	(32)(1)(d), (32)(2)

## 6. Bibliography of Resources and Links

ID	DESCRIPTION/LINKS	NOTES	
1	<a href="#">Microsoft Professional Services Data Protection Addendum</a>		
2	<a href="#">Microsoft Professional Services Security Documentation</a>		
3	Training and Awareness Program Description	Available on request through customer's account management team.	
4	<a href="#">Microsoft Professional Services GDPR Control Set</a>		
5	Microsoft Enterprise Business Continuity Management Documentation	Available on request through customer's account management team.	
6	<a href="#">Who can access your data and on what terms</a>		



ID	DESCRIPTION/LINKS	NOTES	
7	<a href="#">Microsoft Professional Services Data Subject Requests for the GDPR and CCPA</a>		
8	<a href="#">Microsoft Professional Services and Breach Notification Under the GDPR</a>		
9	<a href="#">Key Information from Microsoft Professional Services for Customer Data Protection Impact Assessments</a>		
10	<a href="#">ISO 27001 Audit Report</a>		
11	<a href="#">Microsoft Professional Services ISO/IEC 27001:2013 ISMS Statement of Applicability</a>	SOA on request through customer's account management team.	
12	<a href="#">Microsoft Trust Center Compliance offerings</a>		
13	<a href="#">Microsoft DPO Information</a>		

## Learn more

- [Microsoft Trust Center](#)

# Accountability Readiness Checklist for Microsoft 365

2/5/2021 • 30 minutes to read • [Edit Online](#)

## 1. Introduction

This accountability readiness checklist provides a convenient way to access information you may need to support the GDPR when using Microsoft Office 365.

You can manage the items in this checklist with [Compliance Manager](#) by referencing the Control ID and Control Title under *Customer Managed Controls* in the GDPR tile.

In addition, items in this checklist under *5. Data Protection & Security* provide references to controls listed under Microsoft Managed Controls in the GDPR tile in [Compliance Manager](#). Reviewing the Microsoft Implementation Details for these controls provide additional explanation of Microsoft's approach to fulfilling the customer considerations in the checklist item.

The checklist and Compliance Manager are organized using the titles and reference number (in parentheses for each checklist topic) of a set of privacy and security controls for personal data processors drawn from:

- [ISO/IEC 27701](#) for privacy management requirements.
- [ISO/IEC 27001](#) for security techniques requirements.

This control structure is also used to organize the presentation of the internal controls that Microsoft Office 365 implements to support GDPR, which you can download from the [Service Trust Center](#).

## 2. Conditions for collection and processing

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Determine when consent is to be obtained (7.2.3)</i>	The customer should understand legal or regulatory requirements for obtaining consent from individuals prior to processing personal data (when it is required, if the type of processing is excluded from the requirement, etc.), including how consent is collected.	Office 365 does not provide direct support for gaining user consent.	(6)(1)(a), (8)(1), (8)(2)
<i>Identify and document purpose (7.2.1)</i>	The customer should document the purpose for which personal data is processed.	A description of the processing Microsoft performs for you, and the purposes of that processing, that can be included in your accountability documentation. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR [1]</i>	(5)(1)(b), (32)(4)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<p><b><i>Identify lawful basis (7.2.2)</i></b></p>	<p>The customer should understand any requirements related to the lawful basis of processing, such as whether consent must first be given.</p>	<p>A description of processing personal data by Microsoft services for inclusion in your accountability documentation.</p> <p>- <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i>[10]</p>	<p>(5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (10), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)</p>
<p><b><i>Determine when consent is to be obtained (7.2.3)</i></b></p>	<p>The customer should understand legal or regulatory requirements for obtaining consent from individuals prior to processing personal data (when it is required, if the type of processing is excluded from the requirement, etc.), including how consent is collected.</p>	<p>Office 365 does not provide direct support for gaining user consent.</p>	<p>(6)(1)(a), (8)(1), (8)(2)</p>
<p><b><i>Obtain and record consent (7.2.4)</i></b></p>	<p>When it is determined to be required, the customer should appropriately obtain consent. The customer should also be aware of any requirements for how a request for consent is presented and collected.</p>	<p>Office 365 does not provide direct support for gaining user consent.</p>	<p>(7)(1), (7)(2), (9)(2)(a)</p>
<p><b><i>Privacy impact assessment (7.2.5)</i></b></p>	<p>The customer should be aware of requirements for completing privacy impact assessments (when they should be performed, categories of data that might necessitate one, timing of completing the assessment).</p>	<p>How Microsoft services determine when to perform a DPIA, and an overview of the DPIA program at Microsoft including the involvement of the DPO, is provided on the Service Trust Portal <a href="#">Data Protection Impact Assessments (DPIAs) page</a>. For support for your DPIAs see:</p> <p>- <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]</p>	<p>(35)</p>
<p><b><i>Contracts with PII Processors (7.2.6)</i></b></p>	<p>The customer should ensure that their contracts with processors include requirements for aiding with any relevant legal or regulatory obligations related to processing and protecting personal data.</p>	<p>The Microsoft contracts that require us to aid with your obligations under the GDPR, including support for the data subject's rights.</p> <p>- <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR</i> [1]</p>	<p>(5)(2), (28)(3)(e), (28)(9)</p>

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Records related to processing PII (7.2.7)</i>	The customer should maintain all necessary and required records related to processing personal data (that is, purpose, security measures, etc.). Where some of these records must be provided by a sub-processor, the customer should ensure that they can obtain such records.	The tools provided by Microsoft services to help you maintain the records necessary demonstrate compliance and support for accountability under the GDPR. - <i>Search the audit log in Office 365 Security and Compliance Center</i> [16]	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(g), (30)(1)(f), (30)(3), (30)(4), (30)(5)

### 3. Rights of data subjects

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Determining PII principals' rights and enabling exercise (7.3.1)</i>	The customer should understand requirements around the rights of individuals related to the processing of their personal data. These rights may include things such as access, correction, and erasure. Where the customer uses a third-party system, they should determine which (if any) parts of the system provide tools related to enabling individuals to exercise their rights (for example, to access their data). Where the system provides such capabilities, the customer should utilize them as necessary.	The capabilities Microsoft provides to help you support data subject rights. - <i>Office 365 Data Subject Requests for the GDPR</i> [8] - <i>Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability</i> [12] see ISO, IEC 27018, 2014 control A.1.1	(12)(2)
<i>Determining information for PII principals (data subjects) (7.3.2)</i>	The customer should understand requirements for the types of information about processing of personal data that is to be available to be provided to the individual. This may include things such as: - Contact details about the controller or its representative; - information about the processing (purposes, international transfer, and related safeguards, retention period, etc.); - information on how the principal may access and/or amend their personal data; requesting erasure or	Information about Microsoft services that you can include in the data you provide to data subjects. - <i>Office 365 Data Subject Requests for the GDPR</i> [8] - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	(11)(2), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(3), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)

CATEGORY	restriction of processing; CUSTOMER receiving a copy of their personal data, and CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
	<p>portability of their personal data</p> <ul style="list-style-type: none"> <li>- How and from where the personal data were obtained (if not obtained from the principal directly)</li> <li>- information about the right to lodge a complaint and to whom;</li> <li>- information regarding corrections to personal data;</li> <li>- Notification that the organization is no longer in position to identify the data subject (PII principal), in cases where the processing no longer requires the identification of the data subject;</li> <li>- Transfers and/or disclosures of personal data;</li> <li>- existence of automated decision making based solely on automated processing of personal data;</li> <li>- information regarding the frequency with which information to the data subject is updated and provided (that is, "just in time" notification, organization defined frequency, etc.)</li> </ul> <p>Where the customer uses third-party systems or processors, they should determine which (if any) of this information may need to be provided by them and ensure that they can obtain the required information from the third party.</p>		
<p><b><i>Providing information to PII principals (7.3.3)</i></b></p>	<p>The customer should comply with any requirements around how/when/in what form the required information is to be given to an individual related to the processing of their personal data. In cases where a third party may provide required information, the customer should ensure that it is within the parameters required by the GDPR.</p>	<p>Templated information about Microsoft services that you can include in the data you provide to data subjects.</p> <ul style="list-style-type: none"> <li>- <i>Office 365 Data Subject Requests for the GDPR</i> [8]</li> <li>- <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]</li> </ul>	<p>(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)</p>

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<p><i>Provide mechanism to modify or withdraw consent (7.3.4)</i></p>	<p>The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.</p>	<p>Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects when requesting consent. - <i>Office 365 Data Subject Requests for the GDPR</i> [8]</p>	<p>(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)</p>
<p><i>Provide mechanism to object to processing (7.3.5)</i></p>	<p>The customer should understand requirements around rights of data subjects. Where an individual has a right to object to processing, the customer should inform them, and have a way for the individual to register their objection.</p>	<p>Information about Microsoft services relating to object to processing that you can include in the data you provide to data subjects. - <i>Office 365 Data Subject Requests for the GDPR</i> [8] see <i>Step 4: Restrict</i></p>	<p>(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)</p>
<p><i>Sharing the exercising of PII principals' rights (7.3.6)</i></p>	<p>The customer should understand requirements for notifying third-parties with whom personal data has been shared of instances of data modification based on the exercise of individual rights (for example, an individual requesting erasure or modification, etc.)</p>	<p>Information about capabilities in Microsoft services that allow you to discover personal data that you have shared with third parties. - <i>Office 365 Data Subject Requests for the GDPR</i> [8]</p>	<p>(19)</p>
<p><i>Correction or erasure (7.3.7)</i></p>	<p>The customer should understand requirements for informing users about their right to access, correct, and/or erase their personal data and for providing a mechanism for which them to do so. If a third-party system is used and provides this mechanism as part of its functionality, the customer should utilize that functionality as necessary.</p>	<p>Templated information about Microsoft services relating to their ability to access, correct, or erase personal data that you can include in the data you provide to data subjects. - <i>Office 365 Data Subject Requests for the GDPR</i> [8] see <i>Step 5: Delete</i></p>	<p>(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)</p>

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<p><i>Providing copy of PII processed (7.3.8)</i></p>	<p>The customer should understand requirements around providing a copy of the personal data being processed to the individual. These may include requirements around the format of the copy (that is, that it is machine readable), transferring the copy, etc. Where the customer uses a third-party system that provides the functionality to provide copies, they should utilize this functionality as necessary.</p>	<p>Information about capabilities in Microsoft services to allow you to obtain a copy of their personal data that you can include in the data you provide to data subjects.</p> <p>- <i>Office 365 Data Subject Requests for the GDPR</i> [8] see <i>Step 6: Export</i></p>	<p>(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)</p>

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Request management (7.3.9)</i>	The customer should understand requirements for accepting and responding to legitimate requests from individuals related to the processing of their personal data. Where the customer uses a third-party system, they should understand whether that system provides the capabilities for such handling of requests. If so, the customer should utilize such mechanisms to handle requests as necessary.	<p>Information about capabilities in Microsoft services that you can use when defining the information you provide to data subjects as you manage data subject requests.</p> <p>- <i>Office 365 Data Subject Requests for the GDPR</i> [8]</p> <p>customer should understand requirements around automated personal data processing and where decisions are made by such automation. These may include providing information about the processing to an individual, objecting to such processing, or to obtain human intervention. Where such features are provided by a third-party system, the customer should ensure that the third party provides any required information or support.</p> <p>Information about any capabilities in Microsoft services that might support automated decision making that you can use in your accountability documentation, and templated information for data subjects about those capabilities.</p> <p>- <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]</p>	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)

## 4. Privacy by design and default

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
----------	------------------------	------------------------------------	---------------------------



CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Limit collection (7.4.1)</i>	The customer should understand requirements around limits on collection of personal data (for example, that the collection should be limited to what is needed for the specified purpose).	A description of the data collected by Microsoft services. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR [1]</i> - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments [10]</i>	(5)(1)(b), (5)(1)(c)
<i>Limit processing (7.4.2)</i>	The customer is responsible for limiting the processing of personal data so that it is limited to what is adequate for the identified purpose.	A description of the data collected by Microsoft services. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR [1]</i> - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments [10]</i>	(25)(2)
<i>Define and document PII minimization and de-identification objectives (7.4.3)</i>	The customer should understand requirements around de-identification of personal data that may include, when it should be used, the extent to which it should de-identify, and instances when it cannot be used.	Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)
<i>Comply with identification levels (7.4.4)</i>	The customer should use and comply with de-identification objectives and methods set by their organization.	Microsoft applies de-identification and pseudonymization internally, where appropriate, to provide additional privacy safeguards for personal data.	(5)(1)(c)
<i>PII de-identification and deletion (7.4.5)</i>	The customer should understand requirements around the retention of personal data past its use for the identified purposes. Where provided tooling by the system, the customer should utilize those tools to erase or delete as necessary.	Capabilities provided by Microsoft cloud services to support your data retention policies. - <i>Office 365 Data Subject Requests for the GDPR [8]</i> see <i>Step 5: Delete</i>	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Temporary files (7.4.6)</i>	The customer should be aware of temporary files that may be created by the system that could lead to non-compliance with policies around processing of personal data (for example, personal data might be retained in a temporary file longer than required or allowed). Where the system provides such tools for temporary file deletion or checking, the customer should utilize such tools to comply with requirements.	A description of capabilities provided by the service to identify personal data to support your temporary file policies. - Office 365 Data Subject Requests for the GDPR [8] see Step1: Discover	(5)(1)(c)
<i>Retention (7.4.7)</i>	The customer should determine how long personal data should be retained, taking into consideration the identified purposes.	Information about the retention of personal data by Microsoft services that you can include in documentation provided to data subjects. - <i>Microsoft Online Services Terms, Data Protection Terms, see Data Security, Retention</i> [1]	(13)(2)(a), (14)(2)(a)
<i>Disposal (7.4.8)</i>	The customer should utilize any deletion or disposal mechanisms provided by the system to delete personal data.	Capabilities provided by Microsoft cloud services to support your data deletion policies. -* Office 365 Data Subject Requests for the GDPR* [8] see <i>Step 5: Delete</i>	(5)(1)(f)
<i>Collection procedures (7.4.9)</i>	The customer should be aware of requirements around the accuracy of personal data (for example, accuracy upon collection, keeping data up-to-date, etc.) and utilize any mechanisms provided by the system for such.	How Microsoft services support the accuracy of personal data, and any capabilities they provide to support your data accuracy policy. - <i>Office 365 Data Subject Requests for the GDPR</i> [8] see <i>Step 3: Rectify</i>	(5)(1)(d)
<i>Transmission controls (7.4.10)</i>	The customer should understand requirements around safeguarding the transmission of personal data, including who has access to transmission mechanisms, records of transmission, etc.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	(15)(2), (30)(1)(e), (5)(1)(f)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<b><i>Identify basis for PII transfer (7.5.1)</i></b>	The customer should be aware of requirements for transferring personal data (PII) to a different geographic location and document what measures are in place to meet such requirements.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	Articles (44), (45), (46), (47), (48), and (49)
<b><i>Countries and organizations to which PII might be transferred (7.5.2)</i></b>	The customer should understand, and be able to provide to the individual, the countries to which personal data is or may be transferred. Where a third-party/processor may perform this transfer, the customer should obtain this information from the processor.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	(30)(1)(e)
<b><i>Records of transfers of PII (personal data) (7.5.3)</i></b>	The customer should maintain all necessary and required records related to transfers of personal data. Where a third-party/processor performs the transfer, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	A description of the types of personal data that are transferred by Microsoft services and the locations they are transferred between, and the legal safeguards for the transfer. - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments</i> [10]	(30)(1)(e)
<b><i>Records of PII disclosure to third parties (7.5.4)</i></b>	The customer should understand requirements around recording to whom personal data has been disclosed. This may include disclosures to law enforcement, etc. Where a third-party/processor discloses the data, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	Documentation provided about the categories of recipients of disclosures of personal data including available records of disclosure. - <i>Who can access your data and on what terms</i> [6]	(30)(1)(d)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Joint controller (7.5.5)</i>	The customer should determine whether they are a joint controller with any other organization, and appropriately document and allocate responsibilities.	Documentation of Microsoft services that are a controller of personal information, including templated information that can be included in documentation to data subjects. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR [1]</i>	

## 5. Data protection & security

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Understanding the organization and its context (5.2.1)</i>	Customers should determine their role in processing personal data (for example, controller, processor, co-controller) to identify the appropriate requirements (regulatory, etc.) for processing personal data.	How Microsoft considers each service as either a processor or controller when processing personal data. - <i>Microsoft Online Services Terms, Data Protection Terms, see Processing of Personal Data; GDPR, Processor, and Controller Roles and Responsibilities [1]</i>	(24)(3), (28)(10), (28)(5), (28)(6), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
<i>Understanding the needs and expectations of interested parties (5.2.2)</i>	Customers should identify parties that may have a role or interest in their processing of personal data (for example, regulators, auditors, data subjects, contracted personal data processors), and be aware of requirements to engage such parties where required.	How Microsoft incorporates the views of all stakeholders in consideration of the risks involved in the processing of personal data. - <i>Key Information from Office 365 for Customer Data Protection Impact Assessments [10]</i> - <i>Office 365 ISMS Manual [14]</i> see 4.2 UNDERSTANDING THE NEEDS AND EXPECTATIONS OF INTERESTED PARTIES - Understanding the needs and expectations of interested parties 5.2.2 in <a href="#">Compliance Manager</a>	(35)(9), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<p><i>Determining the scope of the information security management system (5.2.3, 5.2.4)</i></p>	<p>As part of any overall security or privacy program that a customer may have, they should include the processing of personal data and requirements relating to it.</p>	<p>How Microsoft services include the processing of personal data in information security management and privacy programs.</p> <ul style="list-style-type: none"> <li>- <i>Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability [12]</i> see A.19</li> <li>- <i>SOC 2 Type 2 Audit Report [11]</i></li> <li>- Office 365 ISMS Manual [14] see 4. <i>Context of the Organization</i></li> <li>- 5.2.3 Determining the scope of the information security management system in Compliance Manager</li> <li>- 5.2.4 Information security management system in <a href="#">Compliance Manager</a></li> </ul>	<p>(32)(2)</p>
<p><i>Planning (5.3)</i></p>	<p>Customers should consider the handling of personal data as part of any risk assessment they complete and apply controls as they deem necessary to mitigate risk related to personal data they control.</p>	<p>How Microsoft services consider the risks specific to the processing of personal data as part of their overall security and privacy program.</p> <ul style="list-style-type: none"> <li>- <i>Office 365 ISMS Manual [14]</i> see 5.2 <i>Policy</i></li> <li>- 5.3 Planning in <a href="#">Compliance Manager</a></li> </ul>	<p>(32)(1)(b), (32)(2)</p>
<p><i>Information Security Policies (6.2)</i></p>	<p>The customer should augment any existing information security policies to include protection of personal data, including policies necessary for compliance with any applicable legislation.</p>	<p>Microsoft policies for information security and any specific measures for the protection of personal information.</p> <ul style="list-style-type: none"> <li>- <i>Microsoft Office 365 (All-Up) ISO/IEC 27001:2013 ISMS Statement of Applicability [12]</i> see A.19</li> <li>- <i>SOC 2 Type 2 Audit Report [11]</i></li> <li>- 6.2 Information security policies in <a href="#">Compliance Manager</a></li> </ul>	<p>24(2)</p>

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Organization of Information Security Customer consideration (6.3)</i>	The customer should, within their organization, define responsibilities for security and protection of personal data. This may include establishing specific roles to oversee privacy-related matters, including a DPO. Appropriate training and management support should be provided to support these roles.	An overview of the role of Microsoft's Data Protection Officer, the nature of his duties, reporting structure and contact information. - <i>Microsoft's Data Protection Officer</i> [18] - <i>Office 365 ISMS Manual</i> [14] see 5.3 <i>ORGANIZATIONAL ROLES, RESPONSIBILITIES, AND AUTHORITIES</i> - 6.3 Organization of information security in <a href="#">Compliance Manager</a>	(37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
<i>Human Resource Security (6.4)</i>	The customer should determine and assign responsibility for providing relevant training related to protecting personal data.	An overview of the role of Microsoft's Data Protection Officer, the nature of his duties, reporting structure and contact information. - <i>Microsoft's Data Protection Officer</i> [18] - <i>Office 365 ISMS Manual</i> [14] see 5.3 <i>ORGANIZATIONAL ROLES, RESPONSIBILITIES, AND AUTHORITIES</i> - 6.4 Human resources security in <a href="#">Compliance Manager</a>	(39)(1)(b)
<i>Classification of Information (6.5.1)</i>	The customer should explicitly consider personal data as part of a data classification scheme.	Capabilities in Office 365 to support personal data classification. - <i>Office 365 Information Protection for GDPR</i> [5] see Architect a classification schema for personal data - 6.5.1 Classification of Information in <a href="#">Compliance Manager</a>	(39)(1)(b)
<i>Management of removable media (6.5.2)</i>	The customer should determine internal policies for the use of removable media as it relates to the protection of personal data (for example, encrypting devices).	How Microsoft services protect the security of personal information on any removable media. - <i>FedRAMP Moderate FedRAMP System Security Plan</i> [3] see 13.10 Media Protection (MP) - Management of removable media in <a href="#">Compliance Manager</a>	(32)(1)(a), (5)(1)(f)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Physical media transfer (6.5.3)</i>	The customer should determine internal policies for protecting personal data when transferring physical media (for example, encryption).	How Microsoft services protect personal data during any transfer of physical media. - FedRAMP Moderate FedRAMP System Security Plan [3] see 13.10 Media Protection (MP) - 6.5.3 Physical media transfer in <a href="#">Compliance Manager</a>	(32)(1)(a), (5)(1)(f)
<i>User access management (6.6.1)</i>	The customer should be aware of which responsibilities they have for access control within the service they are using, and manage those responsibilities appropriately, using the tools available.	The tools provided by Microsoft services to help you enforce access control. - Office 365 Security Documentation [2] see <a href="#">Protect access to data and services in Office 365</a> - 6.6.1 in <a href="#">Compliance Manager</a>	(5)(1)(f)
<i>User registration and de-registration (6.6.2)</i>	The customer should manage user registration and de-registration within the service they utilize, using the tools available to them.	The tools provided by Microsoft services to help you enforce access control. - Office 365 Security Documentation [2] see <a href="#">Protect access to data and services in Office 365</a> - 6.6.2 User registration and de-registration in <a href="#">Compliance Manager</a>	(5)(1)(f)
<i>User access provisioning (6.6.3)</i>	The customer should manage user profiles, especially for authorized access to personal data, within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, access to applications and the registration and de-registration of users. - Office 365 Security Documentation [2] see <a href="#">Protect access to data and services in Office 365</a> - Use Tenant Restrictions to manage access to SaaS cloud applications [15] - User access provisioning in <a href="#">Compliance Manager</a>	(5)(1)(f)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Management of privileged access (6.6.4)</i>	The customer should manage user IDs to facilitate tracking of access (especially to personal data), within the service they utilize, using the tools available to them.	How Microsoft services support formal access control to personal data, including user IDs, roles, and the registration and de-registration of users. - Office 365 Security Documentations 2 see <a href="#">Protect access to data and services in Office 365</a> - Use Tenant Restrictions to manage access to SaaS cloud applications [15] - 6.6.4 Management of privileged access in <a href="#">Compliance Manager</a>	(5)(1)(f)
<i>Secure log on procedures (6.6.5)</i>	The customer should utilize provided mechanisms in the service to ensure secure log on capabilities for their users where necessary.	How Microsoft services support internal access control policies related to personal data. - Who can access your data and on what terms [6] - 6.6.5 Secure log-on procedures in <a href="#">Compliance Manager</a>	(5)(1)(f)
<i>Cryptography (6.7)</i>	The customer should determine which data may need to be encrypted, and whether the service they are utilizing offers this capability. The customer should utilize encryption as needed, using the tools available to them.	How Microsoft services support encryption and pseudonymization to reduce the risk of processing personal data. - FedRAMP Moderate FedRAMP System Security Plans (SSP) see <i>Cosmos</i> pp29 - 6.7 Cryptography in <a href="#">Compliance Manager</a>	(32)(1)(a)
<i>Secure disposal or reuse of equipment (6.8.1)</i>	Where the customer uses cloud computing services (PaaS, SaaS, IaaS) they should understand how the cloud provider ensures that personal data is erased from storage space prior to that space being assigned to another customer.	How Microsoft services ensure that personal data is erased from storage equipment before that equipment is transferred or reused. - FedRAMP Moderate FedRAMP System Security Plan [3] see 13.10 Media Protection (MP) - 6.8.1 Secure disposal or reuse of equipment in <a href="#">Compliance Manager</a>	(5)(1)(f)



CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Clear desk and clear screen policy (6.8.2)</i>	The customer should consider risks around hardcopy material that displays personal data, and potentially restrict the creation of such material. Where the system in use provides the capability to restrict this (for example, settings to prevent printing or copying/pasting of sensitive data), the customer should consider the need to utilize those capabilities.	What Microsoft implements to manage hardcopy. - Microsoft maintains these controls internally, see Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability [12] A.10.2, A.10.7, and A.4.1 - 6.8.2 Clear desk and clear screen policy in <a href="#">Compliance Manager</a>	(5)(1)(f)
<i>Separation of development, testing, and operational environments (6.9.1)</i>	The customer should consider the implications of using personal data in development and testing environments within their organization.	How Microsoft ensures that personal data is protected in development and test environments. - Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability [12] see A.12.1.4 - 6.9.1 Separation of development, testing, and operational environments in <a href="#">Compliance Manager</a>	5(1)(f)
<i>Information backup (6.9.2)</i>	The customer should ensure that they use system provided capabilities to create redundancies in their data and test as necessary.	How Microsoft ensures the availability of data that may include personal data, how accuracy of restored data is ensured, and the tools and procedures Microsoft services provide to allow you to back up and restore data. - FedRAMP Moderate FedRAMP System Security Plan [3] see 10.9 Availability - 6.9.2 Information Backup in <a href="#">Compliance Manager</a>	(32)(1)(c), (5)(1)(f)
<i>Event logging (6.9.3)</i>	The customer should understand the capabilities for logging provided by the system and utilize such capabilities to ensure that they can log actions related to personal data that they deem necessary.	The data Microsoft service records for you, including user activities, exceptions, faults and information security events, and how you can access those logs for use as part of your record keeping. - Search the audit log in Office 365 Security and Compliance Center [16] - 6.9.3 Event logging in <a href="#">Compliance Manager</a>	(5)(1)(f)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Protection of log information (6.9.4)</i>	The customer should consider requirements for protecting log information that may contain personal data or that may contain records related to personal data processing. Where the system in use provides capabilities to protect logs, the customer should utilize these capabilities where necessary.	How Microsoft protects logs that may contain personal data. - Search the audit log in Office 365 Security and Compliance Center [16] - 6.9.4 Protection of log information in <a href="#">Compliance Manager</a>	(5)(1)(f)
<i>Information transfer policies and procedures (6.10.1)</i>	The customer should have procedures for cases where personal data may be transferred on physical media (such as a hard drive being moved between servers or facilities). These may include logs, authorizations, and tracking. Where a third-party or other processor may be transferring physical media, the customer should ensure that that organization has procedures in place to ensure security of the personal data.	How Microsoft services transfer physical media that may contain personal data, including the circumstances when transfer might occur, and the protective measures taken to protect the data. - FedRAMP Moderate FedRAMP System Security Plan [3] see 13.10 Media Protection (MP) - 6.10.1 Information transfer policies and procedures in <a href="#">Compliance Manager</a>	(5)(1)(f)
<i>Confidentiality or non-disclosure agreements (6.10.2)</i>	The customer should determine the need for confidentiality agreements or the equivalent for individuals with access to or responsibilities related to personal data.	How Microsoft services ensure that individuals with authorized access to personal data have committed themselves to confidentiality. - SOC 2 Type 2 Audit Report [11] see CC1.4 pp33 - Confidentiality or non-disclosure agreements 6.10.2 in <a href="#">Compliance Manager</a>	(5)(1)(f), (28)(3)(b), (38)(5)

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<p><i>Securing application services on public networks (6.11.1)</i></p>	<p>The customer should understand requirements for encryption of personal data, especially when sent over public networks. Where the system provides mechanisms to encrypt data, the customer should utilize those mechanisms where necessary.</p>	<p>Descriptions of the measures Microsoft services take to protect data in transit, including encryption of the data, and how Microsoft services protect data that may contain personal data as it passes through public data networks, including any encryption measures.</p> <ul style="list-style-type: none"> <li>- Encryption in the Microsoft Cloud [17] see <i>Encryption of customer data in transit</i></li> <li>- 6.11.1 Securing application services on public networks in <a href="#">Compliance Manager</a></li> </ul>	<p>(5)(1)(f), (32)(1)(a)</p>
<p><i>Secure system engineering principles (6.11.2)</i></p>	<p>The customer should understand how systems are designed and engineered to consider protection of personal data. Where a customer uses a system engineered by a third party, it is their responsibility to ensure that such protections have been considered.</p>	<p>How Microsoft services include personal data protection principles as a mandatory part of our secure design/engineering principles.</p> <ul style="list-style-type: none"> <li>- SOC 2 Type 2 Audit Report [11] see <i>Security Development Lifecycle</i> pp23, CC7.1 pp45</li> <li>- Secure system engineering principles in <a href="#">Compliance Manager</a></li> </ul>	<p>(25)(1)</p>
<p><i>Supplier Relationships (6.12)</i></p>	<p>The customer should ensure that any information security and personal data protection requirements and that are the responsibility of a third party are addressed in contractual information or other agreements. The agreements should also address the instructions for processing.</p>	<p>How Microsoft services address security and data protection in our agreements with our suppliers and how we ensure those agreements are effectively implemented.</p> <ul style="list-style-type: none"> <li>- Who can access your data and on what terms [6]</li> <li>- Contracts for sub-processors: Contracting with Microsoft [7]</li> <li>- 6.12 Supplier Relationships in <a href="#">Compliance Manager</a></li> </ul>	<p>(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)</p>

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<p><b><i>Management of information security incidents and improvements (6.13.1)</i></b></p>	<p>The customer should have processes for determining when a personal data breach has occurred.</p>	<p>How Microsoft services determine if a security incident is a breach of personal data, and how we communicate the breach to you.</p> <ul style="list-style-type: none"> <li>- Office 365 and Breach Notification Under the GDPR [9]</li> <li>- Management of information security incidents and improvements 6.13.1 in <a href="#">Compliance Manager</a></li> </ul>	<p>(33)(2)</p>
<p><b><i>Responsibilities and procedures (during information security incidents) (6.13.2)</i></b></p>	<p>The customer should understand and document their responsibilities during a data breach or security incident involving personal data. Responsibilities may include notifying required parties, communications with processors or other third-parties, and responsibilities within the customer's organization.</p>	<p>How to notify Microsoft services if you detect a security incident or breach of personal data</p> <ul style="list-style-type: none"> <li>- Office 365 and Breach Notification Under the GDPR [9]</li> <li>- 6.13.2 Responsibilities and procedures in <a href="#">Compliance Manager</a></li> </ul>	<p>(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)</p>
<p><b><i>Response to information security incidents (6.13.3)</i></b></p>	<p>The customer should have processes for determining when a personal data breach has occurred.</p>	<p>Descriptions of the information Microsoft services provide to help you decide if a breach of personal data has occurred.</p> <ul style="list-style-type: none"> <li>- Office 365 and Breach Notification Under the GDPR [9]</li> <li>- 6.13.3 Response to information security incidents in <a href="#">Compliance Manager</a></li> </ul>	<p>(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)</p>
<p><b><i>Protection of records (6.15.1)</i></b></p>	<p>The customer should understand the requirements for records related to personal data processing that need to be maintained.</p>	<p>How Microsoft services store records relating to the processing of personal data</p> <ul style="list-style-type: none"> <li>- Search the audit log in Office 365 Security and Compliance Center [16]</li> <li>- Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability [12] see A.18.1.3</li> <li>- Office 365 ISMS Manual [14], see <i>9 Performance evaluation</i></li> </ul>	<p>(5)(2), (24)(2)</p>

CATEGORY	CUSTOMER CONSIDERATION	SUPPORTING MICROSOFT DOCUMENTATION	ADDRESSES GDPR ARTICLE(S)
<i>Independent review of information security (6.15.2)</i>	The customer should be aware of requirements for assessments of the security of personal data processing. This may include internal or external audits, or other measures for assessing the security of processing. Where the customer is dependent on another organization of third party for all or part of the processing, they should collect information about such assessments performed by them.	How Microsoft services test and assesses the effectiveness of technical and organizational measures to ensure the security of processing, including any audits by third parties. - Microsoft Online Services Terms, Data Protection Terms, see Data Security, Auditing Compliance [1] - Office 365 ISMS Manual [14]see 9 Performance evaluation - 6.15.2 Independent review of information security in <a href="#">Compliance Manager</a>	(32)(1)(d), (32)(2)
<i>Technical compliance review (6.15.3)</i>	The customer should understand requirements for testing and evaluating the security of processing personal data. This may include technical tests such as penetration testing. Where the customer uses a third-party system or processor, they should understand what responsibilities they have for securing and testing the security (for example, managing configurations to secure data and then testing those configuration settings). Where the third party is responsible for all or part of the security of processing, the customer should understand what testing or evaluation the third party performs to ensure the security of the processing.	How Microsoft services are tested security based on identified risks, including tests by third parties, and the types of technical tests and any available reports from the tests. - Microsoft Online Services Terms, Data Protection Terms, see Data Security, Auditing Compliance [1] - For a listing of external certifications, see <i>Microsoft Trust Center Compliance offerings</i> [13] - For more information about penetration testing your applications, see FedRAMP Moderate FedRAMP System Security Plan (SSP) [3], CA-8 Penetration Testing (M) (H) pp204 - 6.15.3 Technical compliance review in <a href="#">Manager</a>	(32)(1)(d), (32)(2)

## 6. Bibliography of resources and links

ID	DESCRIPTION/LINK
1	<a href="#">Online Service Terms</a>
2	<a href="#">Office 365 Security Documentation</a>
3	<a href="#">FedRAMP Moderate FedRAMP System Security Plan (SSP)</a>

ID	DESCRIPTION/LINK
4	<a href="#">Microsoft Cloud Security Policy</a>
5	<a href="#">Office 365 Information Protection for GDPR</a>
6	<a href="#">Who can access your data and on what terms?</a>
7	<a href="#">Contracts for sub-processors: Contracting with Microsoft</a>
8	<a href="#">365 Data Subject Requests for GDPR</a>
9	<a href="#">Office 365 and Breach Notification Under the GDPR</a>
10	<a href="#">Key Information from Office 365 for Customer Data Protection Impact Assessments</a>
11	<a href="#">SOC 2 Type 2 Audit Report</a>
12	<a href="#">Microsoft Office 365 ISO/IEC 27001:2013 ISMS Statement of Applicability</a>
13	<a href="#">Microsoft Trust Center Compliance offerings</a>
14	<a href="#">Office 365 ISMS Manual</a>
15	<a href="#">Use Tenant Restrictions to manage access to SaaS cloud applications</a>
16	<a href="#">Search the audit log in Office 365 Security and Compliance Center</a>
17	<a href="#">Encryption in the Microsoft Cloud</a>
18	<a href="#">Microsoft's Data Protection Officer</a>

## Learn more

- [Microsoft Trust Center](#)
- [Service Trust Portal](#)

# Data Subject Requests and the GDPR and CCPA

2/5/2021 • 4 minutes to read • [Edit Online](#)

The General Data Protection Regulation (GDPR) introduces new rules for organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents no matter where you or your enterprise are located. Additional details can be found in the [GDPR Summary topic](#).

Similarly, the California Consumer Privacy Act (CCPA), provides privacy rights and obligations to California consumers, including rights similar to GDPR's Data Subject Rights, such as the right to delete, access, and receive (portability) their personal information. The CCPA also provides for certain disclosures, protections against discrimination when electing exercise rights, and "opt-out/ opt-in" requirements for certain data transfers classified as "sales". This document guides you to information on the completion of Data Subject Requests (DSRs) under the GDPR and CCPA using Microsoft products and services.

- [Office 365](#)
- [Azure](#)
- [Intune](#)
- [Dynamics 365](#)
- [Visual Studio Family](#)
- [Azure DevOps Services](#)
- [Microsoft Support and Professional Services](#)

## Terminology

Helpful definitions for GDPR terms used in this document:

- *Data Controller (Controller)*: A legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- *Personal data and data subject*: Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly.
- *Processor*: A natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller.
- *Customer Data*: Data produced and stored in the day-to-day operations of running your business.

## What is a DSR?

The General Data Protection Regulation (GDPR) gives rights to people (known in the regulation as data subjects) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the data controller or just controller). The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller.

California Consumer Privacy Act (CCPA) provides privacy rights and obligations to California consumers, including rights similar to GDPR's Data Subject Rights, such as the right to delete, access, and receive (portability) their personal information.

As a controller, you are obligated to promptly consider each DSR and provide a substantive response either by taking the requested action or by providing an explanation for why the DSR cannot be accommodated by the controller. A controller should consult with its own legal or compliance advisers regarding the proper disposition of any given DSR.

Several processes may be involved completing a DSR, subject to your organization's GDPR-compliance rules.

- **Discovery.** The process of determining what data is needed to complete a DSR.
- **Access.** Retrieval and potential transmission to the data subject of discovered information.
- **Rectify.** Implement changes or other requested personal data changes.
- **Restrict.** Changing the access or processing of persona data by restricting access, or removing data from the Microsoft cloud.
- **Export.** Providing a "structured, commonly used, machine-readable format" of personal data to the data subject, as provided by the GDPR's "right of data portability."
- **Delete.** Permanent removal of personal data from the Microsoft cloud.

## Specific DSR Considerations

### Insights generated by Microsoft Products or Services

[Insights](#) may be generated by services (MyAnalytics, etc.) Office 365 includes online services that provide insights to users and organizations that use them. Data generated by these services may produce personal data relevant to a DSR. Follow the link in the list below for details regarding service-specific DSR processes.

### DSRs for system-generated logs

Logs and related data generated by Microsoft may contain data deemed personal under GDPR's definition of "personal data." Restricting or rectifying data in system-generated logs is not supported. Data in system-generated logs constitutes factual actions conducted within the Microsoft cloud and diagnostic data; modifications would compromise the historical record of actions and increase fraud and security risks. Microsoft provides the ability to access, export, and delete system-generated logs that may be necessary to complete a DSR. Examples of such data may include:

- Product and service usage data such as user activity logs
- User search requests and query data
- Data generated by product and services resulting from system functionality and interaction by users or other systems.

### Yammer and Kaizala

Deleting a user's account will not remove system-generated logs for Yammer and Kaizala. To remove the data from these applications, see one of the following resources:

- [Manage GDPR data subject requests in Yammer Enterprise](#)
- [Export or delete a user's organizational data in Kaizala](#)

### National Clouds

In some national clouds, a global IT Administrator needs to delete system-generated logs.

### Microsoft Services

If your organization or users engage with Microsoft to receive, support related to Microsoft products and services some of this data may contain personal data. For more information, see [Microsoft Support and Professional Services Data Subject Requests for the GDPR](#).

### Microsoft Controller Products

In some circumstances, your organization's users may access Microsoft products or services for which Microsoft is the data controller. In those cases, your users need to initiate their own DSRs directly to Microsoft, and Microsoft fulfills the requests directly to the user.

### Third-party Products

For third-party products and services accessed through Microsoft account authentication, any data subject requests should be directed to the applicable third party.



## Data Subject Request admin tools

- **Security & Compliance Center:** User-generated data is exported by the [Security & Compliance Center](#) or in-application features.
- **Azure AD Admin Center:** Delete a data subject from Azure Active Directory and related services using [Azure AD Admin Center](#).
- **Microsoft Data Log Export:** System-generated logs can be exported by tenant administrators using the [Microsoft Data Log Export](#).

## Learn more

- [Microsoft Trust Center](#)

# Manage GDPR data subject requests with the DSR case tool in the Security & Compliance Center

2/5/2021 • 26 minutes to read • [Edit Online](#)

The EU General Data Protection Regulation (GDPR) is about protecting and enabling individuals' privacy rights inside the European Union (EU). The GDPR gives individuals in the European Union (known as data subjects) the right to access, retrieve, correct, erase, and restrict processing of their personal data. Under the GDPR, personal data means any information relating to an identified or identifiable natural person. A formal request by a person to their organization to take an action on their personal data is called a Data Subject Request or DSR. For detailed information about responding to DSRs for data in Office 365, see [Office 365 Data Subject Request Guide](#).

To manage investigations in response to a DSR submitted by a person in your organization, you can use the DSR case tool in the Security & Compliance Center to find content stored in:

- Any user mailbox in your organization. This includes Skype for Business conversations and one-to-one chats in Microsoft Teams
- All mailboxes associated with an Microsoft 365 Group and all team mailboxes in Microsoft Teams
- All SharePoint Online sites and OneDrive for Business accounts in your organization
- All Teams sites and Microsoft 365 Group sites in your organization
- All public folders in Exchange Online

Using the DSR case tool you can:

- Create a separate case for each DSR investigation.
- Control who has access to the DSR case by adding people as members of the case; only members can access the case and can only see their cases in the list of cases on the **DSR cases** page in the Security & Compliance Center. Also, you can assign different permissions to different members of the same case. For example, you can allow some members to only view the case and search results and allow other members to create searches and export search results.
- Use the built-in search to search for all content created or uploaded by a specific data subject.
- Optionally revise the built-in search query and rerun the search to narrow the search results.
- Add other content searches associated with the DSR case. This includes creating searches that return partially indexed items and system-generated logs from the Office Roaming Service.
- Export data in response to a DSR access or export request.
- Delete cases when the DSR investigation process is complete. This removes all searches and export jobs associated with the case.

Here's the high-level process for using the DSR case tool to manage DSR investigations:

[Step 1: Assign eDiscovery permissions to potential case members](#)

[Step 2: Create a DSR case and add members](#)

[Step 3: Run the search query](#)

## Step 4: Export the data

### (Optional) Step 5: Revise the built-in search query

### More information about using the DSR case tool

#### IMPORTANT

Our tools can help admins perform DSR access or export requests by enabling them to utilize the built-in search and export functionality found in the DSR case tool. The tool helps to facilitate a best-effort method to export data that's relevant to a DSR request submitted by a data subject. However, it's important to note that search results can vary based on the data subject or the admin actions taken that may impact whether or not an item would be deemed as "personal data" for export purposes. For example, if the data subject was the last person to modify a file they didn't create, the file might not be returned in the search results. Similarly, an admin could export data without including partially indexed items or all versions of SharePoint documents. Therefore, the tools provided can help facilitate accessing and exporting data requests; however, the results are subject to specific admin and data subject usage scenarios.

## Step 1: Assign eDiscovery permissions to potential case members

By default, a global administrator can access the DSR case tool in the Security & Compliance Center. By design, other users such as a data privacy officer, a human resources manager, or other people involved in DSR investigations don't have access to the DSR case tool and will have to be assigned the appropriate permissions to access the tool. The easiest way to do this is to go to the **Permissions** page in the Security & Compliance Center and add users to the eDiscovery Manager role group. You also have to assign these permissions so you can add them as members of the DSR case that you create in Step 2.

For step-by-step instructions, see [Assign eDiscovery permissions in the Office 365 Security & Compliance Center](#).

#### NOTE

By default, a global administrator (or other members of the Organization Management role group in the Security & Compliance Center) don't have the necessary permissions to export Content Search results (see Step 4 in this article). To address this, an admin can add themselves as a member of the eDiscovery Manager role group.

## Step 2: Create a DSR case and add members

The next step is to create a DSR case. When you create a case, you can choose to start the built-in search or you can create the case without starting the search. The following procedure instructs you to create the case without starting the search and then show you how to add members to the case.

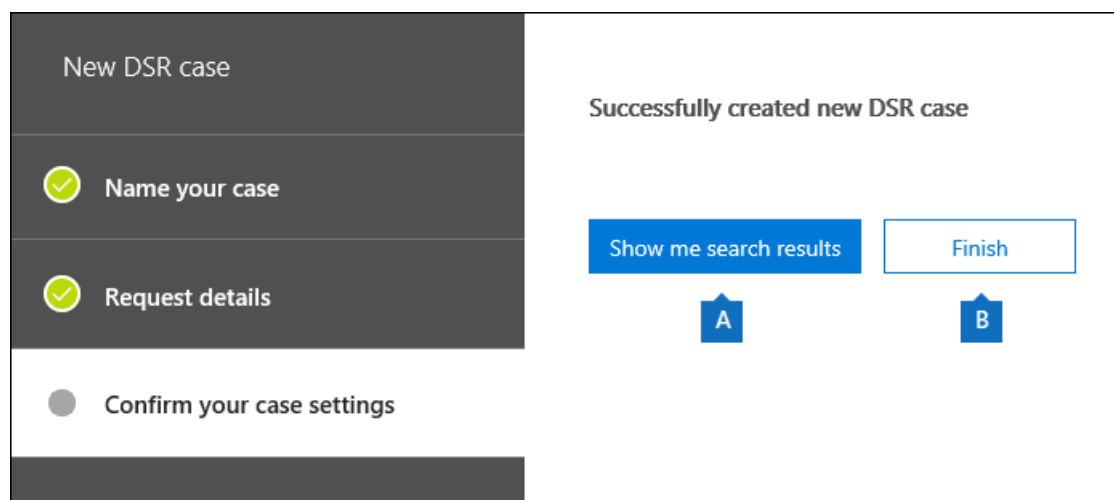
1. Go to <https://protection.office.com> and sign in using your work or school account.
2. In the Security & Compliance Center, click **Data privacy** > **Data subject requests**, and then click **+ New DSR case**.
3. On the **New DSR case** flyout page, give the case a name, type an optional description, and then click **Next**. The name of the case must be unique in your organization.

#### TIP

Consider adding the name of the person who submitted the DSR request that you're investigating in the name and/or description of the new case. Note that only members of this case (and eDiscovery Administrators) will be able to see the case in the list of cases on the **Data subject requests** page.

4. On the **Request details** page, under **Data subject (the person who filed this request)**, select the person that you want to find and export data for and then click **Next**.
5. On the **Confirm your case settings** page, you can change the case name and description, and select a different data subject. Otherwise, click **Save**.

A page is displayed that confirms the new DSR case has been created.



At this point, you can do one of two things:

- a. Clicking **Show me search results** starts the search. This is the default selection. The built-in search that's run when you select this option and the results that are returned are discussed in Step 3.
  - b. Clicking **Finish** closes the new DSR case without starting the built-in search. When you select this option, the new DSR case is displayed on the **Data subject requests** page.
6. Click **Finish** so that you can go in to the new DSR case and add members to it.
  7. On the **Data subject requests** page, click the name of the DSR case that you created.
  8. On the **Manage this case** flyout page, under **Manage members**, click **Add**.

Under **Users**, a list of people that are assigned the appropriate eDiscovery permissions is displayed. The people you assigned eDiscovery permissions to in Step 1 will be displayed in this list.

9. Select the people to add as members of the DSR case, click **Add**, and then save your changes.

You can also add role groups as members of DSR case by clicking **Add** under **Manage role groups**.

## Step 3: Run the search query

After you create a DSR case and add members, the next step is to run the built-in search that's associated with the case. This default search query does the following things:

- Searches all mailboxes in your organization for all email items that were sent or received by the data subject. This is accomplished by using the *Participants* email property, which searches for the data subject in all the people fields in an email message. This property returns items in which the data subject is in the **From**, **To**, **CC**, and **BCC** fields. Public folders in Exchange Online are also searched for messages sent or received by the data subject.
- Searches all sites in your organization for documents and items created or uploaded by the data subject. This is accomplished by using the following site properties:
  - The *Author* property returns items where the data subject is listed in the author field in Office documents. This value persists, even if the document is copied and uploaded by someone else.

- The *CreatedBy* property returns items that were created or uploaded by the data subject.

Here's what the keyword query looks like for the built-in search that gets automatically created when you create a DSR case.

```
participants:"<email address>" OR author:"<display name>" OR createdby:"<display name>"
```

For example, if the name of the data subject is Ina Leonte, the keyword query would look like this:

```
participants:"ina@contoso.com" OR author:"Ina Leonte" OR createdby:"Ina Leonte"
```

#### To run the built-in search for a DSR case:

1. In the Security & Compliance Center, click **Data privacy** > **Data subject requests**, and then click **Open** next to the DSR case that you created in Step 2.

Click the **Search** tab at the top of the page, and then click the checkbox next to the built-in search that was created when you created the DSR case. The search has the same name as the DSR case.

2. In the search flyout page, click **Open query**.

When you open the query, the search is started and will complete in a few moments.

3. When the search is complete, click **Preview results** to preview the search results. For more information, see [Preview search results](#).

#### TIP

You can also view the search query statistics to see the number of mailbox and site items that are returned by the search, and the top content locations that contain items that match the search query. For more information, see [View information and statistics about a search](#).

You can edit the built-in search query, change the content locations that are searched, and then rerun the search. See [Step 5](#) for more information.

## Step 4: Export the data

After you run the built-in search, you can export the search results. Alternatively, before you export the data, you may want to revise the query to reduce the number of search results. See [Step 5](#) for more information about narrowing the search results.

When you export search results, mailbox items can be downloaded in PST files or as individual messages. When you export content from SharePoint and OneDrive accounts, copies of native Office documents and other documents are exported. A results file that contains information about every exported item is included with the search results. For more detailed information about exporting, see [Export Content Search results](#).

#### NOTE

By default, a global administrator (or other members of the Organization Management role group in the Security & Compliance Center) don't have the necessary permissions to export Content Search results. To address this, an admin can add themselves as a member of the eDiscovery Manager role group.

The computer you use to export data has to meet the following system requirements:

- 32-bit or 64-bit versions of Windows 7 and later versions

- Microsoft .NET Framework 4.7
- A supported browser:
  - Microsoft Edge
- Or
- Microsoft Internet Explorer 10 and later versions

**NOTE**

Microsoft doesn't manufacture third-party extensions or add-ons for ClickOnce applications. Exporting data using an unsupported browser with third-party extensions or add-ons isn't supported.

**To export data from the built-in search in a DSR case:**

1. In the Security & Compliance Center, click **Data privacy** > **Data subject requests**, and then click **Open** next to the DSR case that you want to export data from.
2. Click the **Search** tab at the top of the page, and then click the checkbox next to the built-in search that was created when you created the DSR case. Or click another search to export data from that search.
3. On the search flyout page, click **More**, and then select **Export results** from the drop-down list.
4. On the **Export results** page, select the following recommended options for DSR export requests.

# Export results

When you start this export, we'll begin getting these search results ready for download. This may take a while depending on the size of your search results. [Learn more](#)

## Population:

Searchable Files: Ina Leonte\_DSRCASE

## Output options:

- All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons
- All items, including ones that have unrecognized format, are encrypted, or weren't indexed for other reasons
- Only items that have an unrecognized format, are encrypted, or weren't indexed for other reasons

A

## Export Exchange content as:

- One PST file for each mailbox
- One PST file containing all messages
- One PST file containing all messages in a single folder
- Individual messages

B

Enable de-duplication for Exchange content

Include versions for SharePoint files

Export files in a compressed (zipped) folder. Includes only individual messages and SharePoint documents.

C

## Estimation:

	Number	Volume	Updated to
Searchable items	394 results	58.21 MB	Apr 16, 2018 3:25:19 PM
Unsearchable items	9 results	912.83 KB	Apr 16, 2018 3:25:19 PM
Total items	403 results	59.1 MB	Apr 16, 2018 3:25:19 PM

After starting the export, a new export object with name "Ina Leonte\_DSRCASE\_Export" will be created in the Export table. To see status and download results, select the "Export" menu option.

Export

Cancel

a. Under **Output options**, select the first option (**All items, excluding ones that have ones that have an unrecognized format, are encrypted, or weren't indexed for other reasons**) to export indexed items only. The reason you don't want to export partially indexed items from the built-in search is because partially indexed items from other users will also be exported. To export only the partially indexed items for the data subject, we recommend that you create a separate search. For more information, see [Exporting partially indexed items](#) in the "More information about using the DSR case tool" section.

b. Under **Export Exchange content as**, select the third option, **One PST file containing all messages in a single folder**. Because some of the results may be for items that originated in another

user's mailbox, this option just lists the item in a single folder without indicating the actual mailbox and is the best option to use when you de-duplicate the results as recommended in the next item. This option also lets the data subject review items in chronological order (items are sorted by sent date) without having to navigate the original mailbox folder structure for each item.

c. Select **Enable de-duplication** option to excludes duplicate email messages. We recommend this option because the built-in search searches all mailboxes in your organization. So if multiple copies of the same message are found in the mailboxes that were searched, this option means that only one copy of a message will be exported. This option, together with exporting messages in one PST file in a single folder, results in the best user experience for DSR export requests. The Results.csv export report lists all locations where duplicate messages were found.

Optionally, you can select **Include versions for SharePoint documents** option to export all versions of SharePoint and OneDrive documents. This requires that versioning is turned on for document libraries. This option helps to ensure that all relevant data is exported.

5. After you choose the export settings, click **Export**.

The search results are prepared for downloading, which means they're uploaded to the Azure Storage area for your organization in the Microsoft cloud. The next steps show you how to download this data to your local computer.

6. Click the **Export** tab to display the export job you created. Export jobs have the same name as the corresponding search with **\_Export** appended to the end of search name.
7. Click the export job that you just created to display the export flyout page. This page shows information about the search, such as the size and total number of items to be exported, and the percentage of the items that have been transferred to an Azure storage area. Click **Refresh** to update the upload status information.
8. Under **Export key**, click **Copy to clipboard**. You use this key in step 11 to download the search results.
9. Click **Download results** at the top of the export flyout page.
10. In the pop-up window at the bottom of the page, click **Open** to open the **eDiscovery Export Tool**. The **eDiscovery Export Tool** will be installed the first time you download search results.
11. In the **eDiscovery Export Tool**, paste the export key that you copied in step 8 in the appropriate box.
12. Click **Browse** to specify the location where you want to download the search result files.

#### **NOTE**

Due to the high amount of disk activity (reads and writes), you should download search results to a local disk drive; don't download them to a mapped network drive or other network location.

13. Click **Start** to download the search results to your computer.

The **eDiscovery Export Tool** displays status information about the export process, including an estimate of the number (and size) of the remaining items to be downloaded. When the export process is complete, you can access the files in the location where they were downloaded. For more information about the reports that included when you download Content Search results, see the [More information](#) section in "Export Content Search results".

After the data is exported, the search results and export reports are located in a folder that has the same name as the DSR case. The PST files that contain mailbox items are located in a subfolder named **Exchange**. Documents and other items from sites are located in a subfolder named **SharePoint**.



## (Optional) Step 5: Revise the built-in search query

After you run the built-in search, you can revise it to narrow the scope to return fewer search results. You can do this by adding conditions to the query. A condition is logically connected to the keyword query by the **AND** operator. That means to be returned in the search results, items must satisfy both the keyword query and any conditions you add. This is how conditions help to narrow the results. If you add two or more unique conditions to a search query (conditions that specify different properties), those conditions are logically connected by the **AND** operator. That means only items that satisfy all the conditions (in addition to the keyword query) are returned. If you add multiple values (separated by commas or semi-colons) to a single condition, those values are connected by the **OR** operator. That means items are returned if they contain any of the specified values for the property in the condition.

Here are some examples of the conditions that you can add to the built-in search query of a DSR case. The name of the actual property used in a search query is shown parentheses.

- **File type** (  `filetype`  ) – Specifies the extension of a document or file. Use this condition to search for documents and files created by specific Office applications, such as Word, Excel, and OneNote.
- **Message type** (  `kind`  ) – Specifies the type of email item to search for. For example, you can use the syntax  `kind:email OR kind:im`  to return only email messages and Skype for Business conversations or one-to-one chats in Microsoft Teams.
- **Compliance tag** (  `compliancetag`  ) – Specifies a label assigned to an email message or a document. This condition returns items that are classified with a specific label. Labels are used to classify email and documents for data governance and enforce retention rules based on the classification defined by the label. This is a useful condition for DSR investigations because your organization may be using labels to classify content related to data privacy or that contains personal data or sensitive information. For the value of this condition, use the complete label name or the first part of the label name with a wildcard. For more information, see [Learn about retention policies and retention labels in Office 365](#).

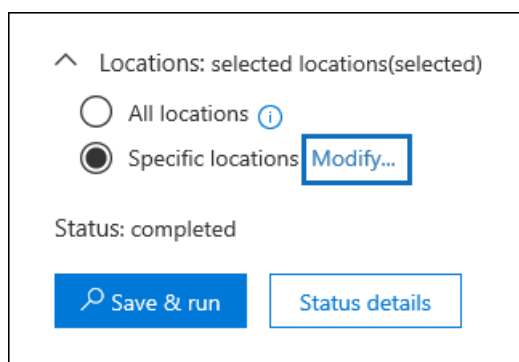
For a list and description of all the conditions available in the DSR case tool, see [Search conditions](#) in the "Keyword queries and search conditions for Content Search" article.

### Changing the content locations that are searched

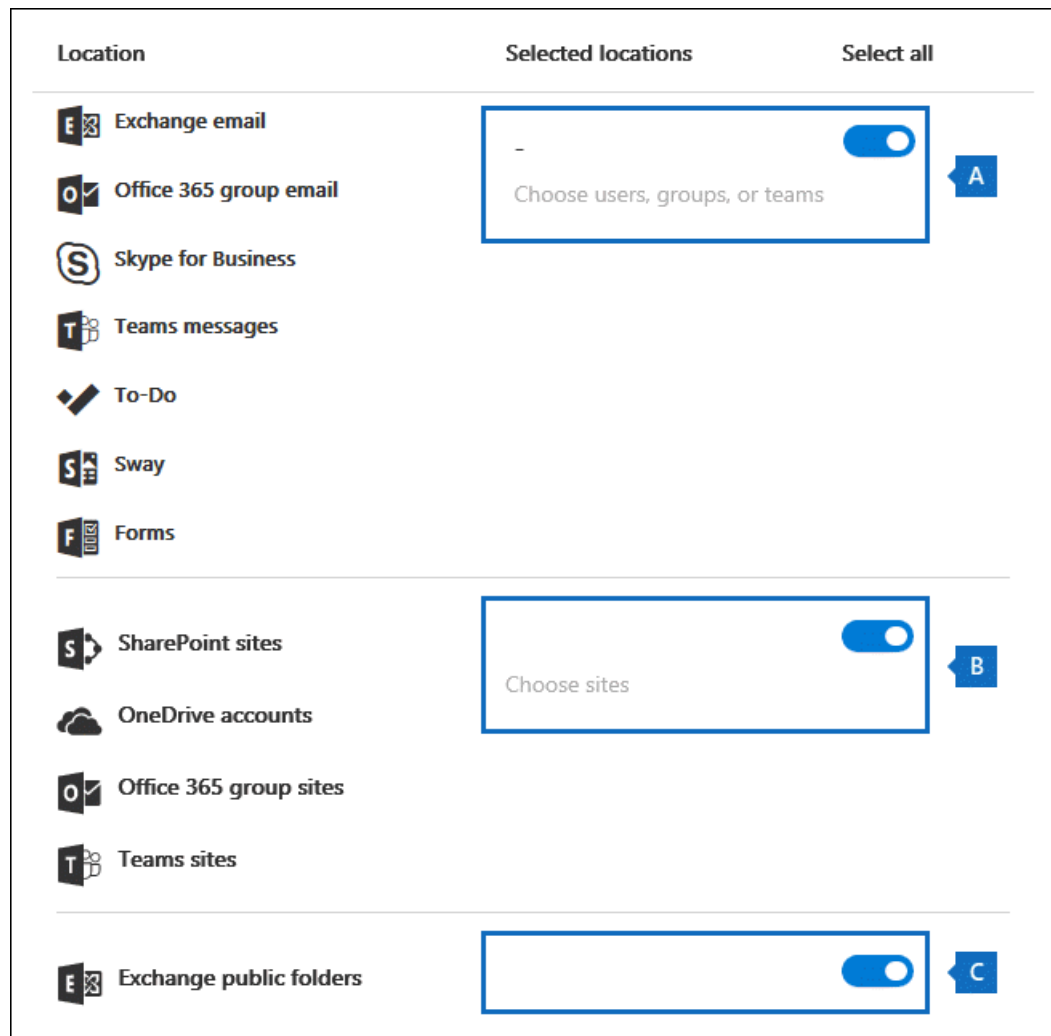
In addition to revising the built-in search for a DSR case, you can also change the content locations that are searched. As previously explained, the built-in search searches every mailbox and site in the organization, and any Exchange Online public folders. For example, you could narrow the search to only search the data subject's mailbox and OneDrive account and selected SharePoint sites. If you choose to search specific sites, you have to add each site that you want to search.

To modify the content locations to search:

1. Open the built-in search that you want to change the content locations for.
2. In the search query, under **Locations**, click **Modify** next to the **Specific locations** option.



The **Modify locations** flyout page is displayed. Here's a description of the content locations in the built-in search and some information about modifying the locations that are searched.



a. The toggle under **Select all** in mailbox section at the top of the flyout page is selected, which indicates that all mailboxes are searched. To narrow the scope of the search, click the toggle to unselect it, and then click **Choose users, groups, or teams** and choose specific mailboxes to search.

b. The toggle under **Select all** in the sites section in the middle of the flyout page is selected, which indicates that all sites are searched. To narrow the search to selected sites, you would unselect the toggle and then click **Choose sites**. You have to add each specific site that you want to search, including the data subject's OneDrive account.

c. The toggle in the Exchange public folders section is selected, which means all Exchange public folders are searched. You can only search all Exchange public folders or none of them. You can't choose specific ones to search.

3. If you modify the content locations in the built-in search, click **Save & run** to restart the search.

#### NOTE

When you search all mailbox locations or just specific mailboxes, data from other Office 365 applications that's saved to user mailboxes is included when you export the results of the search. This data won't be included in the estimated search results and isn't available for preview. But it's included when you export and download the search results. For more information the applications that store data in a user's mailbox, see [Content stored in Exchange Online mailboxes](#).

## More information about using the DSR case tool

The following sections contain more information about using the DSR case tool to respond to DSR export requests.

[Exporting data from the Office Roaming Service](#)

[Exporting partially indexed items](#)

[Searching and exporting data from Microsoft Teams and Microsoft 365 Groups](#)

[Searching Exchange public folders](#)

### **Exporting data from the Office Roaming Service**

You can use the DSR case tool to search for and export usage data that's generated by the Office Roaming Service. Roaming is a service that stores Office-related settings, such as Office theme, custom dictionary, language settings, developer mode, and auto correct.

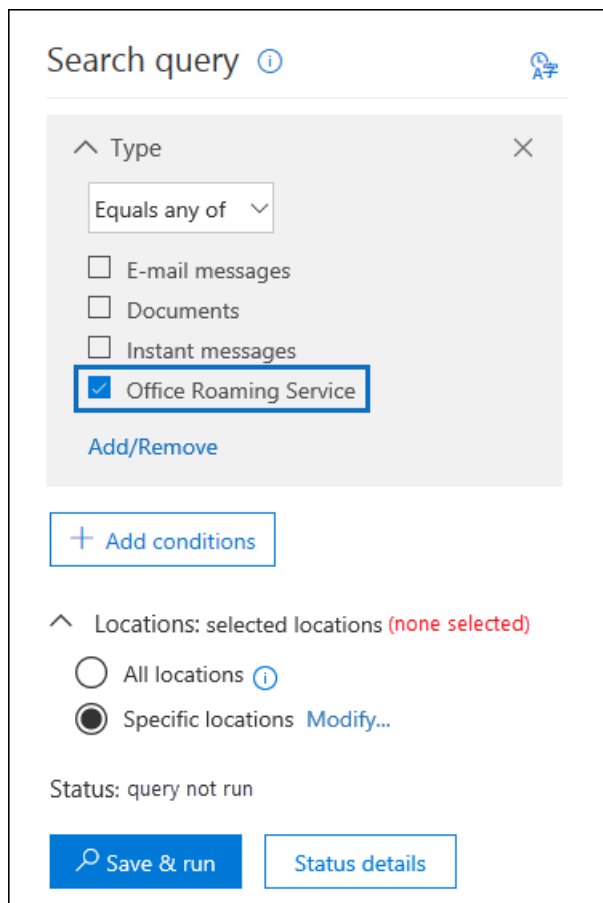
The data from the Office Roaming service is stored in a data subject's mailbox in a hidden folder located in a non-interpersonal message (non-IPM) subtree of Exchange Online mailboxes. This means that the data is hidden from the user's view when they use Outlook or other mail clients to access their mailbox. For more information about hidden folders, see [MAPI Hidden Folders](#).

You can create a separate content search (and associate it with a DSR case) that returns the Office Roaming Service usage data in the data subject's mailbox. This data isn't included in the search statistics and it won't be available for preview. But you can export it and then give it to the data subject in response to a DSR export request.

When you export data from the Office Roaming Service, the data is saved to a separate folder that's located in the **ApplicationDataRoot** folder, which is under a folder that is name with the data subject's email address. This data is exported as JSON files, which are human-readable text files similar to XML or TXT files, that are attached to email messages. Currently, this folder is named with the globally unique identifier (GUID): **1caee58f-eb14-4a6b-9339-1fe2ddf6692b**. In future versions of the DSR case tool, the GUID will be replaced with the name of the actual application.

#### **To search for and export Office Roaming Service data:**

1. In the Security & Compliance Center, click **Data privacy** > **Data subject requests**, and then click **Open** next to the DSR case for the data subject that you want to export usage data for.
2. Click the **Search** tab at the top of the page, and then click **+ Guided search**.
3. Click **Cancel** on the **Name your search** page.
4. Under **Search query**, in the **Type** condition, select the check box next to **Office Roaming Service**.



The **Type** condition (which are email message classes) should be the only item in the search query. You can delete the **Keywords** box or leave it blank.

5. Under **Locations**, make sure that **Specific locations** is selected, and then click **Modify**.
6. On top part of the **Modify locations** flyout page (the mailbox section), click **Choose users, groups, or teams**.
7. On the **Edit locations** page, click **Choose users, groups, or teams**, choose the data subject's mailbox, and then save your selection.
8. Click **Save & run**, and then name the search and save it.

The search is started.

#### To export Office Roaming Service data:

1. When the search that you created in the previous step is complete, click the **Search** tab at the top of the page, and then click the checkbox next to the search. You may have to click **Refresh** to display the search.
2. On the search flyout page, click **More**, and then select **Export results** from the drop-down list.
3. On the **Export results** page, select the recommended options to export usage data.

**Output options:**

All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons

All items, including ones that have unrecognized format, are encrypted, or weren't indexed for other reasons A

Only items that have an unrecognized format, are encrypted, or weren't indexed for other reasons

**Export Exchange content as:**

One PST file for each mailbox

One PST file containing all messages B

One PST file containing all messages in a single folder

Individual messages

Enable de-duplication for Exchange content

Include versions for SharePoint files C

Export files in a compressed (zipped) folder. Includes only individual messages and SharePoint documents.

a. Under **Output options**, select the first option (**All items, excluding ones that have ones that have an unrecognized format, are encrypted, or weren't indexed for other reasons**) to export indexed items only.

b. Under **Export Exchange content as**, select the second option, **One PST file containing all messages**.

c. Leave the remaining export options unselected.

4. After you choose the export settings, click **Export**.

The search results are prepared for downloading, which means they're uploaded to the Azure storage area for your organization in the Microsoft cloud. The next steps show you how to download this data to your local computer.

5. Click the **Export** tab to display the export job you created. The export jobs have the same name as the corresponding search with **\_Export** appended to the end of search name.

6. Click the export job that you just created to display the export flyout page.

7. Under **Export key**, click **Copy to clipboard**. You use this key in step 10 to download the search results.

8. Click **Download results** at the top of the export flyout page.

9. In the pop-up window at the bottom of the page, click **Open** to open the **eDiscovery Export Tool**. The **eDiscovery Export Tool** will be installed the first time you download search results.

10. In the **eDiscovery Export Tool**, paste the export key that you copied in step 7 in the appropriate box.

11. Click **Browse** to specify the location where you want to download the search result files.

#### NOTE

Due to the high amount of disk activity (reads and writes), you should download search results to a local disk drive; don't download them to a mapped network drive or other network location.

12. Click **Start** to download the search results to your computer.

The **eDiscovery Export Tool** displays status information about the export process, including an estimate of the number (and size) of the remaining items to be downloaded. When the export process is complete, you can open the Exchange PST file in Outlook and then go to the **ApplicationDataRoot** folder to access the subfolder for the Roaming service.

As previously explained, the JSON files that contain usage data are attached to messages. To view a JSON file, click a message and then open the attached JSON file.

#### Exporting partially indexed items

We recommend that you don't export partially indexed items (also called unindexed items) from the built-in search that's created when you create a DSR case. That's because the search results will more than likely include partially indexed items for other users in your organization, and not just partially indexed items for the data subject). Instead, we recommend that you create a separate Content Search that's associated with the DSR case that's designed to export only the partially indexed items related to the data subject.

Here's a high-level process to export partially indexed items. After they're export, you can review them to determine if an item is responsive to a DSR access or export request.

1. Open the DSR case and create a search on the **Search** page.
2. Use the following criteria for configuring the search query and the content locations to search:
  - Use an empty/blank keyword query. This returns all items in the content locations that are searched.
  - Search only the data subject's Exchange Online mailbox and their OneDrive account.
3. After you run the search and it completes, you can export and download the search results (as described in [Step 4](#)). Use the following settings to export partially indexed items.
  - Under **Output options**, select the third option (**Only items that have an unrecognized format, are encrypted, or weren't indexed for other reasons**) to export partially indexed items only.
  - Under **Export Exchange content as**, you can select any option based on your preferences.
  - Selecting the **Include versions for SharePoint documents** option exports versions of documents if a version is partially indexed.

For more information about partially indexed items, see:

- [Partially indexed items in Content Search in Office 365](#)
- [Exporting partially indexed items](#)

#### Searching and exporting data from Microsoft Teams and Microsoft 365 Groups

Conversations that are part of the Chat list in Microsoft Teams (called Team chats or one-to-one chats) are stored in the Exchange Online mailbox of the users who participate in the chats. Also, the files a person shares in a one-to-one chat are stored in the OneDrive account of the person who shares the file. Because the built-in search searches all mailboxes and OneDrive accounts in the organization, team chats and documents shared in a chat session (that the data subject created or uploaded) are returned by built-in search in a DSR case.

Alternatively, conversations that are part of a Teams channel (also called channel messages) are stored in the mailbox that's associated with a team. These types of conversations that the data subject participated in are also returned by the built-in search because all mailboxes associated with Teams are searched. Additionally, files that a data subject shares in a Teams channel are stored on the team's SharePoint site. Files created or uploaded by the data subject are returned by the built-in search in a DSR case because the sites associated with Teams are included in the search.

Similarly, mailboxes and SharePoint sites that correspond to an Microsoft 365 Group are also included in the built-in search. This means that email messages sent or received by the data subject and files created or uploaded by the data subject are returned.

For more information about using Content Search to search for items in Microsoft Teams and Microsoft 365 Groups or to see how to get a list of members, see the "Searching Microsoft Teams and Microsoft 365 Groups" section in [Content Search in Microsoft 365](#).

### Searching Exchange public folders

The built-in search in a DSR case will only return email messages that the data subject sent to a mail-enabled public folder or messages that someone else sent to a public folder and also copied the data subject. It doesn't return messages that the data subject posted to a public folder. To search for items that the data subject posted to a public folder, you can create a separate Content Search that searches for any item posted to a public folder by the data subject.

Here's a high-level process to search for items that the data subject posted to a public folder.

1. Open the DSR case and create a search on the **Search** page.
2. Use the following criteria for configuring the search query and the content locations to search:

- In the **Keywords** box, use the following search query:

```
itemclass:ipm.post AND "<email address of the data subject>"
```

- Search all Exchange public folders
- After you run the search and it completes, you can export and download the search results (as described in [Step 4](#)). Use the following settings to export partially indexed items.

# Azure Data Subject Requests for the GDPR and CCPA

2/5/2021 • 19 minutes to read • [Edit Online](#)

## Introduction to Data Subject Requests (DSRs)

The European Union [General Data Protection Regulation \(GDPR\)](#) gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of personal data, requesting corrections to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request* or DSR.

Similarly, the California Consumer Privacy Act (CCPA), provides privacy rights and obligations to California consumers, including rights similar to GDPR's Data Subject Rights, such as the right to delete, access and receive (portability) their personal information. The CCPA also provides for certain disclosures, protections against discrimination when electing exercise rights, and "opt-out/ opt-in" requirements for certain data transfers classified as "sales". Sales are broadly defined to include the sharing of data for a valuable consideration. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

The guide discusses how to use Microsoft products, services and administrative tools to help our controller customers find and act on personal data to respond to DSRs. Specifically, this includes how to find, access, and act on personal data that reside in the Microsoft cloud. Here's a quick overview of the processes outlined in this guide:

- **Discover:** Use search and discovery tools to more easily find customer data that may be the subject of a DSR. Once potentially responsive documents are collected, you can perform one or more of the DSR actions described in the following steps to respond to the request. Alternatively, you may determine that the request doesn't meet your organization's guidelines for responding to DSRs.
- **Access:** Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it that can be available to the data subject.
- **Rectify:** Make changes or implement other requested actions on the personal data, where applicable.
- **Restrict:** Restrict the processing of personal data, either by removing licenses for various Azure services or turning off the desired services where possible. You can also remove data from the Microsoft cloud and retain it on-premises or at another location.
- **Delete:** Permanently remove personal data that resided in the Microsoft cloud.
- **Export/Receive (Portability):** Provide an electronic copy (in a machine-readable format) of personal data or personal information to the data subject. Personal information under the CCPA is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. The defined term "personal information" roughly lines up with "personal data" under GDPR. However, the CCPA also includes family and household data. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

Each section in this guide outlines the technical procedures that a data controller organization can take to respond to a DSR for personal data in the Microsoft cloud.



# Terminology

The following provides definitions of terms that are relevant to this guide.

- **Controller:** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller, or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Personal data and data subject:** Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- **Processor:** A natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller.
- **Customer Data:** All data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, a customer through use of the enterprise service. Customer Data includes both (1) identifiable information of end users (for example, user names and contact information in Azure Active Directory) and Customer Content that a customer uploads into or creates in specific services (for example, customer content in an Azure Storage account, customer content of an Azure SQL Database, or a customer's virtual machine image in Azure Virtual Machines).
- **System-Generated Logs:** Logs and related data generated by Microsoft that help Microsoft provide enterprise services to users. System-generated logs contain primarily pseudonymized data, such as unique identifiers — typically a number generated by the system that cannot on its own identify an individual person but is used to deliver the enterprise services to users. System-generated logs may also contain identifiable information about end users, such as a user name.

## How to use this guide

This guide consists of two parts:

- **Part 1: Responding to Data Subject Requests for Customer Data:** Part 1 of this guide discusses how to access, rectify, restrict, delete, and export data from applications in which you have authored data. This section details how to execute DSRs against both Customer Content and also identifiable information of end users.
- **Part 2: Responding to Data Subject Requests for System-Generated Logs:** When you use Microsoft's enterprise services, Microsoft generates some information, known as System-Generated Logs, in order to provide the service. Part 2 of this guide discusses how to access, delete, and export such information for Azure.

## Understanding DSRs for Azure Active Directory and Microsoft service accounts

When considering services provided to enterprise customers, execution of DSRs must always be understood within the context of a specific Azure Active Directory (AAD) tenant. Notably, DSRs are always executed within a given AAD tenant. If a user is participating in multiple tenants, it is important to emphasize that a given DSR is *only* executed within the context of the specific tenant the request was received within. This is critical to understand as it means the execution of a DSR by one enterprise customer **will not** impact the data of an adjacent enterprise customer.

The same also applies for Microsoft Service Accounts (MSA) within the context of services provided to an enterprise customer: execution of a DSR against an MSA account *associated with an AAD tenant* **will only** pertain to data within the tenant. In addition, it is important to understand the following when handling MSA

accounts within a tenant:

- If an MSA user creates an Azure subscription, the subscription will be handled as if it were an AAD tenant. Consequently, DSRs are scoped within the tenant as described above.
- If an Azure subscription created via an MSA account is deleted, **it will not affect** the actual MSA account. Again, as noted above, DSRs executing within the Azure subscription are limited to the scope of the tenant itself.

DSRs against an MSA account itself, **outside a given tenant**, are executed via the Consumer Privacy Dashboard. Please refer to the Windows Data Subject Request Guide for further details.

## Part 1: DSR Guide for customer data

### Executing DSRs against customer data

Microsoft provides the ability to access, delete, and export certain Customer Data through the Azure Portal and also directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services (also referred to as *in-product experiences*). Details regarding such in-product experiences are described in the respective services' reference documentation.

#### IMPORTANT

Services supporting in-product DSRs require direct usage of the service's application programming interface (API) or user interface (UI), describing applicable CRUD (create, read, update, delete) operations. Consequently, execution of DSRs within a given service must be done in addition to execution of a DSR within the Azure Portal in order to complete a full request for a given data subject. Please refer to specific services' reference documentation for further details.

### Step 1: Discover

The first step in responding to a DSR is to find the personal data that is the subject of the request. This first step — finding and reviewing the personal data at issue — will help you determine whether a DSR meets your organization's requirements for honoring or declining a DSR. For example, after finding and reviewing the personal data at issue, you may determine the request doesn't meet your organization's requirements because doing so may adversely affect the rights and freedoms of others.

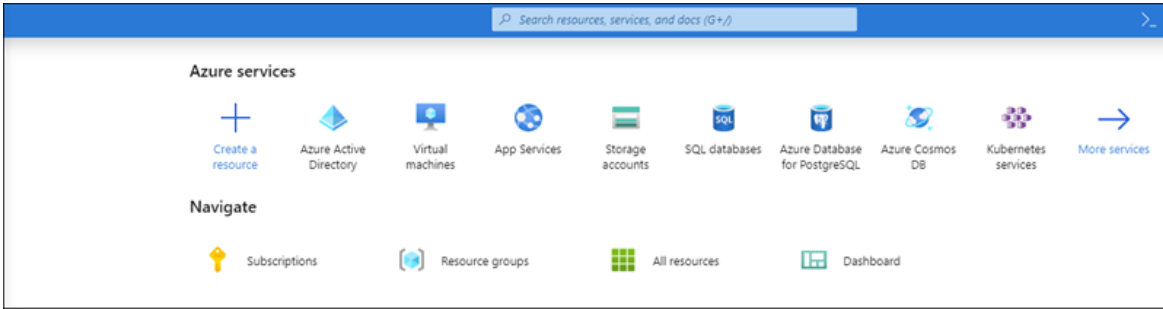
After you find the data, you can then perform the specific action to satisfy the request by the data subject.

[Azure Active Directory](#) is Microsoft's cloud-based, multi-tenant directory and identity management service. You can locate identifiable information of end users, such as customer and employee user profiles and user work information that contain personal data in your [Azure Active Directory](#) (AAD) environment by using the [Azure portal](#).

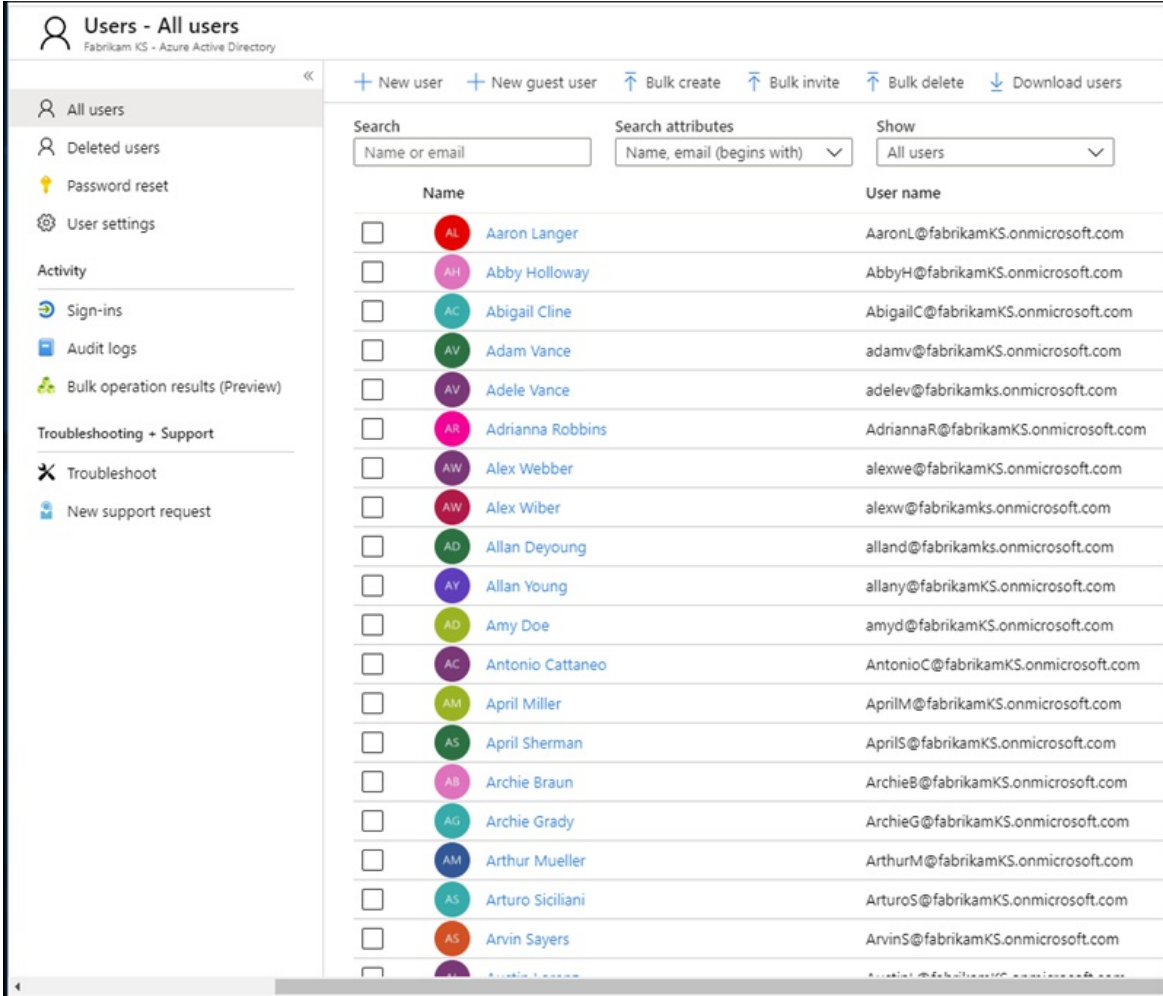
This is particularly helpful if you want to find or change personal data for a specific user. You can also add or change user profile and work information. You must sign in with an account that's a global admin for the directory.

#### How do I locate or view user profile and work information?

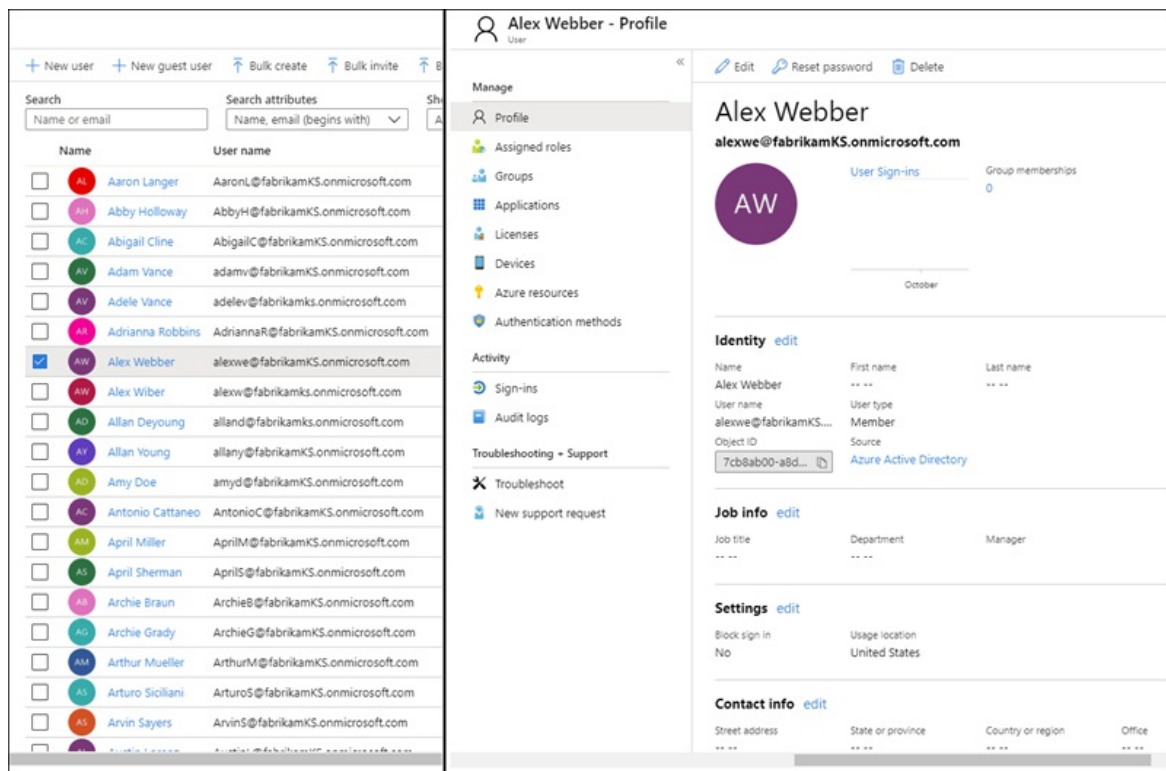
1. Sign in to the [Azure portal](#) with an account that's a global admin for the directory.
2. Select **Azure Active Directory**.



3. Select Users.



4. On the All users blade, select a user from the list, and then, on the blade for the selected user, select Profile to view user profile information that might contain personal data.



5. If you need to add or change user profile information, you can do so by selecting **Edit** in the command bar, then select **Save** after making changes.

### Service-specific interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

### Step 2: Access

After you've found Customer Data containing personal data that is potentially responsive to a DSR, it is up to you and your organization to decide which data to provide to the data subject. You can provide them with a copy of the actual document, an appropriately redacted version, or a screenshot of the portions you have deemed appropriate to share. For each of these responses to an access request, you will have to retrieve a copy of the document or other item that contains the responsive data.

When providing a copy to the data subject, you may have to remove or redact personal information about other data subjects and any confidential information.

### Azure Active Directory

Microsoft offers both a portal and in-product experiences providing the enterprise customer's tenant administrator the capability to manage DSR access requests. DSR Access requests allow for access of the personal data of the user, including: (a) identifiable information about an end-user and (b) system-generated logs.

### Service-specific interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

### Step 3: Rectify

If a data subject has asked you to rectify the personal data that resides in your organization's data, you and your organization will have to determine whether it's appropriate to honor the request. Rectifying the data may include taking actions such as editing, redacting, or removing personal data from a document or other type or item. The most expedient way to do this for Microsoft Support and FastTrack data is provided below.

## Azure Active Directory

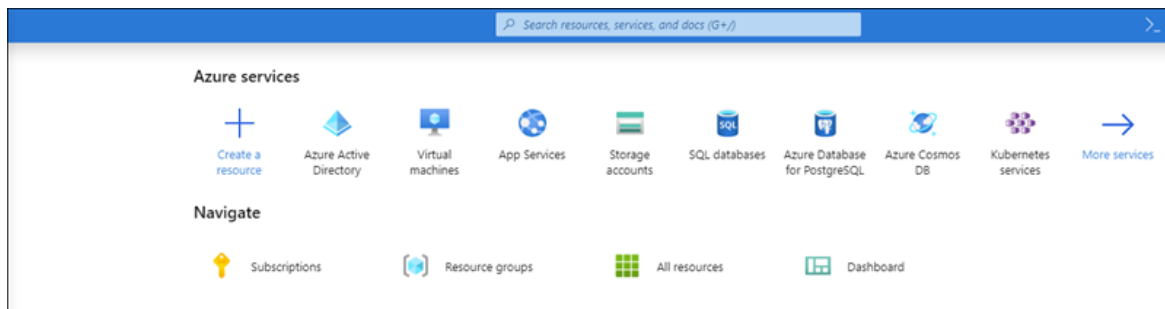
Enterprise customers have the ability to manage DSR rectify requests, including limited editing features per the nature of a given Microsoft service. As a data processor, Microsoft does not offer the ability to correct system-generated logs as it reflects factual activities and constitutes a historical record of events within Microsoft services. With respect to Azure Active Directory, limited editing features exist to rectify identifiable information about an end-user, as described further below.

### Azure Active Directory: rectify/correct inaccurate or incomplete personal data

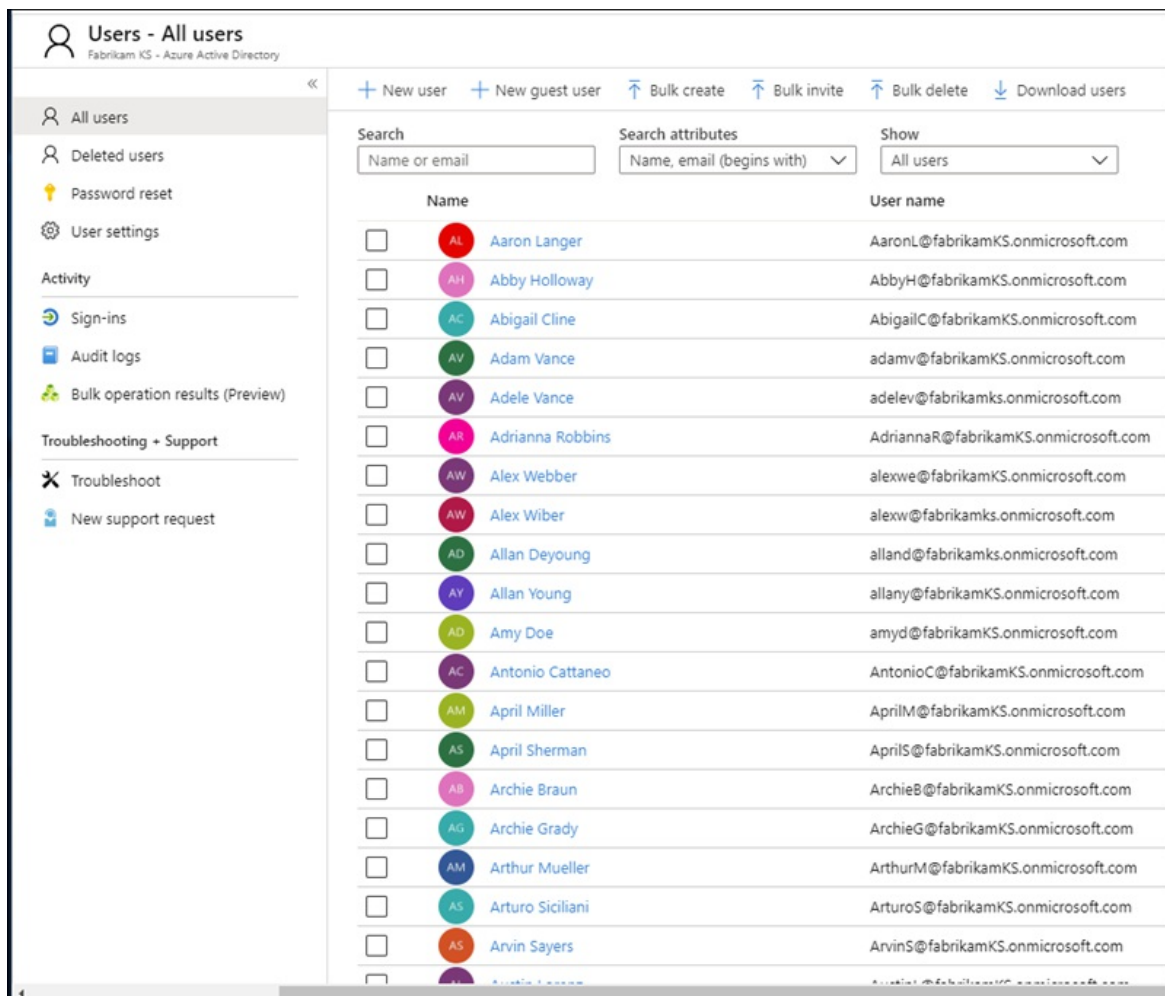
You can correct, update, or delete identifiable information about end users, such as customer and employee user profiles and user work information that contain personal data, such as a user's name, work title, address, or phone number, in your [Azure Active Directory](#) (AAD) environment by using the [Azure portal](#). You must sign in with an account that's a global admin for the directory.

#### How do I correct or update user profile and work information in Azure Active Directory?

1. Sign in to the [Azure portal](#) with an account that's a global admin for the directory.
2. Select [Azure Active Directory](#).

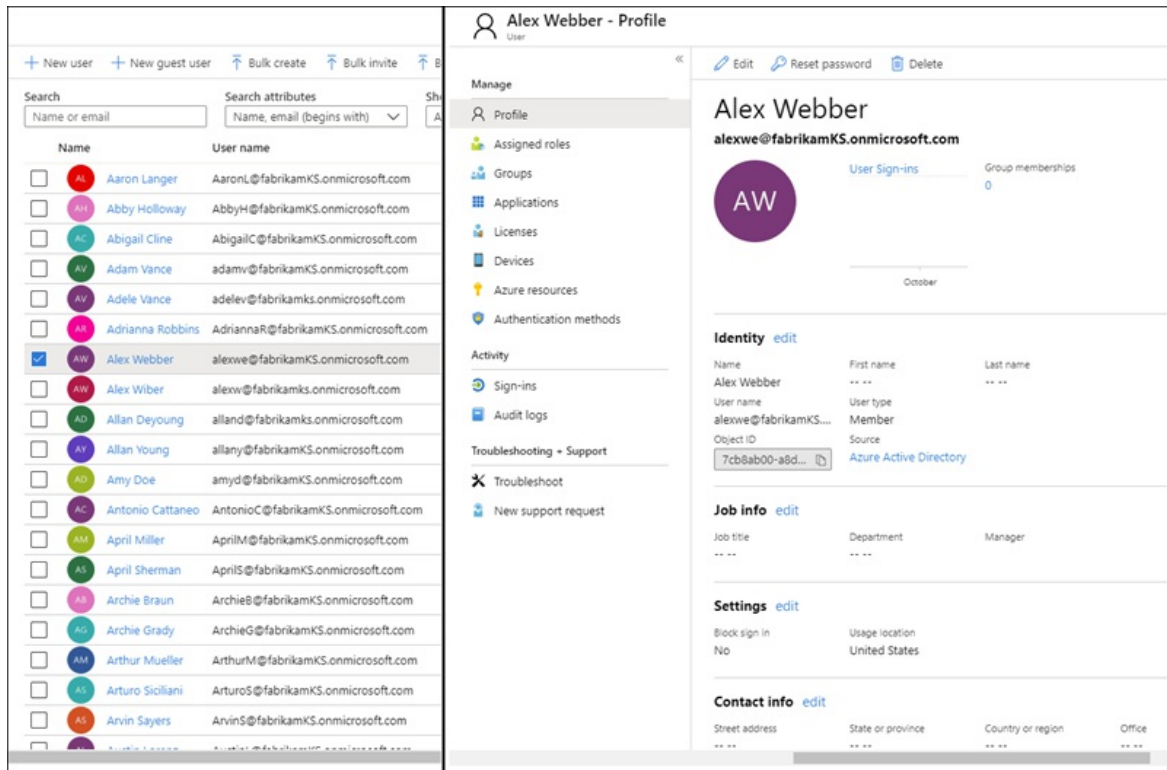


3. Select [Users](#).

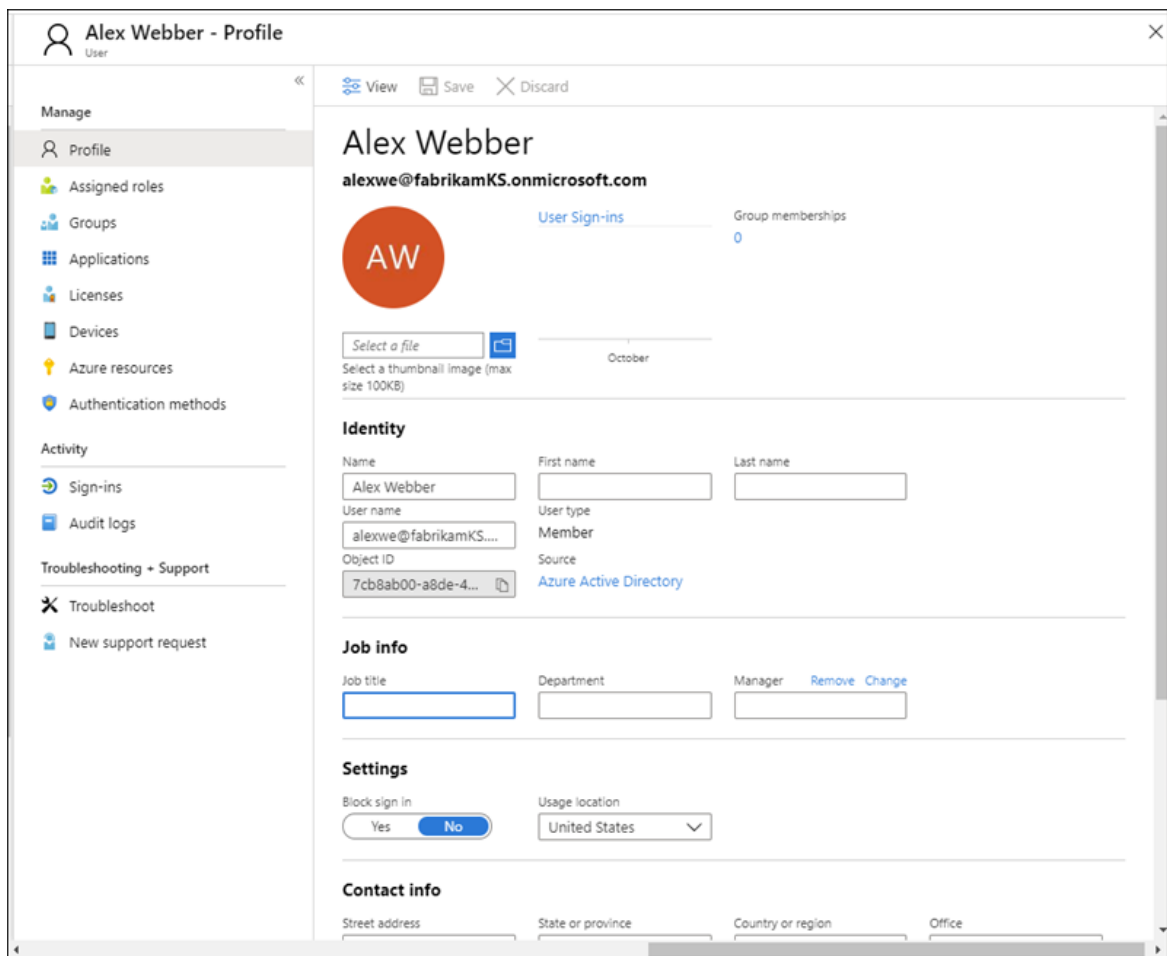


4. On the **All users** blade, select a user from the list, and then, on the blade for the selected user, select

Profile to view the user profile information that needs to be corrected or updated.



5. Correct or update the user profile information including work information by selecting **Edit** in the command bar, then select **Save** after making changes.



### Service-Specific Interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services'

reference documentation, describing applicable CRUD (create, read, update, delete) operations.

#### Step 4: Restrict

Data subjects may request that you restrict processing of their personal data. We provide both the Azure Portal and pre-existing application programming interfaces (APIs) or user interfaces (UIs). These experiences provide the enterprise customer's tenant administrator the capability to manage such DSRs through a combination of data export and data deletion. A customer may (1) export an electronic copy of the personal data of the user, including (a) account(s), (b) system-generated logs, and (c) associated logs, followed with (2) deletion of the account and associated data residing within Microsoft systems.

#### Step 5: Delete

The "right to erasure" by the removal of personal data from an organization's Customer Data is a key protection in the GDPR. Removing personal data includes removing all personal data and system-generated logs, except audit log information. When a user is **soft deleted** (see details below), the account is disabled for 30 days. If no further action is taken during this 30-day period, the user is **permanently deleted** (again, see details below). Upon a **permanent delete**, the user's account, personal data, and system-generated logs are expunged within an additional 30 days. If a tenant admin immediately issues a **permanent delete**, the user's account, personal data, and system-generated logs are expunged within 30 days of issuance.

#### IMPORTANT

You must be a tenant administrator to delete a user from the tenant.

#### Delete a user and associated data through the Azure portal

After you receive a delete request for a data subject, you can use the Azure portal to delete both a user and the associated personal information as well as system-generated logs.

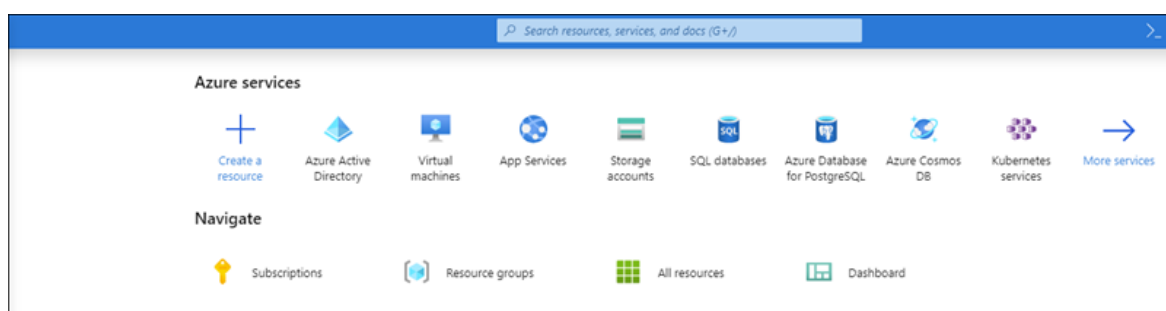
Deleting this data also means deleting the user from the tenant. Users are initially soft-deleted, which means the account can be recovered by a tenant admin within 30 days of being marked for soft-delete. After 30 days, the account is automatically, and permanently, deleted from the tenant. Prior to that 30 days, you can manually delete a soft-deleted user from the recycle bin.

Here's the high-level process for deleting users from your tenant.

1. Go to the Azure portal and locate the user.
2. Delete the user. When you initially delete the user, the user's account is sent to the Recycle Bin. **At this point, the user is soft deleted, meaning the account is disabled, but not expunged from Azure Active Directory.**
3. Go to the Recently deleted users list and permanently delete the user. **At this point the user is permanently deleted (also known as hard deleted), meaning the account has been expunged from Azure Active Directory**

To delete a user from an Azure tenant

1. Sign in to the [Azure portal](#) with an account that's a global admin for the directory.
2. Select **Azure Active Directory**.



### 3. Select Users.

The screenshot shows the 'Users - All users' page in the Azure Active Directory portal. The page title is 'Users - All users' and the subtitle is 'Fabrikam KS - Azure Active Directory'. The left sidebar contains navigation options: All users, Deleted users, Password reset, User settings, Activity, Sign-ins, Audit logs, Bulk operation results (Preview), Troubleshooting + Support, Troubleshoot, and New support request. The main content area has a search bar and a table of users. The table has two columns: 'Name' and 'User name'. The user 'Alex Wiber' is highlighted in blue. The 'Delete user' button is visible in the top right corner.

	Name	User name
<input type="checkbox"/>	Aaron Langer	AaronL@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Abby Holloway	AbbyH@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Abigail Cline	AbigailC@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Adam Vance	adamv@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Adele Vance	adelev@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Adrianna Robbins	AdriannaR@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Alex Webber	alexwe@fabrikamKS.onmicrosoft.com
<input checked="" type="checkbox"/>	Alex Wiber	alexw@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Allan Deyoung	alland@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Allan Young	allany@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Amy Doe	amyd@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Antonio Cattaneo	AntonioC@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	April Miller	AprilM@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	April Sherman	AprilS@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Archie Braun	ArchieB@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Archie Grady	ArchieG@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Arthur Mueller	ArthurM@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Arturo Siciliani	ArturoS@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Arvin Sayers	ArvinS@fabrikamKS.onmicrosoft.com

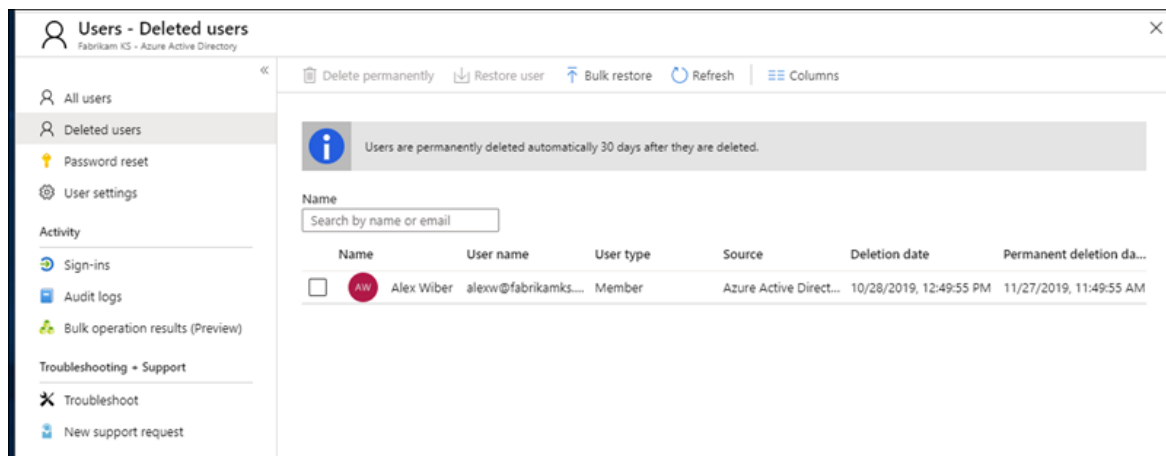
### 4. Check the box next to the user you want to delete, select **Delete user**, and then select **Yes** in the box asking if you want to delete the user.

The screenshot shows the 'Users - All users' page in the Azure Active Directory portal. The page title is 'Users - All users' and the subtitle is 'Fabrikam KS - Azure Active Directory'. The left sidebar contains navigation options: All users, Deleted users, Password reset, User settings, Activity, Sign-ins, Audit logs, Bulk operation results (Preview), Troubleshooting + Support, Troubleshoot, and New support request. The main content area has a search bar and a table of users. The user 'Alex Wiber' is highlighted in blue, and the checkbox next to it is checked. The 'Delete user' button is visible in the top right corner.

	Name	User name
<input type="checkbox"/>	Aaron Langer	AaronL@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Abby Holloway	AbbyH@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Abigail Cline	AbigailC@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Adam Vance	adamv@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Adele Vance	adelev@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Adrianna Robbins	AdriannaR@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Alex Webber	alexwe@fabrikamKS.onmicrosoft.com
<input checked="" type="checkbox"/>	Alex Wiber	alexw@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Allan Deyoung	alland@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Allan Young	allany@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Amy Doe	amyd@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Antonio Cattaneo	AntonioC@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	April Miller	AprilM@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	April Sherman	AprilS@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Archie Braun	ArchieB@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Archie Grady	ArchieG@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Arthur Mueller	ArthurM@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Arturo Siciliani	ArturoS@fabrikamKS.onmicrosoft.com
<input type="checkbox"/>	Arvin Sayers	ArvinS@fabrikamKS.onmicrosoft.com

### 5. On the **All users** blade, select **Deleted users**.

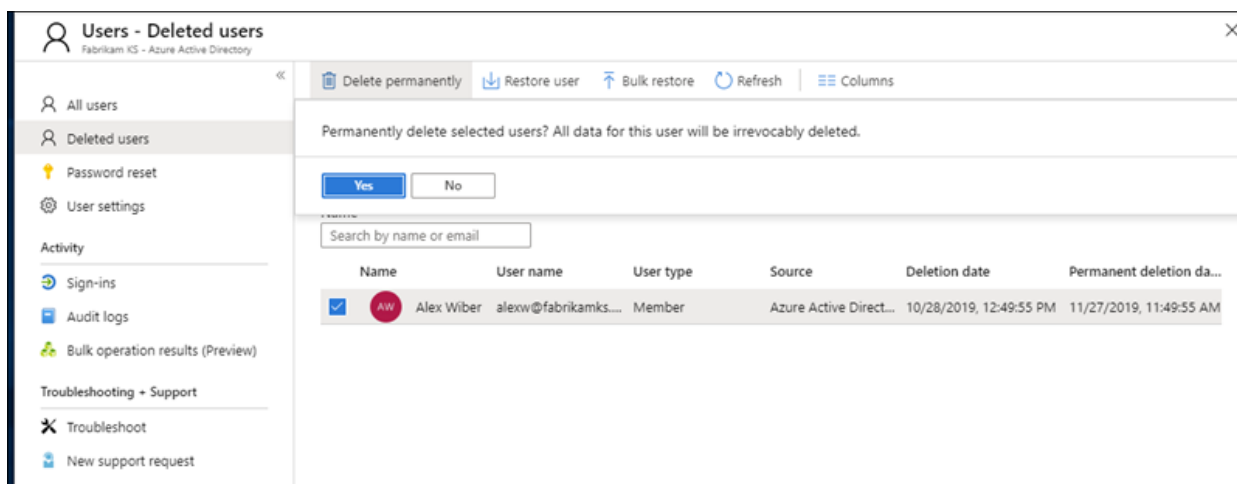




6. Select the same user again, select **Delete permanently** in the command bar, and then select **Yes** in the box asking if you're sure.

### IMPORTANT

Be aware that by clicking **Yes** you are permanently, and irrevocably, deleting the user and all associated data and system-generated logs. If you do this by mistake, you'll have to manually add the user back to the tenant. The associated data and system-generated logs are non-recoverable.



### Service-specific interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

## Step 6: Export

The "right of data portability" allows a data subject to request a copy of their personal data in an electronic format (that's a "structured, commonly used, machine read-able, and interoperable format") that may be transmitted to another data controller. Azure supports this by enabling your organization to export the data in the native JSON format, to your specified Azure Storage Container.

### IMPORTANT

You must be a tenant administrator to export user data from the tenant.

### Azure Active Directory

With respect to Customer Data, Microsoft offers both a portal and in-product experiences providing the

enterprise customer's tenant administrator the capability to manage export requests for identifiable information about an end user.

### Service-specific interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

## Part 2: System-Generated Logs

Microsoft also provides you with the ability to access, delete, and export certain system-generated logs associated with a user's use of Azure.

### IMPORTANT

The ability to restrict or rectify system-generated logs is not supported. System-generated logs constitute factual actions conducted within the Microsoft cloud and diagnostic data, and modifications to such data would compromise the historical record of actions, increasing fraud and security risks.

### Executing DSRs against System-Generated Logs

Microsoft provides the ability to access, delete, and export certain system-generated logs through the Azure Portal and also directly via programmatic interfaces or user interfaces for specific services. Details are described in the respective services' reference documentation.

### IMPORTANT

Services supporting in-product DSRs require direct usage of the service's application programming interface (API) or user interface (UI). Consequently, execution of an in-product DSRs **must be done in addition to execution of a DSR within the Azure Portal in order to complete a full request for a given data subject. Please refer to specific services' reference documentation for further details.**

### Step 1: Access

The tenant admin is the only person within your organization who can access system-generated logs associated with a particular user's use of Azure. The data retrieved for an access request will be provided in a machine-readable format and will be provided in files that will allow the user to know which services the data is associated with. As noted above, the data retrieved will not include data that may compromise the security of the service.

#### Azure Active Directory

Microsoft offers both a portal and in-product experiences providing the enterprise customer's tenant administrator the capability to manage access requests. Access requests will allow for access of the personal data of the user, including: (a) identifiable information about an end user and (b) service-generated logs. The process is identical to that described in the Azure Active Directory section of Part 1, Step 2: Access.

#### Service-specific interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

### Step 2: Delete

The tenant admin is the only person within your organization who can execute a DSR delete request for a particular user within an Azure tenant.

#### Azure Active Directory

Microsoft offers both a portal and in-product experiences providing the enterprise customer's tenant administrator the capability to manage DSR delete requests. DSR delete requests follow the same as described in the Delete a user and associated data through the Azure portal section of Part 1, Step 5: Delete.

### Service-specific interfaces

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

### Step 3: Export

The tenant admin is the only person within your organization who can access system-generated logs associated with a particular user's use of Azure. The data retrieved for an export request will be provided in a machine-readable format and will be provided in files that will allow the user to know which services the data is associated with. As noted above, the data retrieved will not include data that may compromise the security or stability of the service.

### Export system-generated logs using the Azure portal

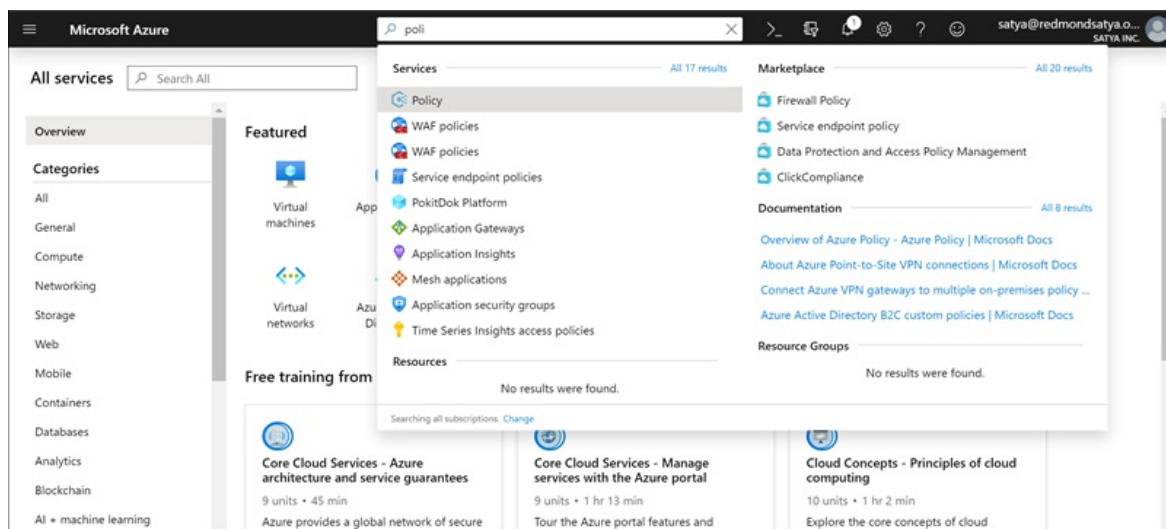
After you receive an export request for a data subject, you can use the Azure portal to export system-generated logs associated with a given user.

Here's the high-level process for exporting data from your tenant.

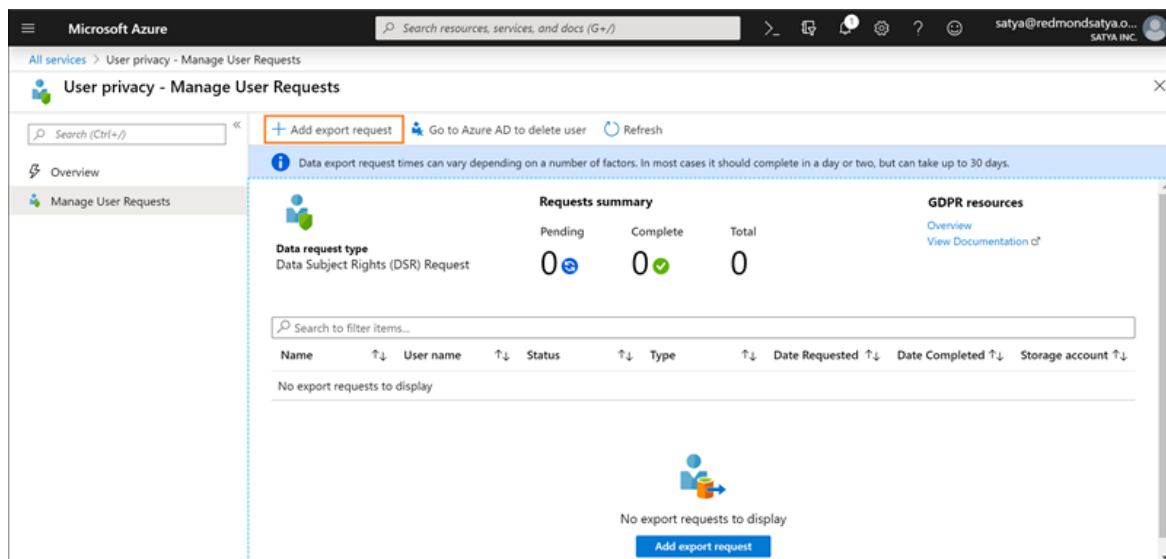
1. Go to the Azure portal and create an export request on behalf of the user.
2. Export the data and send file to user.

To export a user's info from an Azure tenant

1. Open the Azure portal, select **All services**, type *policy* into the filter, and then select **Policy**.



2. In the **Policy** blade, select **User privacy**, select **Manage User Requests**, and then select **Add export request**.



### 3. Complete the Export data request:

The screenshot shows the 'New export data request' form in the Azure portal. The form includes the following fields and options:

- User \***: A dropdown menu with the placeholder text 'Search by name or email'.
- Export destination**: A text area with the instruction 'Select the Azure subscription and storage account to export the data to. If you do not have an Azure subscription you can create a new Azure subscription. [Create subscription](#)'.
- Azure Subscription \***: A dropdown menu with the selected value 'MSFT Corp AMEX- Pay-As-You-Go'.
- Storage account \***: A dropdown menu with a 'Create new' link below it.

At the bottom of the form, there is a disclaimer: 'By clicking Create, you understand that Microsoft will have read and write permissions to this storage account for fulfilling this request and agree to the terms and conditions. [Terms and Agreements](#)'. Below the disclaimer are two buttons: 'Create' and 'Cancel'.

- **User.** Type the email address of the Azure Active Directory user that requested the export.
- **Subscription.** Select the account you use to report resource usage and to bill for services. This is also the location of your Azure storage account.
- **Storage account.** Select the location of your Azure Storage (Blob). For more info, see the [Introduction to Microsoft Azure Storage — Blob storage](#) article.
- **Container.** Create a new (or select an existing) container as the storage location for the user's exported privacy data.

### 4. Select Create.

The export request goes into **Pending** status. You can view the report status on the **User privacy** —

Overview blade.

**IMPORTANT**

Because personal data can come from multiple systems, it's possible that the export process might take up to one month to complete.

**Service-Specific Interfaces**

Microsoft provides the ability to discover Customer Data directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. Details are described in the respective services' reference documentation, describing applicable CRUD (create, read, update, delete) operations.

**Notify about exporting or deleting issues**

If you run into issues while exporting or deleting data from the Azure portal, go to the Azure portal **Help + Support** blade and submit a new ticket under **Subscription Management > Other Security and Compliance Request > Privacy Blade and GDPR Requests**.

## Learn more

- [Microsoft Trust Center](#)

# Azure DevOps Services Data Subject Requests for the GDPR and CCPA

2/5/2021 • 3 minutes to read • [Edit Online](#)

The European Union [General Data Protection Regulation \(GDPR\)](#) gives rights to people, known in the regulation as *data subjects*, to manage the personal data that's collected by a *data controller*. A data controller, or just *controller*, is an employer or other type of agency or organization. Personal data is defined broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data. These rights include obtaining copies of personal data, requesting corrections to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request*, or DSR.

Similarly, the California Consumer Privacy Act (CCPA), provides privacy rights and obligations to California consumers, including rights similar to GDPR's Data Subject Rights, such as the right to delete, access and receive (portability) their personal information. The CCPA also provides for certain disclosures, protections against discrimination when electing exercise rights, and "opt-out/ opt-in" requirements for certain data transfers classified as "sales". Sales are broadly defined to include the sharing of data for a valuable consideration. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

For general information about GDPR, see the [GDPR section of the Service Trust portal](#).

This guide discusses how to use Microsoft tools to export or delete personal data collected during an authenticated (signed-in) session of Azure DevOps Services (formerly known as Visual Studio Team Services).

## Additional privacy information

The [Microsoft Privacy Statement](#), [Online Services Terms \(OST\)](#), and [Microsoft's GDPR Commitments](#) articles describe our data processing practices.

## Personal data we collect

Microsoft collects data from users to operate and improve Azure DevOps Services. Azure DevOps Services collects two categories of data — customer data and system-generated logs. Customer data includes user-identifiable transactional and interactional data that Azure DevOps Services needs to operate the service. System-generated logs include service usage data that is aggregated for each product area and feature.

## Delete Azure DevOps data

The first step to delete associated Azure DevOps Services customer data and to anonymize personally identifiable data found in system-generated logs is to close your Azure Active Directory (AAD) identity account or Microsoft Account (MSA). Azure DevOps Services is relied upon as a system of record with strict integrity, traceability, and audit rules. These existing obligations affect our delete and retention obligations for GDPR. Closing the identity account does not alter, remove, or change artifacts and records associated with the individual identity in the Azure DevOps organization. We have ensured that when an entire Azure DevOps organization is deleted, all associated personally identifiable data, and system-generated logs found in that organization are removed from our system (after the requisite Azure DevOps organization 30-day soft-delete period).

## Export Azure DevOps data

Controllers can export customer data and system-generated logs collected from their data subjects by one of two methods, depending upon the identity provider (MSA or AAD) used to sign in to the Azure DevOps service.

- Users that authenticate using an account that is backed by an Azure tenant, for example, AAD account or MSA account associated with an Azure subscription, can follow the instructions in [Azure Data Subject Requests for the GDPR](#).
- Users that authenticate using an MSA identity can use this [Privacy Request site](#) to view activity data tied to their MSA identity across multiple Microsoft services. In this scenario, the user is a controller for their own personal data.

## Export or delete issues

For AAD identities, if you run into issues while exporting or deleting data from the Azure portal, go to the Azure portal **Help + Support** blade and submit a new ticket under **Subscription Management > Other Security and Compliance Request > Privacy Blade and GDPR Requests**.

For MSA identities, if you run into issues while exporting data from the Privacy Request site, log on to the [Privacy Request site](#) and submit a request for help from the Microsoft Privacy team via the request webform.

## Learn more

Microsoft is committed to ensuring that your Azure DevOps Services data remains secure and private, without exception. Visit the [Azure DevOps Services data protection overview](#) whitepaper to learn more about how we protect your Azure DevOps Services data.

## See also

- [Microsoft's GDPR commitments to customers of our generally available enterprise software products](#)
- [Microsoft Trust center](#)
- [Service Trust portal](#)
- [Microsoft privacy dashboard](#)
- [Microsoft privacy response center](#)
- [Azure Data Subject Requests for the GDPR](#)

# Dynamics 365 Data Subject Requests for the GDPR and CCPA

2/5/2021 • 21 minutes to read • [Edit Online](#)

The European Union [General Data Protection Regulation \(GDPR\)](#) gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called in this document a *Data Subject Rights Request* or DSR request.

Similarly, the California Consumer Privacy Act (CCPA), provides privacy rights and obligations to California consumers, including rights similar to GDPR's Data Subject Rights, such as the right to delete, access, and receive (portability) their personal information. The CCPA also provides for certain disclosures, protections against discrimination when electing exercise rights, and "opt-out/ opt-in" requirements for certain data transfers classified as "sales". Sales are broadly defined to include the sharing of data for a valuable consideration. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

The guide discusses how to use Microsoft's products, services, and administrative tools to help our controller customers find and act on personal data to respond to DSR requests. Specifically, this includes how to find, access, and act on personal data or personal information that reside in Microsoft's cloud. Here's a quick overview of the processes outlined in this guide:

- **Discover:** Use search and discovery tools to more easily find customer- data that may be the subject of a DSR request. Once potentially responsive documents are collected, you can perform one or more of the DSR actions described in the following steps to respond to the request. Alternatively, you may determine that the request doesn't meet your organizations guidelines for responding to DSR requests.
- **Access:** Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it that is available to the data subject.
- **Rectify:** Make changes or implement other requested actions on the personal data, where applicable.
- **Restrict:** Restrict the processing of personal data, either by removing licenses for various online services or turning off the desired services where possible. You can a
- **Delete:** Permanently remove personal data that resided in Microsoft's cloud.
- **Export/Receive (Portability):** Provide an electronic copy (in a machine-readable format) of personal data or personal information to the data subject. Personal information under the CCPA is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. The defined term "personal information" roughly aligns with "personal data" under GDPR. However, the CCPA also includes family and household data. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

Each section in this guide outlines the technical procedures that a data controller organization can take to respond to a DSR request for personal data in Microsoft's cloud

## GDPR terminology

The following list provides definitions of terms that are relevant to this guide:



- **Controller:** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller, or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Personal data and data subject:** Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- **Processor:** A natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller.
- **Customer Data:** All data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, a customer through use of the enterprise service. Customer Data includes both (1) identifiable information of end users (for example, user names and contact information in Azure Active Directory) and Customer Content that a customer uploads into or creates in specific services (for example, customer content in an Azure Storage account, customer content of an Azure SQL Database, or a customer's virtual machine image in Azure Virtual Machines).
- **System-Generated Logs:** Logs and related data generated by Microsoft that help Microsoft provide enterprise services to users. System-generated logs contain primarily pseudonymized data, such as unique identifiers—typically a number generated by the system that cannot on its own identify an individual person but is used to deliver the enterprise services to users. System-generated logs may also contain identifiable information about end users, such as a user name.

## How this guide can help you meet your controller responsibilities

The guide, divided into two parts, describes how to use Dynamics 365 products, services, and administrative tools to help you find and act on data in the Microsoft cloud in response to requests by data subjects who are exercising their rights under the GDPR. The first part addresses personal data that is included in customer data, followed by a part addressing other pseudonymized personal data captured in system-generated logs.

- **Part 1: Responding to Data Subject Rights (DSR) requests for Personal Data included in customer data:** Part 1 of this guide discusses how to access, rectify, restrict, delete, and export personal data from Dynamics 365 applications (software as a service), which is processed as part of the customer data you have provided to the online service.
- **Part 2: Responding to data subject rights requests for Pseudonymized Data:** When you use Dynamics 365 enterprise services, Microsoft generates some information (referred to within this document as *system-generated logs*) to provide the service, which is limited to the usage footprint left behind by end users to identify their actions in the system. Although this data cannot be attributed to a specific data subject without the use of additional information, some of it may be deemed personal under the GDPR. Part 2 of this guide discusses how to access, delete, and export system-generated logs produced by Dynamics 365.

## Preparing for data subject rights investigations

When data subjects exercise their rights and make requests, consider the following points:

- Properly identify the person and role—such as employee, customer, vendor—by using information that the data subject gave you as part of his or her request. This information might be a name, an employee ID or customer number, or other identifier.
- Record the data and time of the request. (You have 30 days to complete the request.)
- Affirm that the request meets your organization's requirements for honoring or declining a data subject's request. For example, you must make sure that executing the request doesn't conflict with any other legal, financial, or regulatory obligations that you have, or infringe on the rights and freedoms of others.

- Verify that you have the information that is related to the request.

## Part 1: Responding to Data Subject Rights Requests for personal data Included in customer data

In the following articles, you'll find information to help you prepare for and respond to DSR requests for personal data included in customer data processed in Dynamics 365. It is important to note that personal data could be present in other categories of data processed by Microsoft during the course of the service of an online services subscription, such as administrator data or support data defined in the Microsoft Privacy Statement. This document is limited to assist you in the process of discovery and management of DSR requests affecting personal data present in the customer data that you have provided to Dynamics 365.

Dynamics 365 is an online service that offers multiple data processing capabilities as a software-as-a-service (SaaS). As such, Dynamics 365 offers a broad array of functionality intended to process a diverse collection of data, which could vary by nature, purpose or other specific attributes, such as sales data, transactions, financials, HR information, etc. In light of this diversity, Dynamics 365 offers multiple forms, fields, schemas, end points, and logic to process customer data, which is also reflected in the multiple ways in which DSR requests could be addressed in each application. When Dynamics 365 applications offer several ways to address specific DSR requests, we will note those in this guide by pointing to the technical descriptions offered by each application.

### Dynamics 365

#### Finding customer data

The first step in responding to a data subject rights request is to search for and identify the customer data that is the subject of the request.

Classifying customer data appropriately is the cornerstone of working with personal data in Dynamics 365 Customer Engagement business applications. Dynamics 365 for Customer Engagement offers flexibility to build out an application extension around data classification. Proper classification enables you to identify information as personal data, thereby making it possible to locate and retrieve it when responding to requests from a data subject. It can also help enable compliance with legislative and regulatory requirements for collecting and managing personal data.

Microsoft provides capabilities that assist you in responding to data subject rights requests, and thereby accessing customer data. However, it is your responsibility to ensure that personal data is located and classified appropriately.

*Dynamics 365 for Customer Engagement* provides multiple methods for you to search for personal data within records such as: Advanced Find Search and Search for Records. These functions all enable you to identify (find) personal data.

- [Advanced Find Search](#)
- [Search for Records](#) across multiple record types

In Dynamics 365 for Marketing, you have the following additional capabilities:

1. [Build Power BI reports](#) in order to filter and identify customer data.
2. Utilize the Insight Views on contacts and objects of marketing execution to identify additional data points that may contain customer data.

*Dynamics 365 Customer Service Insights* provides a list of resources to help you [find customer data](#) in order to respond to GDPR requests from customers.

*Dynamics 365 for Finance and Operations* provide several ways for you to search for customer data. You as a Tenant Admin can perform the following actions to search for customer data:

- Organize your customer data in a way that serves the purpose of rapidly discovering personal data, see [how](#)

to [classify data inventory](#) for this purpose.

- Use the [Person search report](#) to find and collect personal data.
- [Extend the Person search report](#) by authoring a new entity or extending an existing entity.
- Use search and filter features to find specific personal data and export that data by using the Microsoft Office Export functionality or print that information to a .pdf using browser extensions.
- Author a custom form that locates and exports personal data.
- Author an external portal or website that allows an authenticated customer to see his or her personal data.

*Dynamics 365 Business Central* provides several ways for you to search for customer data. For details, see [Searching, filtering, and sorting data](#).

*Dynamics 365 for Talent* provides advanced search and filter features to find specific personal data and Microsoft Office Export functionality to export or print that information to a .pdf using browser extensions.

- Use the [Person search report](#) to find and collect customer data.
- [Extend the Person search report](#) by authoring a new entity or extending an existing entity.

### **Providing a copy of customer data**

Customer data in *Dynamics 365 for Customer Engagement* can be exported using the comprehensive entity export capabilities. Customer data can be exported to a static Excel file to facilitate a data portability request. Using Excel, you can then edit the personal data to be included in the portability request and then save as a commonly used, machine-readable format such as .csv or .xml. Dynamics 365 for Customer Engagement records also can be exported via the [Common Data Service Web API](#).

Additionally, for Dynamics 365 for Marketing a [dedicated API](#) is provided that allows customer to build extensions that retrieve additional records of captured customer interactions that may contain personal data. The API loads all the relevant information from the back-end system and assembles it into a single, portable document.

*Dynamics 365 Customer Service Insights* enables you to [provide a copy of customer data](#) by using data export.

Customer data in *Dynamics 365 for Finance and Operations* can be exported using the comprehensive entity export capabilities. Using [Data management and integration entities](#), the Tenant Admin may utilize provided entities, create new, or extend existing, entities for a repeatable personal data export to Excel or a number of other common formats using [Data import and export jobs](#). Alternatively, many lists can be exported to a static Excel file to facilitate a data portability request. When customer data is exported to Excel, you can then edit the personal data to be included in the portability request and then save the file as a commonly used, machine-readable format such as .csv or .xml. You may also consider using the *Person Search Report* to provide the data subject with data that you've classified as personal data.

In *Dynamics 365 Business Central*, you can make use of two features to provide a copy of customer data to a data subject:

You can export customer data to an Excel file. In Excel, you can then edit the customer data to be included in the portability request, and save it in a commonly used, machine-readable format, such as .csv or .xml. For details, see [Exporting your business data to Excel](#).

In *Dynamics 365 for Talent*, you may use [Extend the Person search report](#) to gather information in support of a request for a copy of the data subject's personal data.

### **Rectifying customer data**

*Dynamics 365 for Customer Engagement* gives you following methods for correcting inaccurate or incomplete customer data, or erasing customer data:

- Search for customer data using the capabilities mentioned in "Finding customer data" and directly edit data

in Customer Engagement Forms. Edits can be done at a single row level or multiple rows can be modified directly.

- Bulk editing multiple Customer Engagement records, you can utilize the Microsoft Office add-in to export data to Microsoft Excel, make your changes, and then import that modified data from Excel into Dynamics 365 for Customer Engagement.

Additionally, for Dynamics 365 for Marketing you can also:

- Update-my-data landing page, by editing single or multiple rows directly
- Prepare a [subscription centers](#) page that has as many editable contact fields that can be included. This page enables an end user to update their own information as much as possible.

*Dynamics 365 Customer Service Insights* also provides capabilities that enable organizations to [rectify or make changes to customer data](#).

In *Dynamics 365 for Finance and Operations*, you may also use of [customization tools](#), but the decision and implementation is your responsibility.

*Dynamics 365 Business Central* offers two ways to correct inaccurate or incomplete customer data.

To quickly bulk-edit multiple Business Central records, you can export lists to Excel using the [Business Central Excel Add-in](#) to correct multiple records, and then publish the modified data from Excel in Business Central. For details, see [Exporting your Business Data to Excel](#).

You can change customer data stored in any field—such as information about a customer in the Customer card—by manually editing the data element containing the target personal data. For details, see [Entering data](#).

#### **Brief note about modifying entries in business transactions**

Transactional records, such as general, customer, and tax ledger entries, are essential to the integrity of an enterprise resource planning system. Personal data that is part of a financial or other transaction is kept "as is" for compliance with financial laws (for example, tax laws), prevention of fraud (such as security audit trail), or compliance with industry certifications. Therefore, Dynamics 365 for Finance and Operations and Dynamics 365 Business Central restrict modifying data in such records.

If you store personal data in business transaction records, the only way to correct, delete, or restrict processing of personal data to honor a data subject's request is to use the Dynamics 365 Business Central [customization capabilities](#). [The decision to honor a modification data subject request](#) and implementation thereof is your responsibility.

#### **Restricting the processing of customer data**

When you receive a request from a data subject to restrict processing of customer data, you can easily extract the affected customer data from the online service and store it in a separate container (that is, on-premise storage or separate web service with data isolation capabilities) isolated from the processing functions offered by any cloud application.

Alternative mechanism such as data processing block is offered by *Dynamics 365 Business Central*, where users are offered the ability to block specific data subject's record. For details, see [Restrict data processing for a data subject](#). When a record is marked as blocked, Dynamics 365 Business Central will discontinue processing the customer data of that data subject. You cannot create new transactions that use a blocked record; for example, you cannot create a new invoice for a customer, when either the customer or salesperson is blocked.

#### **Deleting customer data**

When a data subject asks you to delete their customer data, there are several ways to do so:

- Bulk editing multiple Dynamics 365 records, you can utilize the Microsoft Office add-in to export data to Microsoft Excel, make your changes, and then import that modified data from Excel back into the online service.

- You can delete customer data stored in any field by locating the data you want to delete and then manually deleting the data element containing the target customer data, for example like employing a hard delete on the contact record representing the data subject and other records that contain personal data

Additionally, For Dynamics 365 Marketing, deletion of a contact will assure that interaction data with personal information will be removed as well. For any custom fields or entities, you must customize your system to make sure it deletes all customer data from related records and/or unlinks them from the contact record so that all personal information is removed. More information: [Developer Guide \(Marketing\)](#).

*Dynamics 365 Customer Service Insights* also provides organizations with capabilities to [delete customer data](#).

Alternatively, in *Dynamics 365 for Finance and Operations* you may use [customization tools](#) to erase/modify customer data.

In *Dynamics 365 Business Central*, when a data subject asks you to delete their personal data that happens to be included in your customer data, there are several ways to address this request:

- To quickly bulk-edit multiple Business Central records, you can export data to Excel using the [Business Central Excel Add-in](#) to delete multiple records, and then publish these changes from Excel back in Business Central. For details, see [Exporting your Business Data to Excel](#).
- You can delete customer data stored in any field by manually deleting the data element containing the target customer data. For details, see [Entering data](#).
- You can directly delete customer data, for example by deleting a contact and then running the Delete Canceled Interaction Log Entries batch job to delete interactions for that contact.
- You can [delete documents](#) containing customer data—for example, memos and posted sales and purchase invoices.

Besides bulk or individual deletion of discrete records, please note that only terminated workers can be fully deleted from *Dynamics 365 for Talent*. [Follow these steps to delete terminated workers](#).

### Exporting customer data

To respond to a data portability request, customer data in *Dynamics 365 for Customer Engagement* can be exported using the comprehensive entity export capabilities. Customer data can be exported to a static Excel file to facilitate a data portability request. Using Excel, you can then edit the personal data to be included in the portability request and then save as a commonly used, machine-readable format such as .csv or .xml.

Additionally, for Dynamics 365 for Marketing a [dedicated API](#) is provided that allows customer to build extensions that retrieve additional records of captured customer interactions that may contain personal data. The API loads all the relevant information from the back-end system and assembles it into a single, portable document.

For *Dynamics 365 Customer Service Insights*, you [export customer data](#) through the Azure management portal.

*Dynamics 365 for Finance and Operations* offers [Data management and integration entities that enables provided entities, newly created entities, or extended entities for a repeatable personal data export to Excel or a number of other common formats using [Data import and export jobs](#). Alternatively, many lists can be exported to a static Excel file to facilitate a data portability request. When customer data is exported to Excel in this fashion, you can then edit the personal data to be included in the portability request and then save the file as a commonly used, machine-readable format such as .csv or .xml.

Both Dynamics 365 for Finance and Operations and *Dynamics 365 for Talent* offer Person Search Report to provide the data subject with data that you've classified as personal data.

*Dynamics 365 Business Central* offers the following features:

- You can export customer data to an Excel file. In Excel, you can then edit the customer data to be included in the portability request, and save it in a commonly used, machine-readable format, such as .csv or .xml. For details, see [Exporting your business data to Excel](#).
- You can export customer data to an Excel file. In Excel, you can then edit the customer data to be included in the portability request, and save it in a commonly used, machine-readable format, such as .csv or .xml. For details, see [Exporting your business data to Excel](#).

## Part 2: Responding to DSRs for system-generated logs

Microsoft also provides you with the ability to access, export, and delete system-generated logs that may be deemed personal under the GDPR's broad definition of "personal data." Examples of system-generated logs that may be deemed personal under GDPR include:

- Product and service usage data such as user activity logs
- User search requests and query data
- Data generated by product and services as a product of system functionality and interaction by users or other systems

The ability to restrict or rectify data in system-generated logs is not supported. Data in system-generated logs constitutes factual actions conducted within the Microsoft cloud and diagnostic data, and modifications to such data would compromise the historical record of actions and increase fraud and security risks.

### Accessing and exporting system-generated logs

Admins can access system-generated logs associated with a particular user's use of Dynamics 365 services and applications. To access and export system-generated logs:

1. Go to the [Microsoft Service Trust Portal](#) and sign in using the credentials of a Dynamics 365 global administrator.
2. In the **Privacy** drop-down list at the top of the page, click **Data Subject Request**.
3. On the **Data Subject Request** page, under **System-Generated Logs**, click **Data Log Export**.

#### NOTE

The **Data Log Export** is displayed. Note that a list of export data requests submitted by your organization is displayed.

4. To create a new request for a user, click **Create Export Data Request**.

After you create a new request, it will be listed on the **Data Log Export** page where you can track its status. After a request is complete, you can click a link to access the system-generated logs, which will be exported to your organization's Azure Storage location within 30 days of creating the request. The data will be saved in common, machine-readable file formats such as JSON or XML. If you don't have an Azure account and Azure Storage location, you'll need to create an Azure account and/or Azure Storage location for your organization so that the Data Log Export tool can export the system-generated logs.

Azure supports this request by enabling your organization to export the data in the native JSON format, to your specified Azure Storage Container. [Introduction to Microsoft Azure Storage—Blob storage](#) article. The data retrieved will not include data that may compromise the security and stability of the service.

#### IMPORTANT

You must be a tenant administrator to export user data from the tenant.

The following table summarizes accessing and exporting system-generated logs:

QUESTION	ANSWER
How long does the Microsoft Data Log Export tool take to complete a request?	This can depend on several factors. In most cases it should complete in one or two days, but it can take up to 30 days.
What format will the output be in?	The output will be structured machine-readable files such as XML, CSV, or JSON.
What data does the Data Log Export tool return?	The Data Log Export tool returns system-generated logs that Microsoft stores. Exported data will span across various Microsoft services including Office 365, Azure, and Dynamics.
*Who has access to Data Log Export tool to submit access requests for system-generated logs?	Dynamics 365 global administrators will have access to the GDPR Log Manager utility.
How is data returned to the user?	Data will be exported to your organization's Azure Storage location; it will be up to admins in your organization to determine how they will show/return this data to users.
What will data in system-generated logs look like?	Example of a system-generated log record in JSON format:  <pre>"DateTime": "2017-04-28T12:09:29-07:00", "AppName": "SharePoint", &gt;Action": "OpenFile", "IP": "154.192.13.131", "DevicePlatform": "Windows 1.0.1607"</pre>

### Deleting system-generated logs

To delete system-generated logs retrieved through an access request, you must remove the user from the service and permanently delete their Azure Active Directory account. For instructions on how to permanently delete a user, see the [Step 5: Delete](#) section in the Azure Data Subject Requests topic. It's important to note that permanently deleting a user account is irreversible once initiated. Permanently deleting a user account removes the user's data from system-generated logs, except for data that may compromise the security or stability of the service, for nearly all Dynamics 365 services within 30 days.

## Learn more

- [Microsoft Trust Center](#)

# Intune Data Subject Requests for the GDPR and CCPA

2/5/2021 • 10 minutes to read • [Edit Online](#)

The European Union [General Data Protection Regulation \(GDPR\)](#) gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of personal data, requesting corrections to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request* or DSR.

Similarly, the California Consumer Privacy Act (CCPA), provides privacy rights and obligations to California consumers, including rights similar to GDPR's Data Subject Rights, such as the right to delete, access, and receive (portability) their personal information. The CCPA also provides for certain disclosures, protections against discrimination when electing exercise rights, and "opt-out/ opt-in" requirements for certain data transfers classified as "sales". Sales are broadly defined to include the sharing of data for a valuable consideration. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

The guide discusses how to use Microsoft products, services, and administrative tools to help our controller customers find and act on personal data to respond to DSRs. Specifically, this guidance includes how to find, access, and act on personal data or personal information that reside in the Microsoft cloud. Here's a quick overview of the processes outlined in this guide:

- **Discover:** Use search and discovery tools to more easily find customer data that may be the subject of a DSR. Once potentially responsive documents are collected, you can perform one or more of the DSR actions described in the following steps to respond to the request. Alternatively, you may determine that the request doesn't meet your organization's guidelines for responding to DSRs.
- **Access:** Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it that can be available to the data subject.
- **Rectify:** Make changes or implement other requested actions on the personal data, where applicable.
- **Restrict:** Restrict the processing of personal data, either by removing licenses for various Azure services or turning off the desired services where possible. You can also remove data from the Microsoft cloud and retain it on-premises or at another location.
- **Delete:** Permanently remove personal data that resided in the Microsoft cloud.
- **Export/Receive (Portability):** Provide an electronic copy (in a machine-readable format) of personal data or personal information to the data subject. Personal information under the CCPA is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. The defined term "personal information" roughly aligns with "personal data" under GDPR. However, the CCPA also includes family and household data. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

Each section in this guide outlines the technical procedures that a data controller organization can take to respond to a DSR for personal data in the Microsoft cloud.

## Terminology

The following list provides definitions of terms that are relevant to this guide.



- **Controller:** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller, or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Personal data and data subject:** Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- **Processor:** A natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller.
- **Customer Data:** All data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, a customer through use of the enterprise service. Customer Data includes both (1) identifiable information of end users (for example, user names and contact information in Azure Active Directory) and Customer Content that a customer uploads into or creates in specific services (for example, customer content in an Azure Storage account, customer content of an Azure SQL Database, or a customer's virtual machine image in Azure Virtual Machines).
- **System-Generated Logs:** Logs and related data generated by Microsoft that help Microsoft provide enterprise services to users. System-generated logs contain primarily pseudonymized data, such as unique identifiers—typically a number generated by the system that cannot on its own identify an individual person but is used to deliver the enterprise services to users. System-generated logs may also contain identifiable information about end users, such as a user name.

#### How to use this guide

This guide consists of two parts:

- **Part 1: Responding to Data Subject Requests for Customer Data:** Part 1 of this guide discusses how to access, rectify, restrict, delete, and export data from applications in which you have authored data. This section details how to execute DSRs against both Customer Content and also identifiable information of end users.
- **Part 2: Responding to Data Subject Requests for System-Generated Logs:** When you use Microsoft's enterprise services, Microsoft generates some information, known as System-Generated Logs, in order to provide the service. Part 2 of this guide discusses how to access, delete, and export such information for Azure.

#### Understanding DSRs for Azure Active Directory and Microsoft Intune

When considering services provided to enterprise customers, execution of DSRs must always be understood within the context of a specific Azure Active Directory tenant. Notably, DSRs are always executed within a given Azure Active Directory tenant. If a user is participating in multiple tenants, it is important to emphasize that a given DSR is *only* executed within the context of the specific tenant the request was received within. This context is critical to understand as it means the execution of a DSR by one enterprise customer **will not** impact the data of an adjacent enterprise customer.

The same also applies for Microsoft Intune provided to an enterprise customer: execution of a DSR against an Intune account *associated with an Azure Active Directory tenant* **will only** pertain to data within the tenant. In addition, it is important to understand the following when handling Intune accounts within a tenant:

- If an Intune user creates an Azure subscription, the subscription will be handled as if it were an Azure Active Directory tenant. Consequently, DSRs are scoped within the tenant as described previously.
- If an Azure subscription created via an Intune account is deleted, **it will not affect** the actual Intune account. Again, as noted previously, DSRs executing within the Azure subscription are limited to the scope of the tenant itself.

DSRs against an Intune account itself, **outside a given tenant**, are executed via the Consumer Privacy

Dashboard. Refer to the Windows Data Subject Request Guide for further details.

## Part 1: DSR Guide for Customer Data

### Executing DSRs against Customer Data

Microsoft provides the ability to access, delete, and export certain Customer Data through the Azure portal and also directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services (also referred to as *in-product experiences*). Details regarding such in-product experiences are described in the respective services' reference documentation.

#### IMPORTANT

Services supporting in-product DSRs require direct usage of the service's application programming interface (API) or user interface (UI), describing applicable CRUD (create, read, update, delete) operations. Consequently, execution of DSRs within a given service must be done in addition to execution of a DSR within the Azure Portal in order to complete a full request for a given data subject. Please refer to specific services' reference documentation for further details.

### Step 1: Discover

The first step in responding to a DSR is to find the personal data that is the subject of the request. This first step - finding and reviewing the personal data at issue - will help you determine whether a DSR meets your organization's requirements for honoring or declining a DSR. For example, after finding and reviewing the personal data at issue, you may determine the request doesn't meet your organization's requirements because doing so may adversely affect the rights and freedoms of others.

After you find the data, you can then perform the specific action to satisfy the request by the data subject. For details, see the following resources:

- [Data collection](#)
- [Data storage and processing](#)
- [View personal data](#)

### Step 2: Access

After you've found Customer Data containing personal data that is potentially responsive to a DSR, it is up to you and your organization to decide which data to provide to the data subject. You can provide them with a copy of the actual document, an appropriately redacted version, or a screenshot of the portions you have deemed appropriate to share. For each of these responses to an access request, you will have to retrieve a copy of the document or other item that contains the responsive data.

When providing a copy to the data subject, you may have to remove or redact personal information about other data subjects and any confidential information.

The following explains how to get a copy of data in response to a DSR access request.

#### Azure Active Directory

Microsoft offers both a portal and in-product experiences providing the enterprise customer's tenant administrator the capability to manage DSR access requests. DSR Access requests allow for access of the personal data of the user, including: (a) identifiable information about an end user and (b) system-generated logs.

#### Service-Specific Interfaces

Microsoft Intune provides the ability to [discover Customer Data](#) directly via user interfaces (UIs) or pre-existing application programming interfaces (APIs).

### Step 3: Rectify

If a data subject has asked you to rectify the personal data that resides in your organization's data, you and your

organization will have to determine whether it's appropriate to honor the request. Rectifying the data may include taking actions such as editing, redacting, or removing personal data from a document or other type of item.

As a data processor, Microsoft does not offer the ability to correct system-generated logs as it reflects factual activities and constitutes a historical record of events within Microsoft services. With respect to Intune, admins can't update device or app-specific information. If an end user wants to correct any personal data (like the device name), they must do so directly on their device. Such changes are synchronized the next time they connect to Intune.

#### **Step 4: Restrict**

Data subjects may request that you restrict processing of their personal data. We provide both the Azure portal and pre-existing application programming interfaces (APIs) or user interfaces (UIs). These experiences provide the enterprise customer's tenant administrator the capability to manage such DSRs through a combination of data export and data deletion. For details, see [Processing personal data](#).

#### **Step 5: Delete**

The "right to erasure" by the removal of personal data from an organization's Customer Data is a key protection in the GDPR. Removing personal data includes removing all personal data and system-generated logs, except audit log information. For details, see [Delete end user personal data](#).

## Part 2: System-Generated Logs

Audit logs provide tenant admins with a record of activities that generate a change in Microsoft Intune. Audit logs are available for many manage activities and typically create, update (edit), delete, and assign actions. Remote tasks that generate audit events can also be reviewed. These audit logs may contain personal data from users whose devices are enrolled in Intune. Admins can't delete audit logs. For details, see [Audit personal data](#).

## Notify about exporting or deleting issues

If you run into issues while exporting or deleting data from the Azure portal, go to the Azure portal **Help + Support** blade and submit a new ticket under **Subscription Management > Other Security and Compliance Request > Privacy Blade and GDPR Requests**.

## Learn more

- [Microsoft Trust Center](#)

# Microsoft Support and Professional Services Data Subject Requests for the GDPR and CCPA

2/5/2021 • 22 minutes to read • [Edit Online](#)

## Introduction to Microsoft Professional Services

Microsoft Professional Services includes a diverse group of technical architects, engineers, consultants, and support professionals dedicated to delivering on the Microsoft mission of enabling customers to do more and achieve more. Our Professional Services team includes more than 21,000+ total consultants, Digital Advisors, Premier Support, engineers, and sales professionals working across 191 countries, supporting 46 different languages, managing several million engagements per month, and engaging in customer and partner interactions through on-premises, phone, web, community, and automated tools. The organization brings broad expertise across the Microsoft portfolio, using an extensive network of partners, technical communities, tools, diagnostics, and channels that connect us with our enterprise customers.

Find out more about Microsoft Professional Services by going to the [Microsoft Professional Services Security Documentation webpage](#). Microsoft Professional Services takes its obligations under the General Data Protection Regulation (GDPR) seriously. The information in this document is designed to answer customer questions about how Microsoft's support and consulting offerings will respond to and assist customers in responding to Data Subject Request (DSR) obligations under GDPR.

### Introduction to DSRs

The GDPR gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, and deleting it. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request* or DSR. Additionally, it obligates companies working on behalf of a controller (known as the *data processor* or just *processor*) to reasonably assist the controller in fulfilling DSRs.

Similarly, the California Consumer Privacy Act (CCPA), provides privacy rights and obligations to California consumers, including rights similar to GDPR's Data Subject Rights, such as the right to delete, access, and receive (portability) their personal information. The CCPA also provides for certain disclosures, protections against discrimination when electing exercise rights, and "opt-out/ opt-in" requirements for certain data transfers classified as "sales". Sales are broadly defined to include the sharing of data for a valuable consideration. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

This guide discusses how to find, access, and act on personal data that resides in Microsoft IT systems that may have been collected to provide Support and other Professional Services offerings.

In developing a response for DSRs, it is important for Microsoft's customers to understand that Support and Consulting Data is separate from Customer Data in the Online Services or other data that they or their data subjects may have provided to Microsoft. Tools and processes provided for Online Services, the Microsoft Privacy Dashboard, or other Microsoft systems for responding to DSRs cannot be used to respond to DSRs for personal data held by Microsoft Support or other Professional Services.

All requests must be made through a support representative, as described later in this article. Currently there is no self-serve tool for customers to gain access to personal data within the Professional Services organizations.

## Overview of the processes outlined in this guide

- **Discover:** Use search and discovery tools to more easily find customer data that may be the subject of a DSR. Once potentially responsive documents are collected, you can perform one or more of the DSR actions described in the following steps to respond to the request. Alternatively, you may determine that the request doesn't meet your organization's guidelines for responding to DSRs.
- **Access:** Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it that can be available to the data subject.
- **Rectify:** Make changes or implement other requested actions on the personal data, where applicable.
- **Restrict:** Restrict the processing of personal data, either by removing licenses for various Azure services or turning off the desired services where possible. You can also remove data from the Microsoft cloud and retain it on-premises or at another location.
- **Delete:** Permanently remove personal data that resided in the Microsoft cloud.
- **Export/Receive (Portability):** Provide an electronic copy (in a machine-readable format) of personal data or personal information to the data subject. Personal information under the CCPA is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. The defined term "personal information" roughly aligns with "personal data" under GDPR. However, the CCPA also includes family and household data. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

## Terminology

Below are the relevant definitions of terms from the GDPR for this guide:

- **Controller:** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller, or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Personal data and data subject:** Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- **Processor:** A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

## Additional terms and definitions that may be helpful in understanding this guide

- **Support and Consulting Data:** All data, including all text, sound, video, image files, or software, that are provided to Microsoft by, or on behalf of, Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain Support or Professional Services. To clarify, this does not include data collected where Microsoft is the data controller including Customer Contact Data.
- **Customer Contact:** Personal data that may be part of your business relationship with Microsoft, such as personal data contained within your customer contact information. This may include your name, e-mail, or phone number of the Premier Contract Service Manager (CSM), the Global or IT Administrator for an Online Service, or similar roles.
- **Pseudonymized Data:** When you use Microsoft support for Microsoft's enterprise products and services, Microsoft generates some information linked to a Microsoft numeric identifier to provide the support. This information is often referred to as "Pseudonymized Data", although this data cannot be attributed to a specific data subject without the use of additional information, some of it may be deemed personal under GDPR's broad definition for personal data. Within Professional Services, requests to fulfill or assist in fulfilling DSRs will always automatically include addressing pseudonymized data.

## How to use this guide

This guide covers four scenarios a customer may encounter if they have utilized Microsoft Professional Services.

- **DSR for a Customer Contact Engaging Microsoft:** Explanation for how Microsoft will respond to requests from a customer contact or IT administrator to exercise their data subject rights.
- **DSR for an End-User Engaging Microsoft:** Explanation for how Microsoft will respond to requests from a customer's employees or other data subjects to exercise their rights.
- **DSR for Customer Provided Data: Commercial Support:** Explanation for how to receive assistance from Microsoft when a customer has received a request from their employee or other data subjects to exercise their rights, and that data subject's personal data was collected by Microsoft Support during a support engagement.
- **DSR for Customer Provided Data: Consulting Services including FastTrack Migration Services:** Explanation for how to receive assistance from Microsoft when a customer has received a request from their employee or other data subjects to exercise their rights, and that data subject's personal data was collected by Microsoft during a consulting engagement.

## DSR for a Customer Contact Engaging Microsoft

*How Microsoft responds to requests by a customer contact or IT admin to exercise their data subject rights.*

When a customer engages with Microsoft to receive support or consulting services, Microsoft Support automatically collects or retrieves from account records the personal data of the Customer Contact (for example, Premier CSM, Global Admin, IT Admin). This likely includes the name, email, phone, and other personal data of the individual seeking support or consulting services.

The Customer Contact's personal data is part of Microsoft's business relationship with the customer, and Microsoft is the Data Controller, except when this data is collected in the course of providing technical support. Microsoft will respond to DSRs from the Customer Contact around their personal data, regardless of whether they are still with the organization.

When the Customer Contact's Personal Data is collected in the course of providing technical support, Microsoft is the Data Processor.

Customers should understand that the DSR only covers the personal data of the Customer Contact, and no changes or deletions will be made to any of the customer's data submitted as part of engagements (for example, transcripts, case descriptions, files, work product), since Microsoft is the data processor. Additionally, to maintain the engagement's historical record no changes at all will be made to closed engagements, including the record of who opened an engagement.

Upon receiving an inquiry from a Customer Contact regarding a DSR where Microsoft is the Data Controller, Microsoft personnel will refer a customer contact to the [Privacy Response Center](#). This is Microsoft's primary input mechanism for privacy inquiries and complaints. Upon receiving an inquiry, the Privacy Response Center will identify that this is part of a commercial or organizational account and respond accordingly.

Where Microsoft is the Data Processor, please see **DSR for Customer Provided Data: Commercial Support** below.

To maintain customer's business continuity, Microsoft will also not process a DSR associated with an engagement until a replacement contact is confirmed. Upon confirmation of a new contact, Microsoft will swap out the old contact with the new one in open engagements.

Customers may choose to make changes to their data collected during Professional Services engagements through normal support or consulting channels, separate from this DSR. For instance, Microsoft can assist in expunging support engagements, on request (see in the *DSR Guide for Customer Provided Data* section).

*Example for Illustration Purposes Only*

John is a Project Manager for an O365 enterprise customer, with one open Consulting engagement and two closed engagements. Now John is leaving his company and wants his data deleted. John contacts the Privacy

Response Center, who identifies him as the Project Manager. John is informed his name cannot be deleted from the prior (closed) engagements or from any data within the open engagements. However, the Privacy Response Center will replace John as the contact on the current open engagement if he will identify a replacement contact. John lets Microsoft know that Jane will be his replacement contact, and Microsoft makes the change across all systems.

## DSR for an End-User Engaging Microsoft

*How Microsoft responds to requests from a customer's employees or other data subjects to exercise their rights.*

If a customer's employee or other data subject contacts Microsoft to exercise their rights over data that Microsoft has collected as the data processor, then that data subject will be informed that they need to contact Microsoft's customer, as the data controller, to exercise those rights. Microsoft will take no further action.

If the data subject has also contacted Microsoft about exercising their rights for data Microsoft has collected in situations where Microsoft is the data controller (for example, consumer support, commercial customer contact) then Microsoft will separately respond to the individual's data subject right request for that personal data.

*Example for Illustration Purposes Only*

Jane is an employee of an Enterprise customer, Contoso, that has given her a Dynamics 365 account. She contacts Microsoft to have all her data deleted and is referred to the Privacy Response Center. Jane fills out the request form. The Privacy Response Center identifies her as an enterprise end user and lets her know she needs to work through Contoso for the deletion of her enterprise data. They also identify her as a Microsoft X-Box user and delete her data out of her consumer Microsoft account.

## DSR for Customer Provided Data: Commercial Support

*How to receive assistance from Microsoft when a customer has received a request from their employee or other data subjects to exercise their rights, and that data subject's personal data was collected by Microsoft Support during a support engagement.*

When a customer engages with Microsoft Support, Microsoft collects Support Data from the customer to resolve any issues that required a support engagement. This Support Data includes Microsoft's interaction with the customer (for example, chat, phone, email, web submission) plus any content files the customer sends to Microsoft or Microsoft has, with customer's permission, extracted from the customer's IT environment or Online Services tenancy to resolve the support issue. In the case of Premier support, this would also include any data we collect from you to proactively prevent future issues. However, this excludes other information from Microsoft's business relationship with the customer (for example, billing records).

For all Support Data and Contact Data collected in the course of providing support, Microsoft is the data processor. As such, Microsoft's will not respond to direct requests from data subjects regarding Support Data provided when they were associated with a Microsoft commercial customer. Microsoft will work with the customer through their normal support channels to assist them in responding to DSRs.

### Step 1: Discover

The first step in obtaining Microsoft's assistance in responding to a DSR is to find the personal data that is the subject of the DSR. This first step—finding and reviewing the personal data at issue—will help a customer determine whether a DSR meets the organization's policies for honoring a data subject request.

After the customer finds the data, the customer can then perform the specific action to satisfy the request by the data subject. Depending on what the customer is trying to do will determine what level of discovery the customer needs to engage in.

Where Microsoft assists a customer with the resolution of a DSR then this is a business function, and the request

is made through your regular support channel and not through a request to the Privacy Response Center.

In discovering relevant data and obtaining Microsoft's assistance, a customer has several options for how to approach the DSR:

*Option A: Cross-Microsoft Support Customer DSR.* Apply the DSR to all the customer's support data across Microsoft's support environment. To do this, a customer can just ask Microsoft to apply the DSR to all Support Data collected.

*Option B: Specific Customer Engagements.* Use online systems to review tickets, then identify specific engagements containing the relevant personal data and report them Microsoft. Microsoft will attempt to provide assistance to perform a search if the customer does not have the ability to search across engagements (tickets).

*Once engagements are identified, request to apply the DSR to either a specific part of the record or everything related to that engagement across Microsoft.*

To identify specific engagements, customers need to search across their engagements. For Premier customers, the Contract Service Manager ("CSM") for a customer has visibility across all Support Requests (SRs) that are created under that Contract Schedule. For Non-Premier, equivalent support engagement portals are available, such as through Online Services support areas.

The CSM can go to the portal at [Services Hub](#) and select manage all Support Requests.

#### **IMPORTANT**

In addition to the case history in Services Hub, customers may also have personal data of an end user in files that was collected by Microsoft (or, with customer's permission, removed from the Online Service) during a support engagement. Examples may include copies of customer's exchange mailboxes, Azure VMs, or databases. This personal data may or may not be mentioned in the case history (i.e. ticket) for a particular engagement. To review that data, the Customer Contact must be a specific authenticated (via AAD or MSA) Support Request contact that has received a URL for a workspace in Microsoft Support Data Transfer and Management tool (DTM). A Customer Contact will have access to the files, but no global view is available, and Services Hub will not indicate if files exist.

Once customers have identified all the relevant data in the selected support tickets, customers can decide whether to request the deletion of everything related to a ticket or selectively apply the DSR to individual instances of personal data.

## Step 2: Access

After a customer has found Support Data containing personal data that is potentially responsive to a DSR, it is up to the customer to decide which personal data to include in the response. For example, the customer may choose to remove personal data about other data subjects and any confidential information.

Response to the DSR may include a copy of the actual document, an appropriately redacted version, or a screenshot of the portions the customer has deemed appropriate to share. For each of these responses to an access request, the customer will have to retrieve a copy of the document or other item that contains the responsive data.

Access to the personal data of an end user may be from a mention or notation in the various types of content documentation. Since customers may access the engagement ticket and the content, they can provide a summary of personal data themselves without further assistance from Microsoft.

In rare cases, customer may have need to obtain copies of support interaction data (for example, emails, transcribed copies of phone recordings; chat transcripts) between a Microsoft Representative and the Customer's Representative. To the extent required, Microsoft may provide redacted copies of these transcripts



based on need, sensitivity, and difficulty.

## Step 3: Rectify

If a data subject has asked the customer to rectify the personal data that resides in their organization's Support Data, the customer will have to determine whether it's appropriate to honor the request. If the customer chooses to honor the request, then the customer may request that Microsoft make the change. Microsoft may rectify data or may delete customer's data from the support systems and request that the customer resubmit it to Microsoft in corrected format.

## Step 4: Restrict

The customer may at any time close an engagement or contact Microsoft and request the engagement be closed. A closed engagement will prevent any work from being performed.

For extra assurance, customer may contact Microsoft and request that a note be placed in the engagement ticketing system instructing that the case should not be re-opened for any reason absent the customer's permission.

Note: Engagements (tickets) will also be deleted according on a retention and deletion schedule, based on the sensitivity of data, service, and system. If customer requires a copy of data, they should ensure that they have extracted data prior to deletion.

## Step 5: Delete

The "right to erasure" by the removal of personal data from an organization's Support Data is a key protection in the GDPR. Removing personal data includes deleting entire engagements, documents, or files or deleting specific data within an engagement, document, or file.

As a customer investigates or prepares to delete personal data in response to a DSR, here are a few important things to understand about how deletion works for Microsoft Support.

All data at Microsoft has a retention and deletion policy applied to it, which will vary depending on risk and other factors.

Customers requesting the deletion of a data subject's personal data universally across Support systems may do so through your TAM or by filing a Support Request (SR) in Services Hub or equivalent system. You *must* indicate that this is a request to assist with a DSR under GDPR.

*Option A: Cross-Microsoft Support Customer DSR.* For a cross system DSR, customer must provide the personal data that Microsoft needs to identify the required data (for example, email address; phone number). Microsoft will not correlate or research records and will only search directly on identifiers provided by the customer. When data is found, Microsoft will delete all engagements and all associated data.

Important Note: this may result in loss of historical records that are important to customer's organization.

*Option B: Specific Customer Engagements.* For specific engagements that the customer has identified and wants deleted, do not delete tickets out of Services Hub. This will result in personal data remaining in logs and downstream systems that may not be deleted within the needed timeframe. Instead, identify the ticket or personal data within the ticket that must be deleted, and contact Microsoft Support to assist you in deleting that data.

### **Microsoft Support Data Transfer and Management tool (DTM) instructions**

For all these searches, Microsoft will not search across DTM due to the potential sensitivity of content in files. However, if the customer desires, Microsoft will delete all files contained in DTM associated with the customer's

account. Due to the potential for serious customer impact, Microsoft requires a separate request from customer specifying the deletion of DTM files.

- For open cases, the Customer Contact can go into DTM and delete files.
- For cases closed less than 90 days, a request must be made to a TAM or in an SR to have the files removed.
- For cases closed after than 90 days, files have already been automatically deleted.
- Even if the personal data was only located within a file that has been deleted, customers must still have Microsoft run a check across systems for the personal data as some data may have been removed from DTM in the course of providing support.

## Step 6: Export

The "right of data portability" allows a data subject to request a copy of their personal data in an electronic format and request that your organization transmit it to another controller. In the case of Support Data, any usable information that Microsoft has would be in the form of engagement information or files that can be returned to you for re-communication or uploading to another controller.

Note: Exported data may not include Microsoft's intellectual property or any data that may compromise the security or stability of the service.

### *Example for Illustration Purposes Only*

John is a Premier CSM for an Enterprise customer, Contoso, that uses O365 for its employee e-mail and Azure to host a Contoso SQL Database. Contoso has multiple open and closed tickets. Recently, Microsoft Support, with Contoso's permission, moved a copy of the SQL Database into DTM for support and troubleshooting.

John receives a DSR from Jane asking that all her data be deleted. John goes into Services Hub and searches across engagements to identify that Jane had email account issues and so was referenced in two tickets by name and email address. He contacts his TAM, provides the TAM with Jane's name and e-mail address as an identifier, and requests that those two tickets be deleted, along with all downstream data that may have been generated out of those tickets.

He also suspects he was engaged in a chat conversation with support personnel where he mentions Jane, so he requests that chat log to be deleted.

He also knows that Jane's personal data is in the SQL Database. Since the SQL VM was moved into DTM less than 90 days ago, he asks his TAM separately to assist in the immediate deletion of the database out of DTM.

Lastly, since he knows that data may have been removed from the DTM file while providing support, he asks Microsoft to run a check across IT systems for Jane's personal data from the SQL Database.

Microsoft Support performs all these deletions and, based on customer request, the TAM provides him with an attestation statement that the required data has been deleted.

## DSR Guide for Customer Provided Data in Consulting Services including Migration Services

*How to receive assistance from Microsoft when a customer has received a request from their employee or other data subjects to exercise their rights, and that data subject's personal data was collected by Microsoft during a consulting engagement.*

## Microsoft Consulting Services

For Microsoft Consulting Services engagements contracted where the Microsoft Professional Services Data Protection Addendum (<https://aka.ms/professionalservicesdpa>) applies.

Microsoft is the data controller for Customer Contacts working with the engagement team. Those individuals should contact the [Privacy Response Center](#) to fulfill data subject rights.

Microsoft is the data processor for a DSR located within data provided during a consulting engagement. The customer should contact the engagement manager to build in a plan to assist in responding to a DSR based on the data collected and then specific type of consulting services provided. To the extent your request constitutes a level of effort typically seen within a Microsoft Consulting Services engagement, there may be an additional work order required. Additionally, personal data will be deleted after each consulting engagement within a timeframe dependent on the type of consulting engagement. Customer can request data to be deleted sooner and request an attestation of deletion.

## Microsoft FastTrack Services

[Microsoft FastTrack](#) provides IT consulting services to organizations to help them onboard and use Microsoft cloud services such as Microsoft 365, Azure, and Dynamics 365.

Microsoft is the data controller for Customer Contacts working with the FastTrack team. If Customer Contacts wish to access, revise or remove contact information from Microsoft's FastTrack records, customers can have the data subject send the request directly to Office 365 FastTrack GDPR Request inbox

<[o365ftgdpr@microsoft.com](mailto:o365ftgdpr@microsoft.com)>.

For FastTrack migration services, Microsoft is the data processor. In accordance with our Fast Track additional privacy disclosure statement, all data in migration is considered "migration data." If you need to execute DSRs while your organization is engaged in a FastTrack migration project, special care is required.

If you need to process any access, rectify, or export DSR requests while a user's data is being processed through FastTrack migration systems, it will be the customer's responsibility to fulfill such DSRs through your existing source systems in which the user data is stored. Once the user's migration is complete and the data has been migrated to the destination Microsoft cloud service, the guidance provided by Microsoft on how customers can use Microsoft products, services, and administrative tools to find and act on personal data to respond to data subject request will then apply. To view this guidance see [Data Subject Requests for the GDPR](#).

If you need to delete a user account in response to a DSR delete request while your organization is engaged in an ongoing FastTrack migration project, you should be aware that migration systems may retain a copy of user migration data for a period of time following completion of the user's migration and deleting the user account will not automatically delete such user migration data stored in FastTrack migration systems. If you would like the Microsoft FastTrack team to delete user migration data, you can [submit a request](#). In the ordinary course of business, Microsoft FastTrack will delete all data copies once your organization's migration is complete.

## Other Consulting Services

Customer receiving other Professional Services through Microsoft should work through the engagement team for fulfillment of all GDPR requirements. If the engagement team is not able to provide clear instructions on GDPR DSR fulfillment, customers may contact the [Privacy Response Center](#) for assistance.

# Office 365 Data Subject Requests for the GDPR and CCPA

2/5/2021 • 130 minutes to read • [Edit Online](#)

## Introduction to DSRs

The European Union [General Data Protection Regulation \(GDPR\)](#) gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request* or DSR. The controller is obligated to promptly consider each DSR and provide a substantive response either by taking the requested action or by providing an explanation for why the DSR cannot be accommodated by the controller. A controller should consult with its own legal or compliance advisers regarding the proper disposition of any given DSR.

Similarly, the California Consumer Privacy Act (CCPA), provides privacy rights and obligations to California consumers, including rights similar to GDPR's Data Subject Rights, such as the right to delete, access, and receive (portability) their personal information. The CCPA also provides for certain disclosures, protections against discrimination when electing exercise rights, and "opt-out/ opt-in" requirements for certain data transfers classified as "sales". Sales are broadly defined to include the sharing of data for a valuable consideration. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

The guide discusses how to use Office 365 products, services, and administrative tools to help you find and act on personal data or personal information to respond to DSRs. Specifically, this includes how to find, access, and act on personal data or personal information that resides in Microsoft's cloud. Here's a quick overview of the processes outlined in this guide:

- **Discover:** Use search and discovery tools to more easily find customer data that may be the subject of a DSR. Once potentially responsive documents are collected, you can perform one or more of the DSR actions described in the following steps to respond to the request. Alternatively, you may determine that the request doesn't meet your organization's guidelines for responding to DSRs.
- **Access:** Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it that can be available to the data subject.
- **Rectify:** Make changes or implement other requested actions on the personal data, where applicable.
- **Restrict:** Restrict the processing of personal data, either by removing licenses for various Microsoft cloud services or turning off the desired services where possible. You can also remove data from the Microsoft cloud and retain it on-premises or at another location.
- **Delete:** Permanently remove personal data that resided in the Microsoft cloud.
- **Export/Receive (Portability):** Provide an electronic copy (in a machine-readable format) of personal data or personal information to the data subject. Personal information under the CCPA is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. The defined term "personal information" roughly lines up with "personal data" under GDPR. However, the CCPA also includes family and household data. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

## Terminology

Here are definitions of terms from the GDPR that are relevant to this guide.

- **Controller:** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller, or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Personal data and data subject:** Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- **Processor:** A natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller.
- **Customer Data:** All data, including all text, sound, video, or image files, and software, that is provided to Microsoft by, or on behalf of, a customer through use of the enterprise service. Customer Data includes both (1) identifiable information of end users (for example, user names and contact information in Azure Active Directory) and Customer Content that a customer uploads into or creates in specific services (for example, customer content in a Word or Excel document, or in the text of an Exchange Online email; customer content added to a SharePoint Online site, or saved to a OneDrive for Business account).
- **System-Generated Logs:** Logs and related data generated by Microsoft that help Microsoft provide enterprise services to users. System-generated logs contain primarily pseudonymized data, such as unique identifiers (typically a number generated by the system) cannot on its own identify an individual person but is used to deliver the enterprise services to users. System-generated logs may also contain identifiable information about end users, such as a user name.

## How to use this guide

To help you find information relevant to your use case, this guide is divided into four parts.

- **Part 1: Responding to DSRs for Customer Data:** *Customer Data* is data produced and stored in Office 365 in the day-to-day operations of running your business. Examples of the most commonly used Office 365 applications that allow you to author data include Word, Excel, PowerPoint, Outlook, and OneNote. Office 365 also consists of applications such as SharePoint Online, Teams, and Forms that allow you to better collaborate with others. Part 1 of this guide discusses how to discover access, rectify, restrict, delete, and export data from Office 365 applications that have been used to author and store data in Office 365 online services. It addresses products and services for which Microsoft is acting as a data processor to your organization, and thus DSR capability is made available to your tenant administrator.
- **Part 2: Responding to DSRs with Respect to Insights Generated by Office 365:** Office 365 provides certain insights through services like Delve, MyAnalytics, and Workplace Analytics. How these insights are generated and how to respond to DSRs related to them are explained in Part 2 of this guide.
- **Part 3: Responding to DSRs for system-generated Logs:** When you use Office 365 enterprise services, Microsoft generates some information such as service logs that record the use or performance of features in the online services. Most service-generated data contain pseudonymous identifiers generated by Microsoft and this category is thus generally referred to within this document as *system-generated logs*. Although this data can't be attributed to a specific data subject without the use of additional information, some of it may be deemed personal under GDPR's definition for "personal data." Part 3 of this guide discusses how to access, delete, and export system-generated logs.
- **Part 4: Additional resources to assist you with DSRs:** Part 4 of this guide lists limited scenarios in which Microsoft is the data controller when certain Office 365 products and services are used.

## NOTE

In most cases, when users in your organization use Microsoft Office 365 products and services, you are the data controller and Microsoft is the processor. As a data controller, you are responsible for responding to the data subject directly. To assist you with this, Parts 1-3 of this guide detail the technical capabilities available to your organization to respond to a DSR request. In some limited scenarios, however, Microsoft will be the data controller when people use certain Office 365 products and services. In these cases, the information in Part 4 provides guidance on how data subjects can submit DSR requests to Microsoft.

### Office 365 national clouds

The Microsoft Office 365 services are also available in the following national cloud environments: [Office 365 Germany](#), [Office 365 operated by 21Vianet \(China\)](#), and [Office 365 US Government](#). Most of the guidance for managing data subject requests described in this document applies to these national cloud environments. However, due to the isolated nature of these environments, there are some exceptions. Where notable for a given subsection, these exceptions are called out in a corresponding note.

### Hybrid deployments

Your organization may consist of Microsoft offerings that are a combination of cloud-based services and on-premises server products. In general, a hybrid deployment is typically the sharing of user accounts (identity management) and resources (such as mailboxes, web sites, and data) that exist in the cloud and on-premises. Common hybrid scenarios include:

- Exchange hybrid deployments, where some users have an on-premises mailbox and other users have Exchange Online mailboxes.
- SharePoint hybrid deployments, where site and file servers are on-premises and OneDrive for Business accounts are in Office 365.
- The on-premises identity management system (Active Directory) that is synchronized with Azure Activity Directory, which is the underlying directory service in Office 365.

When responding to a DSR request, you may have to determine if data that's responsive to a DSR request is in the Microsoft cloud or in your on-premise organization, and then take the appropriate steps to respond to that request. The Office 365 Data Subject Request Guide (this guide) provides guidance for responding to cloud-based data. For guidance for data in your on-premises organization, see [GDPR for Office on-premises Servers](#).

## Part 1: Responding to DSRs for Customer Data

The guidance for responding to DSRs for Customer Data is divided into the following four sections:

- [Using the Content Search eDiscovery tool to respond to DSRs](#)
- [Using In-App functionality to respond to DSRs](#)
- [Responding to DSR rectification requests](#)
- [Responding to DSR restriction requests](#)

### How to determine the Office 365 applications that may be in scope for a DSR for Customer Data

To help you determine where to search for personal data or what to search for, it helps to identify the Office 365 applications that people in your organization can use to create and store data in Office 365. Knowing this narrows the Office 365 applications that are in-scope for a DSR and helps you determine how to search for and access personal data that's related to a DSR. Specifically, this means whether you can use the Content Search tool or if you'll have to use the in-app functionality of the application the data was created in.

A quick way to identify the Office 365 applications that people in your organization are using to create Customer Data is to determine which applications are included in your organization's Microsoft 365 for business subscription. To do this, you can access user accounts in the Office 365 admin portal and look at the product

licensing information. See [Assign licenses to users](#).

## Using the Content Search eDiscovery tool to respond to DSRs

When looking for personal data within the larger set of data your organization creates and stores using in Office 365, you may want to first consider which applications people have most likely used to author the data you're looking for. Microsoft estimates that over 90% of an organization's data that is stored in Office 365 is authored in Word, Excel, PowerPoint, OneNote, and Outlook. Documents authored in these Office applications, even if purchased through Microsoft 365 Apps for enterprise or an Office perpetual license, are most likely stored on a SharePoint Online site, in a user's OneDrive for Business account, or in a user's Exchange Online mailbox. That means you can use the Content Search eDiscovery tool to search (and perform other DSR-related actions) across SharePoint Online sites, OneDrive for Business accounts, and Exchange Online mailboxes (including the sites and mailboxes associated with Microsoft 365 Groups, Microsoft Teams, EDU Assignments) to find documents and mailbox items that may be relevant to the DSR you're investigating. You can also use the Content Search tool to discover Customer Data authored in other Office 365 applications.

The following list identifies the Office 365 applications that people use to create Customer Authored Content and that can be discovered by using Content Search. This section of the DSR guide provides guidance about how to discover, access, export, and delete data created with these Office 365 applications.

Applications where Content Search can be used to find Customer Data:

- Calendar
- Excel
- Office Lens
- OneDrive for Business
- OneNote
- Outlook/Exchange
- People
- PowerPoint
- SharePoint
- Skype for Business
- Tasks
- Teams
- To Do
- Video
- Visio
- Word

### NOTE

The Content Search eDiscovery tool is not available in [Office 365 operated by 21Vianet \(China\)](#). This means you won't be able to use this tool to search for and export Customer Data in the Office 365 applications shown in Table 1. However, you can use the In-Place eDiscovery tool in Exchange Online to search for content in user mailboxes. You can also use the eDiscovery Center in SharePoint Online to search for content in SharePoint sites and OneDrive accounts. Alternatively, you can ask a document owner to help you find and make changes or deletions to content or export it if necessary. For more information, see:

- [Create an In-Place eDiscovery search](#)
- [Set up an eDiscovery Center in SharePoint Online](#)

## Using Content Search to find personal data

The first step in responding to a DSR is to find the personal data that is the subject of the DSR. This consists of using Office 365 eDiscovery tools to search for personal data (among all your organization's data in Office 365) or going directly to the native application in which the data was created. This first step, finding and reviewing the personal data at issue, will help you determine whether a DSR meets your organization's requirements for honoring or declining a data subject request. For example, after finding and reviewing the personal data at issue, you may determine the request doesn't meet your organization's requirements because doing so may adversely affect the rights and freedoms of others, or because the personal data is contained in a business record your organization has a legitimate business interest in retaining.

As previously stated, Microsoft estimates that over 90% of an organization's data is created with Office applications, such as Word and Excel. This means that you can use the Content Search in the Security & Compliance Center to search for most DSR-related data.

This guide assumes that you or the person searching for personal data that may be responsive to a DSR request is familiar with or has experience using the Content Search tool in the Security & Compliance Center. For general guidance on using Content Search, see [Content Search in Office 365](#). Be sure that the person running the searches has been assigned the necessary permissions in the Security & Compliance Center. This person should be added as a member of the eDiscovery Manager role group in the Security & Compliance Center; see [Assign eDiscovery permissions in the Security & Compliance Center](#). Consider adding other people in your organization who are involved in investigating DSRs to the eDiscovery Manager role group, so they can perform the necessary actions in the Content Search tool such as previewing and exporting search results. However, unless you set up compliance boundaries (as described [here](#)) be aware that an eDiscovery Manager can search all content locations in your organization, including ones that may not be related to a DSR investigation.

After you find the data, you can then perform the specific action to satisfy the request by the data subject.

#### NOTE

In Office 365 Germany, the Security & Compliance Center is located at <https://protection.office.de>.

#### Searching content locations

You can search the following types of content locations with the Content Search tool.

- Exchange Online mailboxes. This includes the mailboxes associated with Microsoft 365 Groups and Microsoft Teams
- Exchange Online public folders
- SharePoint Online sites. This includes the sites associated with Microsoft 365 Groups and Microsoft Teams
- OneDrive for Business accounts

#### NOTE

This guide assumes that all data that might be relevant to a DSR investigation is stored in Office 365; in other words, stored in the Microsoft cloud. Data stored on a user's local computer or on-premises on your organization's file servers is outside the scope of a DSR investigation for data stored in Office 365. For guidance about responding to DSR requests for data in on-premises organizations, see [GDPR for Office on-premises Servers](#).

#### Tips for searching content locations

- Begin by searching all content locations in your organization (which you can search in a single search) to quickly determine which content locations contain items that match your search query. Then you can rerun the search and narrow the search scope to the specific locations that contain relevant items.
- Use search statistics to identify the top locations that contain items that match your search query. See [View keyword statistics for Content Search results](#).
- Search the audit log for recent file and folder activities performed by the user who is the subject of the DSR.



Searching the audit log returns a list of auditing records that contain the name and location of resources the user has recently interacted with. You may be able to use this information to build a content search query. See [Search the audit log in the Security & Compliance Center](#).

#### Building search queries to find personal data

The DSR you're investigating most likely contains identifiers that you can use in the keyword search query to search for the personal data. Here are some common identifiers that can be used in a search query to find personal data:

- Email address or alias
- Phone number
- Mailing address
- Employee ID number
- National ID number or EU member version of a Social Security Number

The DSR that you're investigating most likely will have an identifier and other details about the personal data that is the subject of the request that you can use in a search query.

Searching for just an email address or employee ID will probably return many results. To narrow the scope of your search so it returns content most relevant to the DSR, you can add conditions to the search query. When you add a condition, the keyword and a search condition are logically connected by the **AND** Boolean operator. This means only items that match *both* the keyword and the condition will be returned in the search results.

The following table lists some conditions you can use to narrow the scope of a search. The table also lists the values that you can use for each condition to search for specific document types and mailbox items.

**Table 2: Narrow scope of search by using conditions**

CONDITION	DESCRIPTION	EXAMPLE OF CONDITION VALUE
File type	<p>The extension of a document or file. Use this condition to search for Office documents and files created by Office 365 applications. Use this condition when searching for documents on SharePoint Online sites and OneDrive for Business accounts. The corresponding document property is filetype. For a complete list of file extensions that you can search for, see that Default crawled file name extensions and parsed file types in SharePoint] (<a href="https://technet.microsoft.com/library/jj219530.aspx">https://technet.microsoft.com/library/jj219530.aspx</a>).</p>	<ul style="list-style-type: none"> <li>• csv — Searches for comma-separated value (CSV) files; Excel files can be saved in CSV format and CSV file can easily be imported into Excel</li> <li>• docx — Searches for Word file</li> <li>• mpp — Searches for Project files</li> <li>• one — Searches for OneNote files</li> <li>• pdf — Search for files saved in a PDF format</li> <li>• pptx — Searches for PowerPoint files</li> <li>• xls — Searches for Excel files</li> <li>• vsd — Searches for Visio files</li> <li>• wmv — Searches for Windows Media video files</li> </ul>

CONDITION	DESCRIPTION	EXAMPLE OF CONDITION VALUE
Message type	The email message type to search for. Use this condition to search mailboxes for contacts (People), meetings (Calendar) tasks, or Skype for Business conversations. The corresponding email property is <i>kind</i> .	<ul style="list-style-type: none"> <li>• *contacts — Searches the My Contacts list (People) of a mailbox</li> <li>• *email — Searches email messages</li> <li>• *im — Searches Skype for Business conversations</li> <li>• *meetings — Searches appointments and meeting requests (Calendar)</li> <li>• *tasks — Searches the My Tasks list (Tasks); using this value will also return tasks created in Microsoft To Do.</li> </ul>
Compliance tag	The label assigned to an email message or a document. Labels are used to classify email and documents for data governance and enforce retention rules based on the classification defined by the label. Use this condition to search for items that have been automatically or manually assigned a label. This is a useful condition for DSR investigations because your organization may be using labels to classify content related to data privacy or that contains personal data or sensitive information. See the "Using Content Search to find all content with a specific label applied to it" section in <a href="#">Learn about retention policies and retention labels</a>	complianceTag="personal data"

There are many more email and document properties and search conditions that you can use to build more complex search queries. See the following sections in the [Keyword queries and search conditions for Content Search](#) help topic for more information.

- [Searchable email properties](#)
- [Searchable site \(document\) properties](#)
- [Search conditions](#)

#### Searching for personal data in SharePoint lists, discussions, and forms

In addition to searching for personal data in documents, you can also use Content Search to search for other types of data that's created by using native SharePoint Online apps. This includes data created by using SharePoint lists, discussions, and forms. When you run a Content Search and search SharePoint Online sites (or OneDrive for Business accounts) data from lists, discussions, and forms that match the search criteria will be returned in the search results.

#### Examples of search queries

Here are some examples of search queries that use keywords and conditions to search for personal data in response to a DSR. The examples show two versions of the query: one showing the keyword syntax (where the condition is included in Keyword box) and one showing the GUI-based version of the query with conditions.

#### Example 1

This example returns Excel files on SharePoint Online sites and OneDrive for Business accounts that contain the specified email address. Files might be returned if the email address appears in the file metadata.

### Keyword syntax

```
pilar@contoso.com AND filetype="xlsx"
```

### GUI

The screenshot shows a search interface with two main sections. The top section is titled "Keywords" and contains a text input field with the value "pilar@contoso.com". Below the input field is a checkbox labeled "Show keyword list" with an information icon. The bottom section is titled "File type" and contains a dropdown menu set to "Equals any of". Below the dropdown is a text input field with the value "xlsx". At the bottom of the section, it says "(1 selected)".

### Example 2

This example returns Excel or Word files on SharePoint Online sites and OneDrive for Business accounts that contain the specified employee ID or birth date.

```
(98765 OR "01-20-1990") AND (filetype="xlsx" OR filetype="docx")
```

### GUI

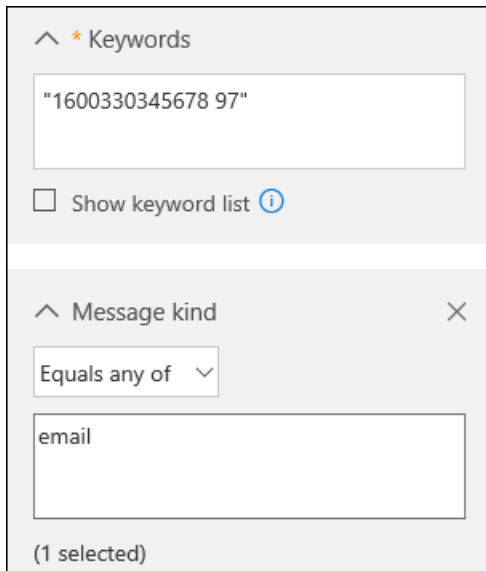
The screenshot shows a search interface with two main sections. The top section is titled "Keywords" and contains a text input field with the value "98765 OR \"01-20-1990\"". Below the input field is a checkbox labeled "Show keyword list" with an information icon. The bottom section is titled "File type" and contains a dropdown menu set to "Equals any of". Below the dropdown is a text input field with the value "xlsx;docx". At the bottom of the section, it says "(2 selected)".

### Example 3

This example returns email messages that contain the specified ID number, which is a France Social Security Number (INSEE)

```
"1600330345678 97" AND kind="email"
```

## GUI



The screenshot shows a search interface with two filter sections. The first section, titled "Keywords", has an expand/collapse arrow and a star icon, and contains a text input field with the value "1600330345678 97" and a checkbox labeled "Show keyword list" with an information icon. The second section, titled "Message kind", has an expand/collapse arrow and a close icon, and contains a dropdown menu set to "Equals any of", a text input field with the value "email", and a status indicator "(1 selected)".

### Working with partially indexed items in Content Search

Partially indexed items (also called *unindexed items*) are Exchange Online mailbox items and documents on SharePoint Online and OneDrive for Business sites that for some reason weren't indexed for search, which means they aren't searchable by using Content Search. Most email messages and site documents are successfully indexed because they fall within the [indexing limits for Office 365](#). The reasons that email messages or files aren't indexed for search include:

- The file type is [unrecognized or unsupported for indexing](#). Though sometimes the file type is supported for indexing but an indexing error occurred for a specific file
- Email messages have an attached file without a valid handler, such as image file (this is the most common cause of partially indexed email items)
- Files attached to email messages are too large or there are too many attached files

We recommend that you learn more about partially indexed items so that you can work with them when responding to DSR requests. For more information, see:

- [Partially indexed items in Content Search in Office 365](#)
- [Investigating partially indexed items in Office 365 eDiscovery](#)
- [Exporting unindexed items](#)

### Tips for working with partially indexed items

It's possible that data responsive to a DSR investigation may be in a partially indexed item. Here's some suggestions for working with partially indexed items:

- After you run a search, the number of estimated partially items is displayed in the search statistics. This estimate doesn't include partially indexed items in SharePoint Online and OneDrive for Business. Export the reports for a Content Search to get information about partially indexed items. The **Unindexed Items.csv** report contains information about unindexed items, including the location of the item, the URL if the item is in SharePoint Online or OneDrive for Business, and the subject line (for messages) or name of the document. For more information, see [Export a Content Search report](#).
- The statistics and list of partially indexed items that are returned with the results of a Content Search are all the partially items from the content locations that are searched.
- To retrieve partially indexed items that are potentially responsive to a DSR investigation, you can do one of the following things:

#### Export all partially indexed items

You export both the results of a content search and the partially indexed items from the content location that

were search. You can also export only the partially indexed items. Then you can open them in their native application and review the content. You have to use this option to export items from SharePoint Online and OneDrive for Business. See [Export Content Search results from the Security & Compliance Center](#).

#### Export a specific set of partially indexed items from mailboxes

Instead of exporting all partially indexed mailbox items from a search, you can rerun a Content Search to search for a specific list of partially indexed items, and then export them. You can do this only for mailbox items. See [Prepare a CSV file for a targeted Content Search in Office 365](#).

### Next steps

After you find the personal data that's relevant to the DSR, be sure to retain the specific Content Search that you used to find the data. You will likely reuse this search to complete other steps in the DSR response process, such as [obtaining a copy of it](#), [exporting it](#), or [permanently deleting it](#).

### Additional considerations for selected applications

The following sections describe things you should keep in mind when searching for data in the following Office 365 applications.

- [Office Lens](#)
- [OneDrive for Business and SharePoint Experience Settings](#)
- [Microsoft Teams for Education](#)
- [Microsoft To Do](#)
- [Skype for Business](#)

#### Office Lens

A person using Office Lens (a camera app supported by devices running iOS, Android, and Windows) can take a picture of whiteboards, hardcopy documents, business cards, and other things that contain a lot of text. Office Lens uses optical character recognition technology that extracts text in an image and save it to an Office document such as a Word, PowerPoint, and OneNote or to a PDF file. Users can then upload the file that contains the text from the image to their OneDrive for Business account in Office 365. That means you can use the Content Search tool to search, access, delete, and export data in files that were created from an Office Lens image. For more information about Office Lens, see:

- [Office Lens for iOS](#)
- [Office Lens for Android](#)
- [Office Lens for Windows](#)

#### OneDrive for Business and SharePoint Online experience settings

In addition to user-created files stored in OneDrive for Business accounts and SharePoint Online sites, these services store information about the user that is used to enable various experiences. Users still in your organization can access much of this information by using in-product functionality. The following information provides guidance on how to access, view, and export OneDrive for Business and SharePoint Online application data.

#### SharePoint user profiles

The user's Delve profile allows users to maintain properties stored in the SharePoint Online user profile, including birthday, mobile phone number (and other contact information), about me, projects, skills and expertise, schools and education, interests, and hobbies.

#### End users

End users can discover, access, and rectify SharePoint Online user profile data using the Delve profile experience. See [View and update your profile in Office Delve](#) for more details.

Another way for users to access their SharePoint profile data is to navigate to the **edit profile page** in their OneDrive for Business account, which can be accessed by going to the **EditProfile.aspx** path under the OneDrive for Business account URL. For example, for a user **user1@contoso.com**, the user's OneDrive for Business account is at:

```
https://contoso-my.sharepoint.com/personal/user1\contoso\com/_layouts/15/OneDrive.aspx
```

The URL for the edit profile page would be:

```
https://contoso-my.sharepoint.com/personal/user1\contoso\com/_layouts/15/EditProfile.aspx
```

Properties sourced in Azure Active Directory can't be changed within SharePoint Online. However, users can go to their **Account** page by selecting their **photo** in the Office 365 header, and then selecting **My account**. Changing the properties here may require users to work with their admins to discover, access, or rectify a user profile property.

#### Admins

An admin can access and rectify profile properties in the SharePoint admin center. In the **SharePoint admin center**, select the **user profiles** tab. select **Manage user profiles**, enter a user's name, and then select **Find**. The admin can right-select any user and select **Edit My Profile**. Properties sourced in Azure Active Directory can't be changed within SharePoint Online.

An admin can export all User Profile properties for a user by using the **Export-SPOUserProfile** cmdlet in SharePoint Online PowerShell. See [Export-SPOUserProfile](#).

For more information about user profiles, see [Manage user profiles in the SharePoint admin center](#).

#### User Information list on SharePoint Online sites

A subset of a user's SharePoint user profile is synchronized to the User information list of every site that they visit or have permissions to access. This is used by SharePoint Online experiences, such as People columns in document libraries, to display basic information about the user, such as the name of the creator of a document. The data in a User Information list matches the information stored in SharePoint user profile and will be automatically rectified if the source is changed. For deleted users, this data remains in the sites they interacted with for referential integrity of SharePoint column fields.

Admins can control which properties are replicable inside the SharePoint admin center. To do this:

1. Go to the **SharePoint admin center** and select the **user profiles** tab.
2. select **Manage User Properties** to see a list of properties.
3. Right-select any property and select **Edit** and adjust various settings.
4. Under **Policy Settings**, the replicable property controls whether the property will be represented in the User information list. Not all properties support adjusting this.

An admin can export all User information properties for a user on a given site by using the **Export-SPOUserInfo** cmdlet in SharePoint Online PowerShell. See [Export-SPOUserInfo](#).

#### OneDrive for Business experience settings

A user's OneDrive for Business experience stores information to help the user find and navigate content of interest to them. Most of this information can be accessed by end users using in-product features. An admin can export the information using a [PowerShell Script](#) and [SharePoint Client-Side Object Model \(CSOM\)](#) commands.

See [Export OneDrive for Business experience settings](#) for more information about the settings, how they are stored, and how to export them.

#### OneDrive for Business and SharePoint Online search

The in-app search experience in OneDrive for Business and SharePoint Online stores a user's search queries for 30 days to increase relevance of search results. An admin can export search queries for a user by using the **Export-SPOQueryLogs** cmdlet in SharePoint Online PowerShell. See [Export-SPOQueryLogs](#).

#### Microsoft Teams for Education

Microsoft Teams for Education offers two additional collaboration features that teachers and students can use that creates and stores personal data: Assignments and OneNote Class Notebook. You can use Content Search

to discover data in both.

#### Assignments

Students files associated with an Assignment are stored in a document library in the corresponding Teams SharePoint Online site. IT admins can use the Content Search tool to search for student files that are related to assignments. For example, an admin could search all SharePoint Online sites in the organization and use the student's name and class or assignment name in the search query to find data relevant to a DSR.

There's other data related to Assignments that isn't stored in the class team SharePoint Online site, which means it's not discoverable with Content Search. This includes:

- Files that the teacher assigns to students as part of the assignment
- Student grades and feedback from the teacher
- The list of documents submitted for an assignment by each student
- Assignment metadata

For this type of data, an IT admin or data owner (such as a teacher) may have to go into the Assignment in the class team to find data relevant to a DSR.

#### OneNote Class Notebook

The OneNote Class Notebook is stored in the class team SharePoint Online site. Every student in a class has a private notebook that's shared with the teacher. There's also a content library where a teacher can share documents with students, and a collaboration space for all students in the class. Data related to these capabilities is discoverable with Content Search.

Here's specific guidance to search for a Class Notebook.

1. Run a Content Search using the following search criteria:

- Search all SharePoint Online sites
- Include the name of the class team as a search keyword; for example, "9C Biology."

2. Preview the search results and look for the item that corresponds to the Class Notebook.

3. Select that item, and then copy the folder path that's displayed in the details pane. This is the root folder for the Class Notebook.

4. Edit the search that you created in step 1 and replace the class name in the keyword query with the folder path of the Class Notebook and precede the folder path with the **path** site property; for example, **path:"[https://contosoedu.onmicrosoft.com/sites/9C Biology/SiteAssets/9C Biology Notebook/](https://contosoedu.onmicrosoft.com/sites/9C%20Biology/SiteAssets/9C%20Biology%20Notebook/)".** Be sure to include the quotation marks and the trailing forward slash.

5. Add a search condition and select the File Type condition and use one for the value of the file type. This returns all OneNote files in the search results. The resulting keyword syntax would look something like [this](#):

```
path:"<https://contosoedu.onmicrosoft.com/sites/9C Biology/SiteAssets/9C Biology Notebook/" AND filetype="one"
```

6. Rerun the Content Search. The search results should include all OneNote files for the Class Notebook from the class team.

#### Microsoft To Do

Tasks (called *to-dos*, which are saved in *to-do lists*) in Microsoft To Do are saved as tasks in a user's Exchange Online mailbox. That means that you can use the Content Search tool to search, access, delete, and export to-dos. For more information, see [Set up Microsoft To Do](#).

#### Skype for Business

Here some additional information about how to access, view, and export personal data in Skype for Business.

- Files attached to a meeting are retained in the actual meeting for 180 days and then become inaccessible. These files can be accessed by meeting participants by joining the meeting from the meeting request and then viewing or downloading the attached file. See the "Use the attachments in the meeting" section in [Preload attachments for a Skype for Business meeting](#).
- Conversations in Skype for Business are retained in the Conversation History folder in user mailboxes. You can use Content Search to search mailboxes for data in Skype conversations.
- A data subject can export their contacts in Skype for Business. To do this, they would right-select a contact group in Skype for Business and select **Copy**. Then they can paste the list of email addresses into a text or Word document.
- If the Exchange Online mailbox of a meeting participant is placed on Litigation Hold or assigned to an Office 365 retention policy, files attached to a meeting are retained in the participants mailbox. You can use Content Search to search for those files in the participant's mailbox if the retention period for the file has not expired. For more information about retaining files, see [Retaining large files attached to a Skype for Business meeting](#).

## Providing a copy of personal data

After you've found personal data that is potentially responsive to a DSR, it's up to you and your organization to decide which data to provide the data subject. For example, you can provide them with a copy of the actual document, an appropriately redacted version, or a screenshot of the portions that you've deemed appropriate to share. For each of these responses to an access request, you'll have to retrieve a copy of the document or other item that contains the responsive data.

When providing a copy to the data subject, you may have to remove or redact personal information about other data subjects and any confidential information.

### Using Content Search to get a copy of personal data

There are two ways to use the Content Search tool to get a copy of a document or mailbox item that you've found after running a search.

- Preview the search results and then download a copy of the document or item. This is a good way to download a few items or files.
- Export the search results and then download a copy of all items returned by the search. This method is more complex, but it's a good way to download lots of items that are responsive to the DSR. Useful reports are also included with you export search results. You can use these reports to get additional information about each item. The **Results.csv** report is useful because it contains a lot of information about the exported items, such as the exact location of the item (for example, the mailbox for email messages or the URL for documents or lists on SharePoint Online and OneDrive for Business sites). This information helps you identify the owner of the item, in case you need to contact them during the DSR investigation process. For more information about the reports that are included when you export search results, see [Export a Content Search report](#).

#### Preview and download items

After you run a new search or open an existing search, you can preview each item that matched the search query to verify that it's related to the DSR you're investigating. This also includes SharePoint lists and web pages that are returned in the search results. You can also download the original file if you have to provide it to the data subject. In both cases, you could take a screenshot to satisfy the data subject's request obtain the information.

Some types of items can't be previewed. If an item or file type isn't supported for preview, you have the option to download an individual item to your local computer or to a mapped network drive or other network location. You can only preview [supported file types](#).

To preview and download items:

1. Open the Content Search in the Security & Compliance Center.



2. If the results aren't displayed, select **Preview results**.
3. select an item to view it.
4. select **Download original file** to download the item to your local computer. You'll also have to download items that can't be previewed.

For more information about previewing search results, see [Preview search results](#).

#### **Export and download items**

You can also export the results of a content search to get a copy of email messages, documents, lists, and web pages containing the personal data, though this method is more involved than previewing items. See the next section for details about [exporting the results of a Content Search](#).

## Exporting personal data

The "right of data portability" allows a data subject to request an electronic copy of personal data that's in a "structured, commonly used, machine-readable format", and to request that your organization transmit these electronic files to another data controller. Microsoft supports this right in two ways:

- Offering Office 365 applications that save data in native, machine-readable, commonly used electronic format. For more information about Office file formats, see [Office File Formats-Technical Documents](#).
- Enabling your organization to export the data in the native file format, or a format (such as CSV, TXT, and JSON) that can be easily imported to another application.

To meet a DSR export request, you can export Office documents in their native file format and export data from other Office 365 applications.

#### **Export and download content using Content Search**

When you export the results of a Content Search, email items can be downloaded as PST files or as individual messages (.msg files). When you export documents and lists from SharePoint Online and OneDrive for Business sites, copies in the native file formats are exported. For example, SharePoint lists are exported as CSV files and Web pages are exported as .aspx or html files.

#### **NOTE**

Exporting mailbox items from a user's mailbox using Content Search requires that the user (whose mailbox you're exporting items from) is assigned an Exchange Online Plan 2 license.

To export and download items:

1. Open the Content Search in the Security & Compliance Center.
2. On the search fly out page, select **More**, and then select **Export results**. You can also export a report.
3. Complete the sections on the **Export results** fly out page. Be sure to use the scroll bar to view all export options.
4. Go back to the Content search page in the Security & Compliance Center, and select the **Export** tab.
5. select **Refresh** to update the page.
6. Under the **Name** column, select the export job that you created. The name of the export job is the name of the content search appended with **\_Export**.
7. On the export fly out page, under **Export key**, select **Copy to clipboard**. You'll use this key in step 10 to download the search results
8. On the top of the fly out page, select **Download results**.
9. If you're prompted to install the **Microsoft Office 365 eDiscovery Export Tool**, select **Install**.
10. In the **eDiscovery Export Tool**, paste the export key that you copied in step 7 in the appropriate box.
11. select **Browse** to specify the location where you want to download the search result files.

12. select **Start** to download the search results to your computer.

When the export process is complete, you can access the files in the location on your local computer where they were downloaded. Results of a content search are downloaded to a folder named after the Content Search. Documents from sites are copied to a subfolder named **SharePoint**. Mailbox items are copied to subfolder named **Exchange**.

For detailed step-by-step instructions, see [Export Content Search results from the Security & Compliance Center](#).

### Downloading documents and lists from SharePoint Online and OneDrive for Business

Another way to export data from SharePoint Online and OneDrive for Business is to download documents and lists directly from a SharePoint Online site or a OneDrive for Business account. You would have to get assigned the permissions to access a site, and then go to the site and download the contents. See:

- [Download files and folders from OneDrive or SharePoint](#)
- [Export SharePoint lists to Excel](#)

For some DSR export requests, you may want to allow the data subject to download content themselves. This enables the data subject to go to a SharePoint Online site or shared folder and select **Sync** to sync all contents in the document library or selected folders. See:

- [Enable users to sync SharePoint files with the new OneDrive sync client](#)
- [Sync SharePoint files with the new OneDrive sync client](#)

## Deleting personal data

The "right to erasure" by the removal of personal data from an organization's Customer Data is a key protection in the GDPR. Removing personal data includes deleting entire documents or files or deleting specific data within a document or file (which would be an action and process like the ones described in the Rectify section in this guide).

As you investigate or prepare to delete personal data in response to a DSR, here are a few important things to understand about how data deletion (and retention) works in Office 365.

- **Soft delete vs. hard delete:** In Office 365 services such as Exchange Online, SharePoint Online, and OneDrive for Business there is the concept of *soft deletion* and *hard deletion*, which relates to the recoverability of a deleted item (usually for a limited period) before it's permanently removed from the Microsoft cloud with no chance of recovery. In this context, a soft-deleted item can be recovered by a user and/or an admin for a limited amount of time before it's hard-deleted. When an item has been hard-deleted, it's marked for permanent removal and is purged when it's processed by the corresponding Office 365 service. Here's how soft delete and hard delete works for items in mailboxes and sites (regardless of whether the data owner or an admin deletes an item):
  - **Mailboxes:** An item is soft-deleted when it's deleted from the Deleted Items folder or when a user deletes an item by pressing **Shift + Delete**. When item is soft-deleted, it's moved to the Recoverable Items folder in the mailbox. At this point, the item can be recovered by the user until the deleted item retention period expires (in Office 365, the deleted item retention period is 14 days, but can be increased up to 30 days by an admin). After the retention period expires, the item is hard-deleted and moved to a hidden folder (called the *Purges* folder). The item will be permanently removed (purged) from Office 365 the next time the mailbox is processed (mailboxes are processed once every seven days).
  - **SharePoint Online and OneDrive for Business sites:** When a file or documented is deleted, it is moved to the site's Recycle Bin (also called the *first-stage Recycle Bin* (which is like the Recycle Bin in Windows)). The item remains in the Recycle Bin for 93 days (the deleted item retention

period for sites in Office 365). After that period, the item is automatically moved to Recycle Bin for the site collection, which also called the *second-stage Recycle Bin*. (Note that users or admins--with the appropriate permissions--can also delete items from the first-stage Recycle Bin). At this point, the item becomes soft-deleted; it can still be recovered by a site collection administrator in SharePoint Online or by the user or admin in OneDrive for Business). When an item is deleted from the second-stage Recycle Bin (either manually or automatically), it becomes hard-deleted and isn't accessible by user or an admin. The retention period is 93 days for both the first-stage and second-stage recycle bins. That means the second-stage Recycle Bin retention starts when the item is first deleted. Therefore, the total maximum retention time is 93 days for both recycle bins.

#### NOTE

Understanding the actions that result in an item being soft-deleted or hard-deleted will help you determine how to delete data in a way that meets GDPR requirements when responding to a deletion request.

- **Legal holds and retention policies:** In Office 365, a "hold" can be place on mailboxes and sites. In short, this means that nothing is permanently removed (hard-deleted) if a mailbox or site is on hold, until the retention period for an item expires or until the hold is removed. This is important in the context of deleting Customer Content in response to a DSR: if an item is hard-deleted from a content location that is on hold, the item is not permanently removed from Office 365. That means it could conceivably be recovered by an IT admin. If your organization has a requirement or policy that data be permanently deleted and unrecoverable in Office 365 in response to DSR, then a hold would have to be removed from a mailbox or site to permanently delete data in Office 365. More than likely, your organization's guidelines for responding to DSRs have a process in place to determine whether a specific DSR deletion request or a legal hold takes precedence. If a hold is removed to delete items, it can be reimplemented after the item is deleted.

#### Deleting documents in SharePoint Online and OneDrive for Business

After you find the document on a SharePoint Online site or in a OneDrive for Business account (by following the guidance in Discover section of this guide) that needs to be deleted, a data privacy officer or IT admin would need to be assigned the necessary permissions to access the site and delete the document. If appropriate, the document owner can also be instructed to delete the document.

Here's the high-level process for deleting documents from sites.

1. Go to the site and locate the document.
2. Delete the document. When you delete a document from a site, it's sent to the first-stage Recycle Bin.
3. Go to the first-stage Recycle Bin (the site Recycle Bin) and delete the same document you deleted in the previous step. The document is sent to the second-stage Recycle Bin. **At this point, the document is soft-deleted.**
4. Go to the second-stage Recycle Bin (which is the site collection Recycle Bin) and delete the same document that you deleted from the first-stage Recycle Bin. **At this point, the document is hard-deleted.**

#### IMPORTANT

You can't delete a document that is located on a site that is on hold (with one of the retention or legal hold features in Office 365). In the case where a DSR delete request takes precedence over a legal hold, the hold would have to be removed from the site before a document could be permanently deleted.

See the following topics for detailed procedures.

- [Delete a file, folder, or link from a SharePoint document library](#)
- [Delete items or empty the Recycle Bin of a SharePoint site](#)
- [Delete items from the site collection recycle bin](#)

- "Get access to the former employee's OneDrive for Business documents" section in [Get access to and back up a former user's data](#)
- [Delete files or folders in OneDrive for Business](#)
- [Delete a list in SharePoint](#)
- [Delete list items in SharePoint Online](#)

### **Deleting a SharePoint site**

You may determine that the best way to respond to a DSR delete request is to delete an entire SharePoint site, which will delete all that data located in the site. You can do this by running cmdlets in SharePoint Online PowerShell.

- Use the [Remove-SPOSite](#) cmdlet to delete the site and move it the SharePoint Online Recycle Bin (soft-delete).
- Use the [Remove-SPODeletedSite](#) cmdlet to permanently delete the site (hard-delete).

You can't delete a site that is placed on an eDiscovery hold or is assigned to a retention policy. Sites must be removed from an eDiscovery hold or retention policy before you can delete it.

### **Deleting a OneDrive for Business site**

Similarly, you may determine to delete a user's OneDrive for Business site in response to a DSR deletion request. If you delete the user's Office 365 account, their OneDrive for Business site is retained (and restorable) for 30 days. After 30 days, it's moved to the SharePoint Online Recycle Bin (soft-deleted), and then after 93 days, it's permanently deleted (hard-deleted). To accelerate this process, you can use the [Remove-SPOSite](#) cmdlet to move the OneDrive for Business site to the Recycle Bin and then use the [Remove-SPODeletedSite](#) cmdlet to permanently delete it. As with sites in SharePoint Online, you can't delete a user's OneDrive for Business site if it was assigned to an eDiscovery hold or a retention policy before the user's account was deleted.

### **Deleting OneDrive for Business and SharePoint Online Experience Settings**

In addition to user-created files stored in OneDrive for Business accounts and SharePoint Online sites, these services store information about the user that is used to enable various experiences. These were previously documented in this document. See the [Additional considerations for selected applications](#) section under [Using the Content Search eDiscovery tool to respond to DSRs](#) for information about how to access, view, and export OneDrive for Business and SharePoint Online application data.

### **Deleting a SharePoint user profile**

The SharePoint user profile will be permanently deleted 30 days after the user account is deleted in Azure Active Directory. However, you can hard-delete the user account, which will remove the SharePoint user profile. For more information, see the [Deleting a user section in this guide](#).

An admin can expedite the deletion of the User Profile for a user by using the [Remove-SPOUserProfile](#) cmdlet in SharePoint Online PowerShell. See [Remove-SPOUserProfile](#). This requires the user to be at least soft-deleted in Azure Active Directory.

### **Deleting User Information lists on SharePoint Online sites**

For users that have left the organization, this data remains in the sites they interacted with for referential integrity of SharePoint column fields. An admin can delete all User information properties for a user on a given site by using the [Remove-SPOUserInfo](#) command in SharePoint Online PowerShell. See [Remove-SPOUserInfo](#) for information about running this PowerShell cmdlet.

By default, this command retains the display name of the user and deleted properties such as telephone number, email address, skills and expertise, or other properties that were copied from the SharePoint Online user profile. An admin can use the [RedactUser](#) parameter to specify an alternate display name for the user in the User Information list. This affects several parts of the user experience and will result in information loss when looking at the history of files in the site.

Finally, the redaction capability will not remove all metadata or content referencing a user from documents. The way to achieve redaction of file content and metadata is described in the [Making changes to content in OneDrive for Business and SharePoint Online](#) section in this guide. This method consists of downloading, deleting, and then uploading a redacted copy of the file.

#### **Deleting OneDrive for Business experience settings**

The recommended way to delete all OneDrive for Business experience settings and information is to remove the user's OneDrive for Business site, after reassigning any retained files to other users. An admin can delete these lists using [PowerShell Script](#) and [SharePoint Client-Side Object Model \(CSOM\)](#) commands. See [Deleting OneDrive for Business experience settings](#) for more information about the settings, how they are stored, and how to delete them.

#### **OneDrive for Business and SharePoint Online search queries**

A user's search queries created in the OneDrive for Business and SharePoint Online search experience are automatically deleted 30 days after the user creates the query.

#### **Deleting items in Exchange Online mailboxes**

You may have to delete items in Exchange Online mailboxes to satisfy a DSR delete request. There are two ways that an IT admin can delete items in mailbox, depending on whether to soft-delete or hard-delete the target items. Like documents on SharePoint Online or OneDrive for Business sites, items in a mailbox that is on hold can't be permanently deleted from Office 365. The hold must be removed before the item can be deleted. Again, you'll have to determine whether the hold on the mailbox or the DSR delete request takes precedence.

##### **Soft-delete mailbox items**

You can use the Content Search Action functionality to soft-delete items that are returned by a Content Search. As previously explained, soft-deleted items are moved to the Recoverable Items folder in the mailbox while hard-deleted items are permanently deleted and cannot be recovered.

Here's a quick overview of this process:

1. Create and run a Content Search to find the items that you want to delete from the user mailbox. You may have to rerun the search to narrow that search results so that only the items that you want to delete are returned in the search results.
2. Use the **New-ComplianceSearchAction -Purge PurgeType SoftDelete** or **New-ComplianceSearchAction -Purge PurgeType HardDelete** command in Office 365 PowerShell to delete items that are returned by the Content Search that was created in the previous step.

For detailed instructions, see [Search for and delete email messages in your organization](#).

##### **Hard-delete items in a mailbox on hold**

As previously explained, if you hard-delete items in a mailbox on hold, items are not removed from the mailbox. They are moved to a hidden folder in the Recoverable Items folder (the **Purges** folder) and will remain there until the hold duration for the item expires or until the hold is removed from the mailbox. If either of those things happen, the items will be purged from Office 365 the next time that the mailbox is processed.

Your organization might determine that items being permanently deleted when the hold duration expires meets the requirements for a DSR deletion request. However, if you determine that mailbox items must be immediately purged from Office 365, you would have to remove the hold from the mailbox and then hard-deleted the items from the mailbox. For detailed instructions, see [Delete items in the Recoverable Items folder of cloud-based mailboxes on hold](#).

#### **NOTE**

To hard-delete mailbox items to satisfy a DSR deletion request by following the procedure in the previous topic, you may have to soft-delete those items while the mailbox is still on hold so that they are moved to the Recoverable Items folder.

# Deleting a user

In addition to deleting personal data in response to a DSR deletion request, a data subject's "right to be forgotten" may also be fulfilled by deleting their user account. Here are some reasons that you might want to delete a user:

- The data subject has left (or is in the process of leaving) your organization.
- The data subject has requested that you delete system-generated logs that have been collected about them. Examples of data in system-generated logs include Office 365 app and service usage data, information about search requests performed by the data subject, and data generated by product and services as a product of system functionality and interaction by users or other systems. For more information, see [Part 3: Responding to DSRs for system-generated Logs](#) in this guide.
- Permanently prevent the data subject from accessing or processing data in Office 365 (as opposed to temporarily restriction access by the methods described in the section [Responding to DSR restriction requests](#)).

After you delete a user account:

- The user can no longer sign-in to Office 365 or access any of your organization's Microsoft resources, such as their OneDrive for Business account, SharePoint Online sites, or their Exchange Online mailbox.
- Personal data, such as email address, alias, phone number, and mailing address, that's associated with the user account is deleted
- Some Office 365 apps remove information about the user. For example, in Microsoft Flow, the deleted user is removed from the list of owners for a shared flow.
- System-generated logs about the data subject, with the exception of data that may compromise the security or stability of the service, will be deleted 30 days after the user account is deleted. For more information, see the section [Deleting system-generated logs](#).

## IMPORTANT

After you delete a user account, that person will lose the ability to sign in to Office 365 and the ability to sign in to any products or services for which he or she formerly relied upon for a work or school account. That person would also be unable to initiate any DSR requests through Microsoft directly in instances where Microsoft is the data controller. For more information, see the [Product and services authenticated with an Org ID for which Microsoft is a data controller](#) section in Part 4 of this guide.

## NOTE

In the event that you are a customer currently engaged in FastTrack migrations, deleting the user account will not delete the data copy held by the Microsoft FastTrack team, which is held for the sole purpose of completing the migration. If, during the migration, you would like the Microsoft FastTrack team to also delete the data copy, you can [submit a request](#). In the ordinary course of business, Microsoft FastTrack will delete all data copies once the migration is complete.

Like the soft-deletion and hard-deletion of data that was described in the previous section on deleting personal data, when you delete a user account, there is also a soft-deleted and hard-deleted state.

- When you initially delete a user account (by deleting the user in the admin center or in the Azure portal), the user account is soft-deleted, and moved the Recycle Bin in Azure for up to 30 days. At this point, the user account can be restored.
- If you permanently deleted the user account, the user account is hard-deleted and removed from the Recycle Bin in Azure. At this point, the user account can't be restored, and any data associated with the user account will be permanently removed from the Microsoft cloud. Hard-deleting an account deletes system-generated logs about the data subject, except for data that may compromise the security or stability of the service.

Here's the high-level process for deleting a user from your organization.

1. Go to the admin center or the Azure portal and locate the user.
2. Delete the user. When you initially delete the user, the user's account is sent to the Recycle Bin. At this point, the user is soft-deleted. The account is retained in the soft-deleted for 30 days, which allows you to restore the account. After 30 days, the account is automatically hard-deleted. For specific instructions, see [Delete users from Azure AD](#).

You can also soft-delete a user account in the admin center. See [Delete a user from your organization](#).

3. If you don't want to wait for 30-days for the user account to be hard-deleted, you can manually hard-delete it. To do this in the Azure portal, go to the Recently deleted users list and permanently delete the user. At this point, the user is hard-deleted. For instructions, see [How to permanently delete a recently deleted user](#).

You can't hard-delete a user in the Office 365 admin portal.

#### NOTE

In Office 365 operated by 21Vianet (China), you can't permanently delete a user as previously described. To permanently delete a user, you can submit a request via the Office 365 admin portal at this [URL](#). Go to **Commerce** and then select **Subscription** -> **Privacy** -> **GDPR** and enter the required information.

### Removing Exchange Online data

One thing to understand when deleting a user is what happens to the user's Exchange Online mailbox. After the user account is hard-deleted (in step 3 in the previous process) the deleted user's mailbox isn't automatically purged from Office 365. It takes up to 60 days after the user account is hard-deleted to permanently remove it from Office 365. Here's the mailbox lifecycle after the user account is deleted and a description of the state of the mailbox data during that time:

- **Day 1-Day 30** — The mailbox can be fully restored by restoring the soft-deleted user account.
- **Day 31-Day 60** — For 30 days after the user account is hard-deleted, an admin in your organization can recover the data in the mailbox and import it into a different mailbox. This provides organizations the ability to recover the mailbox data if necessary.
- **Day 61-Day 90** - An admin can no longer recover the data in the mailbox. The mailbox data will be marked for permanent removal, and it takes up to 30 more days for the mailbox data to be purged from Office 365.

If you determine that this mailbox lifecycle doesn't meet your organization's requirements for responding to a DSR deletion request, you can [contact Microsoft Support](#) *after* you hard-delete the user account, and request Microsoft to manually initiate the process to permanently remove the mailbox data. This process to permanently remove mailbox data starts automatically after day 61 in the lifecycle, so there would be no reason to contact Microsoft after this point in the lifecycle.

## Using In-App functionality to respond to DSRs

While most Customer Data is authored and produced using the applications described in the previous section, Office 365 also offers many other applications that customers can use to produce and store Customer Data. However, Content Search doesn't currently have the ability to find data authored in these other Office 365 applications. To find data generated by these applications, you or the data owner must use in-product functionality or features to find data that may be relevant to a DSR. The following list identifies these Office 365 applications.

Applications where in-app functionality can be used to find Customer Data:

- Access
- Business App for Office 365
- Education
- Flow
- Forms
- Kaizala
- Planner
- Power Apps
- Power BI
- Project
- Publisher
- Stream
- Yammer

## Access

The following sections explain how to use the in-app functionality in Microsoft Access to find, access, export, and delete personal data.

### Discover

There are several ways that you can search for records in an Access database that might be responsive to a DSR request. For a DSR investigation, you can search for records that related to the data subject or search for records that contain specific data. For example, you could either search or go to a record that corresponds to the data subject. Or you can search for records that contain specific data, such as personal data about the data subject. For more information, see:

- [Find records in an Access database](#)
- [Create a simple select query](#)

### Access

After you find the records or fields that are relevant to the DSR request, you can take a screenshot of the data or export it to an Excel file, Word file, or a text file. You can also create and print a report based on a record source, or a select query that you created to find the data. See:

- [Introduction to reports in Access](#)
- [Export data to Excel](#)
- [Export data to a Word document](#)
- [Export data to a text file](#)

### Export

As previously explained, you can export data from an Access database to different file formats. The export file format that you choose might be determined by the specific DSR export request from a data subject. See [Import and export](#) for a list of topics that describe how to export Access data in different file formats.

### Delete

You can delete an entire record or just a field from an Access database. The quickest way to delete a record from an Access database is to open the table in Datasheet view, select the record (row) or just the data in a field that you want to delete, and then press Delete. You can also use a select query that you created to find data and then convert it to a delete query. See:

- [Delete one or more records from a database](#)
- [Create and run a delete query](#)

## Business Apps for Office 365

This section explains how to use the in-app functionality in each of the following Business Apps for Office 365 to respond to DSR requests.



- [Bookings](#)
- [Listings](#)
- [Connections](#)

### **Bookings**

The following sections explain how to use the in-app functionality in Microsoft Bookings to find, access, export, and delete personal data. This applies to both the standalone Bookings app and to Bookings when accessed through the Business center.

Microsoft Bookings allows administrators and users or staff, with a Bookings license in their organization, to set up booking pages so customers can schedule and make changes to appointments, receive confirmation emails, updates, cancellation, and reminders email. Business owners and their staff can also book events on behalf of their customers with Bookings.

The following types of data are created by customers, administrators, or staff:

- **Contact information of customers, partners, and friends** - This data contains name, phone number, email address, address, and notes.
  - Contacts for anyone can be manually created by using the Bookings Web, iOS, and Android clients.
  - Contacts for anyone can be imported from a C1's mobile device into Bookings with the Bookings iOS and Android clients.
  - Contacts are also auto-created at the time of booking creation through the booking workflow for anyone booked, whether the booking is created by a user on a customer's behalf or if it's created by the customer using the owner's booking page.
- **Booking events** - These are meetings between the business owner or their designated staff and a customer, which are created either by the business owner or the customer through the business owner's public booking page. This data includes name, address, email address, phone number, and any other info the business owner collects from the customer at the time of booking.
- **Email confirmations/cancellations/updates** - These are email messages generated and sent by the system in association with specific booking events. They contain personal data about the staff who is scheduled to deliver the relevant service and they contain personal data about the customer that was entered by either the business owner or the customer at the time of booking.

All customer content is stored in the Exchange Online mailbox that hosts the organization's Bookings. This content is retained for as long as the business owner and customer are active in the service, unless they explicitly request that the data be deleted or if they leave the service. This content can be deleted with in-product UI, with a cmdlet, or through deletion of the relevant booking mailbox. Once the deleted action is initiated, the data is deleted within the time period set by the business owner.

If a customer decides to leave the service, their customer contents is deleted after 90 days. For more information about when mailbox content is deleted after a user account is deleted, see [Removing Exchange Online data](#).

### **End User Identifiable Information**

End user Identifiable Information (EUII) includes personal and contact information about the staff that gets scheduled in Bookings. It's added to the Staff details pages when the business owner sets up Bookings and makes updates after the setup. It contains staff member's name, initials, email address, and phone number. This data is stored in the Exchange Online mailbox that hosts Bookings.

This data is retained for as long as the staff member is active in the service unless it's explicitly deleted the business owner or an admin using the in-app UI or by deleting the relevant booking mailbox. When the admin initiates the deletion of staff's details, or if the staff member leaves the service, their details are deleted in accordance with the Exchange Online mailbox's content retention policies set by the business owner or admin.

#### Discover/Access

Bookings gather and store the following types of data:

- **Business profile information:** Customer content about the business using Bookings is collected through the Bookings' Business information form and is synchronized with the Business Center Business Profile if a customer is using Bookings along with the Business center. The only EUII associated with this data is an email address of the C1. This address is where new booking notifications and update emails are sent.
- **Customer contacts:** Contacts can be manually created in the Bookings Web, iOS, and Android clients, or they can be imported from a mobile device. Contacts are also automatically created during the use of the self-service booking page. They contain EUII and are stored in the Bookings mailbox.
- **Staff details:** Customer content includes data about the staff that are eligible to deliver the services created from either the Bookings Web, iOS, or Android clients. Staff details can contain name, email address, and phone number.
- **Booking events:** These are customer meetings and related customer content created by the business using a Web client or Android/iOS app, or created by the customer using a public booking page (or a Facebook page). These events can include name, address, email address, phone number, and appointment details.
- **Meeting requests, email confirmations/cancellations/updates, and email reminders:** These are email messages sent by the system in association with bookings. They contain staff data and customer data that was entered at time of booking.

#### Export

To export data corresponding to the business owner, staff and customers, you can use the Business center privacy portal. See [Export or delete user data using Business center privacy portal](#).

#### Delete

You can delete the following types of Bookings data in response to a DSR deleting request:

- **Business profile information and contacts:** You can delete the Bookings mailbox in the admin center. After you delete the mailbox, you can restore it with 30 days. After 30 days, the account and the corresponding mailbox are permanently deleted. For details about deleting a user account, see the section [Deleting a user](#).
- **Staff details:** You can delete staff from the Bookings dashboard. To permanently detail staff, you can delete their Office 365 account.
- **Bookings events:** You can delete bookings events from the Bookings calendar, which will remove the customer's information.
- **Meeting requests, email confirmations/cancellations/updates, and email reminders:** You can delete these from the Bookings calendar, which will remove the customer's information.

Business owners and admins can also delete their customer's data by using the Business center privacy portal. See [Export or delete user data using Business center privacy portal](#).

Additionally, you can delete business owner and staff data, you can delete the corresponding user account. See the section [Deleting a user](#).

#### Listings

The following sections explain how to use the in-app functionality in Microsoft Listings to find, access, export, and delete personal data.

#### Discover

Listings owner can connect their business to Google, Bing, Yelp, and Facebook to see an aggregated view of ratings and reviews. Listings collect and store the following types of data:

- Google reviews and ratings
- Bing reviews and ratings
- Yelp reviews and ratings
- Facebook reviews and ratings

#### Access

Listings owner can sign in to the Listings dashboard to see their reviews and ratings.

#### Export

To export business owner, staff and customer data, use the Business center privacy portal. See [Export or delete user data using Business center privacy portal](#).

#### Delete

If a Listings owner would like to delete their Listings information, they can disconnect from the provider on the Listings page. After they disconnect, their Listings information will be deleted.

### Connections

The following sections explain how to use the in-app functionality in Microsoft Connections to find, access, export, and delete personal data.

#### Discover

Connections collect and store the following types of data:

- Customers/contacts are created by the business using the web client or mobile app (iOS, Android), or by using the app when a business contact is sent an email marketing campaign. Customer data can include name, address, email address, and tax ID numbers. Contacts are shared across all Business center apps.
- Customers can sign up on the Connections sign-up page and save their personal information.
- Links from email campaigns

#### Access

A Connections owner can sign in to the Connections dashboard and see the email campaigns they've sent.

#### Export

To export business owner, staff and customer data, use the Business center privacy portal. See [Export or delete user data using Business center privacy portal](#).

#### Delete

After a Connections owner sends an email campaign, they can't delete the campaign. If there are any draft campaigns they want to delete, they can sign in to the Connections dashboard and delete the draft campaigns.

### Education

This section explains how to use the in-app functionality of the following Microsoft Education apps to respond to DSR requests.

- Assignments
- Class Notebook

#### Assignments

The following sections explain how to use the in-app functionality in Assignments to find, access, export, and delete personal data.

#### Discover/Access

Assignments stores information that is generated both by teachers and students. Some of this information is store in SharePoint and some is stored in a non-SharePoint location.

#### Finding Assignments data stored in SharePoint

Students files associated with a Submission for Assignment are stored in a document library (named **Student Work**) and files associated with Assignments that are created by teachers and (accessible by students) are stored in a different document library (named **Class Files**). Both document libraries are in the corresponding Class Team SharePoint site.

An admin can use the Content Search tool in the Security & Compliance Center to search for student files (in the Student Work and Class Files libraries) that are related to submissions on assignments and files related to assignments. For example, an admin could search all SharePoint sites in the organization and use the student's name and class or assignment name in the search query to find data relevant to a DSR request.

Similarly, an admin can search for teacher files related to assignments for files that a teacher distributed to students. For example, an admin could search all SharePoint sites in the organization and use the teacher's name and class or assignment name in the search query to find data relevant to a DSR request.

For more information, see:

- [Assignments Admin Documentation](#)
- [Using the Content Search eDiscovery tool to respond to DSRs](#) (in this guide)

#### Finding Assignments data not stored in SharePoint

The following types of Assignments data are not stored in the class team SharePoint site, and therefore aren't discoverable by using Content Search. This data includes the following:

- Student grades and feedback from the teacher
- The list of documents submitted for an assignment by each student
- Assignment details, like the date the assignment is due

To find data, an admin or a teacher would have to go into the Assignment in the Class Team site to find data that may be relevant to a DSR request. An admin can add themselves as an owner to the class and view all the assignments for that class team.

Even if a student is no longer part of a class, their data might still be present in the class and marked as "no longer enrolled". In this case, a student submitting a DSR request would have to provide the admin the list of classes that they were formally enrolled in.

#### Export

You can export Assignments data for a specific student for all classes in which the student is enrolled by using a PowerShell script to get a list of classes for the student and then using a PowerShell script to export the data.

See:

- [Configure Assignments for Teams](#)
- [Get a list of classes for a specific student](#)
- [Export student and teacher data from Assignments](#)

If the student has been removed from the Team Class site, the admin can add the student back to the site before running the export script. Or the admin can use the input file for the script to identify every class that the student was ever enrolled in. You can also use the Assignment export script to export submissions data for all assignments that a teacher has access to.

#### Delete

You can delete Assignments data for a specific student for all classes in which the student is enrolled by using a PowerShell script to get a list of classes for the student and then using a PowerShell script to delete the data. You should do this before you remove the student from the class. See:

- [Configure Assignments for Teams](#)
- [Get a list of classes for a specific student](#)
- [Delete student data from Assignments](#)

If the student has been removed from the Team Class site, the admin can add the student back to the site before running the export script. Or the admin can use the input file for the script to identify every class that the student was ever enrolled in. You can't use the Assignments deletion script to delete teacher data because all Assignments are shared across the Class Team site. As an alternative, an admin would have to add themselves to the Class Team site and then delete a specific Assignment.

#### Class Notebook

Searching for content in Class Notebook is discussed previously in this guide. See the [OneNote Class Notebook](#) section. You can also use the Content Search tool to export data from a Class Notebook. Alternatively, an admin or the data subject can export data from a Class Notebook. See [Save a copy of a Class Notebook](#).

## Flow

The following sections explain how to use the in-app functionality in Microsoft Flow to find, access, export, and delete personal data.

### Discover

People can use Flow to perform data-related tasks such as synchronizing files between applications, copying files from one Office 365 service to another, and collecting data from one Office 365 app and storing it in another. For example, a user could set up a Flow to save Outlook email attachments to their OneDrive for Business account. In this example, you could use the Content Search tool to search the user's mailbox for the email message that contained the attachment or search their OneDrive for Business account for the file. This is an example where data handled by Flow might be discoverable in the Office 365 services connected by a Flow workflow.

Additionally, people can use Flow to copy or upload files from Office 365 to an external service, such as Dropbox. In these cases, a DSR request concerning the data in an external service would have to be submitted to the external service, who is processing the data in this type of scenario.

If an admin receives a DSR request, they can add themselves as an owner of a user's flows. This enables an admin to perform functions including exporting flow definitions, running histories, and performing flow permission reassignments. See [Manage Flows in the Admin Center](#).

An admin's ability to add themselves as an owner of a Flow requires an account with the following permissions:

- Flow/PowerApps Plan 2 license (paid or trial)
  - [Global administrator](#)
- or
- [Azure Active Directory global administrator](#)

Having these privileges enables the admin to use the Flow admin center to access all Flows in the organization.

To add yourself as an owner of a flow.

1. Go to <https://admin.flow.microsoft.com>
2. Sign in with your Office 365 credentials.
3. On the **Environments** page, select the environment for the flows that you want to access. Organizations have a default environment.
4. On the page for the environment that you selected, select **Resources**, and then select **Flows**. A list of all flows in the environment is displayed.
5. select **View details** for the flow that you want to add yourself as a member.
6. Under **Owners**, select **Manage sharing**.
7. On the **Share** flyout, add yourself as a member and then save the change.

After you make yourself an owner, go to **Flow > My flows > Team flows** to access the flow. From there, you can download the run history or export the flow. See:

- [Download flow run history](#)
- [Export and import your flows across environments with packaging](#)

### Access

A user can access the definitions and run histories of their flows.

- **Flow definitions:** A user can export the definition of a flow (which is exported as a Flow package, formatted as JSON in a zipped file). See [Export and import your flows across environments with packaging](#).
- **Flow run histories:** A user can download the run history of each of their flows. A flow run history is

downloaded as a CSV file, which can be opened in Excel to filter or search. Users can also download the run history of multiple flows. See [Download flow run history](#).

#### Delete

An admin can add themselves as an owner of a user's flows in the Flow admin center. If a user leaves your organization and their Office 365 account is deleted, the flows that they are the sole owner of will be retained. This is to help your organization transition the flows to new owners and avoid any disruption to your business for flows that may be used for shared business processes. An admin then needs to determine whether to delete the flows that were owned by the user or reassign to new owners, and take that action.

For shared flows, when a user is deleted from your organization, their name is removed from the list of owners.

#### Export

An admin can export the definition and run history of a user's flows. To do this, an admin must add themselves as an owner of the user's flow in the Flow admin center

- **Flow definitions:** After an admin adds themselves as an owner of a flow, they can go to **Flow > My Flows > Teams flows** to export the flow definition (which is exported as a Flow package, formatted as JSON in a zipped file). See [Export and import your flows across environments with packaging](#).
- **Flow run histories:** Similarly, an admin must add themselves as an owner of a Flow to export its flow run history. The Flow run history is downloaded as a CSV file, which means you can use Excel to filter or search. You can also download the run history of multiple Flows, as long as you have ownership. See [Download flow run history](#).

#### Connections and custom connectors in Flow

Connections require users to provide credentials to connect to APIs, SaaS applications, and custom developed systems. These connections are owned by the user that established the connection and can be [managed](#) in-product. After Flows have been reassigned, an admin can use PowerShell cmdlets to list and delete these connections as part of deleting user data.

Custom connectors allow organizations to extend the capabilities of Flow by connecting to systems where an out-of-box connector is not available. A custom connector author can [share](#) their connector with others in an organization. After receiving a DSR deleting request, an admin should consider reassigning ownership of these connectors to avoid business disruption. To expedite this process, an admin can use PowerShell cmdlets to list, reassign, or delete custom connectors.

#### Forms

The following sections explain how to use the in-app functionality in Microsoft Forms to find, access, export, and delete personal data.

##### Discover

Forms users can go to <https://forms.office.com> and select **My forms** to see the Forms they've created. They can also select **Shared with me** to view Forms others have shared via a link. If there are many Forms to sort through, users can use the in-product search bar to search for Forms by title or author. To determine whether Microsoft Forms is a place where personal data responsive to your DSR is likely to reside, you can ask the Data Subject to search his or her **Shared with me** list to determine which users ("Forms owners") have sent Forms to the Data Subject. You can then ask the forms owners to select **Share** in the top navigation bar and send you a link to a specific form so you can view it and further determine whether it is material to your DSR.

##### Access

After the relevant Forms are found, you can access the responses to the Form by clicking the **Responses** tab. Learn more about how to [check your quiz results](#) or [form results](#). To review response results in Excel, select the **Responses** tab, and then select **Open in Excel**. If you would like to send the Data Subject a copy of the Form, you can either take screenshots of the relevant questions and answers that are in shown in the application in rich text format or send the Data Subject an Excel copy of the results. If you are using Excel and would like to share with the Data Subject only portions of the survey result, you can delete certain rows or columns or redact

the remaining sections before sharing the results. Alternatively, you can go to **Share > Get a link to duplicate** (under Share as a template) to provide the Data Subject with a replicate of the entire Form.

#### **Delete**

Any survey, quiz, questionnaire, or poll can be permanently deleted by its owner. If you would like to honor a DSR "forget me" and delete a form in its entirety, find the Form in the list of forms, select the series of dots (ellipsis) in the upper right corner of the form preview window, and then select **Delete**. Once a Form is deleted, it can't be retrieved. For information, see [Delete a Form](#).

#### **Export**

To export form questions and responses to an Excel file, open the form, select the **Responses** tab, and then select **Open in Excel**.

#### **Kaizala**

The following sections explain how to use the in-app functionality in Microsoft Kaizala to find, access, export, and delete personal data.

#### **Discover**

A user's organizational data, which is data that is shared in organizational groups, can be accessed by an admin from the Kaizala management portal. Organizational data is retained for a duration of time determined by your organization's retention policies. In addition to user data, Kaizala servers also store the following types of organizational data:

- List of members who are part of the organization's groups
- Organization group messages data, which are messages and responses shared across organizational groups
- A list of users in the organizations
- Product and service usage data captured for all users in the organization.
- Kaizala Actions created by the organization
- Kaizala connectors data

A user's consumer data can be accessed by the data subject using the Kaizala mobile app for consumer data. Consumer data includes the following types of data:

- Data belonging to private groups on Kaizala (stored on Kaizala servers for 90 days)
- A user's profile information and the user's contacts
- List of members who are part of the same groups as the user
- Group messages and responses shared across groups
- The user's contact list (stored on Kaizala service)
- Transactions made by the user on Kaizala (applies to Kaizala users in India only)
- Product and service usage data for the user

#### **Access**

Kaizala users can go to their mobile device to see Kaizala content they've created on their device. To determine whether Kaizala mobile apps are a place where personal data responsive to a DSR is likely to reside, you can ask the data subject to search their Kaizala app for the requested information.

#### **Export**

When users in your organization use Kaizala, consumer data is generated, and organizational data may be generated if the user participates in an organization group. Admins can export a user's organizational data from the Kaizala management portal. Kaizala consumer users can export their private data from the Kaizala mobile app. In both cases, note that product and service usage data is also export when an admin or user exports Kaizala data. For details, see:

- [Export or delete a user's organizational data in Kaizala](#)
- [Export or delete your data in the Kaizala mobile app](#)

## Delete

A Kaizala admin can remove a Kaizala user's account in the Kaizala management portal. After a user account is deleted, the user is removed from all groups that belong to your organization and organizational data is deleted from their device.

To remove all private data from the user's mobile device, the Kaizala user can delete their Kaizala account. After the account is deleted, all related Kaizala content including, chats, photos, and other data will be deleted from the device.

For details, see:

- [Export or delete a user's organizational data in Kaizala](#)
- [Export or delete your data in the Kaizala mobile app](#)

## Planner

The following sections explain how to use the in-app functionality in Microsoft Planner to find, access, export, and delete personal data.

### Discover

Planner plans are associated with a Microsoft 365 Group, and the files for Microsoft 365 Groups are stored in an associated SharePoint Online site for the group. That means that you can use Content Search to find Planner files by searching the site for the Microsoft 365 Group. To do this, you need to have the URL for the Microsoft 365 Group. See [Searching Microsoft Teams and Microsoft 365 Groups](#) in the "Content Search in Office 365" help topic for tips about getting information about Microsoft 365 Groups to help you search for Planner files in the corresponding SharePoint Online site.

### Access

As previously explained, you can search the underlying SharePoint Online site and mailbox that are associated with a plan. Then you can preview or download the related search results to access data.

### Delete

You can manually delete a user's personally information by either giving yourself permissions to access the plans the user is part of or signing in as the user to make the changes. See [Delete user data in Microsoft Planner](#).

### Export

You can use a PowerShell script to export a user's data from Planner. When you export the data, a separate JSON file is export for each plan that the user is a part of. See [Export user data from Microsoft Planner](#).

## Power BI

The following sections explain how to use the in-app functionality in Microsoft Power BI to find, access, export, and delete personal data.

### Discover

You can search for content in the different workspaces in Power BI, including dashboards, reports, workbooks, and datasets. Each type of workspace contains a search field that you can use to search that workspace. See [Searching, finding, and sorting content in Power BI service](#).

### Access

You can print dashboards, reports, and visuals from reports in Power BI to produce a physical copy. You can't print entire reports; you can only print one page at a time. To do this, go to a report, use the search field to find specific data, and then print that page. See [Printing from Power BI service](#).

### Delete

To delete dashboards, reports, and workbooks, see [Delete almost anything in Power BI service](#).

Deleting a dashboard, report, or workbook doesn't delete the underlying dataset. Because Power BI relies on a live connection to the underlying source data to be complete and accurate, deleting personal data must be done there. (For example, if you created a Power BI report that is connected to Dynamics 365 for Sales as the live data



source, you would have to make any corrections to the data in Dynamics 365 for Sales.)

After the data is deleted, you can use the [scheduled data refresh](#) capabilities in Power BI to update the dataset that is stored in Power BI, after which the deleted data will no longer be reflected in any Power BI reports or dashboards that used that data. To help comply with GDPR requirements, you should have policies in place to ensure that you are refreshing your data at an appropriate cadence.

### Export

To facilitate a data portability request, you can export dashboards and reports in Power BI:

- You can export the underlying data for dashboards and reports to a static Excel file. See the video in [Printing from Power BI service](#). Using Excel, you can then edit the personal data to be included in the portability request, and save it in a commonly used, machine-readable format such as .csv or .xml.
- You can export (download) a report from the Power BI service in Office 365 to a .pbix file if it was originally published using Power BI Desktop. You can then import this file to Power BI Desktop and publish (export) it to the Power BI service of another organization. See [Export a report from Power BI service to Desktop](#).

### PowerApps

The following sections explain how to use the in-app functionality in Microsoft Power Apps to find, access, export, and delete personal data. These steps outline how an admin can transition apps and their dependent resources to new owners to limit business disruption.

#### Discover

PowerApps is a service for building apps that can be shared and used within your organization. As a part of the process of building or running an app, a user ends up storing several types of resources and data in the PowerApps service, including apps, environments, connections, custom connectors, and permissions.

To help facilitate a DSR request related to PowerApps, you can use the administration operations exposed in the [PowerApps Admin Center](#) and [PowerApps Admin PowerShell cmdlets](#). Access to these tools requires an account with the following permissions:

- A paid PowerApps Plan 2 license or a PowerApps Plan 2 trial license. You can sign up for a 30-day trial license [here](#).
- [Global administrator](#) or
- [Azure Active Directory global administrator](#)

For more information about finding personal data, see [Discover PowerApps personal data](#).

The PowerApps service also includes the Common Data Service For Apps, which enables users to store data in standard and custom entities within a Common Data Service database. You can view the data stored in these entities from the [PowerApps Maker portal](#), and use the in-product search capabilities of [Advanced Find](#) to search for specific data in the entity. For more information around discovering personal data in the Common Data Service, see [Discover Common Data Service personal data](#).

#### Access

Admins have the ability to assign themselves privileges to access and run the apps and associated resources (including flows, connections, and custom connectors) using the [PowerApps Admin Center](#) or [PowerApps Admin PowerShell cmdlets](#).

After you have access to the user's app, you can use a web browser to open the app. After you open an app, you can take a screenshot of the data. See [Use PowerApps in a web browser](#).

#### Delete

Because PowerApps allow users to build line-of-business application that can be a critical part of your organization's day-to-day operations, when a user leaves your organization and their Office 365 account is deleted, the admin needs to determine whether to delete the apps owned by the user or reassign to new owners. This is to help your organization transition apps to new owners and avoid any disruption to your

business for apps that may be used for shared business processes.

For shared data, like apps, admins must decide whether to permanently delete that user's shared data or keep them by reassigning the data to themselves or someone else within their organization. See [Delete PowerApps personal data](#).

Any data that was stored by a user in an entity in a Common Data Service For Apps database will also need to be reviewed and (if desired) deleted by an admin using the in-product capabilities. See [Delete Common Data Service user personal data](#).

#### **Export**

Admins have the ability to export personal data stored for a user within the PowerApps service using the [PowerApps Admin Center](#) and [PowerApps Admin PowerShell cmdlets](#). See [Export PowerApps personal data](#).

You can also use the in-product search capabilities of [Advanced Find](#) to search for a user's personal data in any entity. For details about exporting personal data in the Common Data Service, see [Export Common Data Service personal data](#).

#### **Connections and custom connectors in PowerApps**

Connections require users to provide credentials to connect to APIs, SaaS applications, and custom developed systems. These connections are owned by the user that established the connection and can be [managed](#) in-product. After PowerApps have been reassigned, an admin can use PowerShell cmdlets to list and delete these connections as part of deleting user data.

Custom connectors allow organizations to extend the capabilities of PowerApps by connecting to systems where an out-of-box connector is not available. A custom connector author can [share](#) their connector with others in an organization. After receiving a DSR deleting request, an admin should consider reassigning ownership of these connectors to avoid business disruption. To expedite this process, an admin can use PowerShell cmdlets to list, reassign, or delete custom connectors.

#### **Project Online**

The following sections explain how to use the in-app functionality in Microsoft Project Online to find, access, export, and delete personal data.

##### **Discover and access**

You can use Content Search to search the SharePoint Online site that's associated with a Project (when a Project is first created, there's an option to create an associated SharePoint Online site); Content Search doesn't search the data in an actual project in Project Online, only the associated site. Though Content Search searches for metadata about projects such as people mentioned in the subject) However, this may help you find (and access) the Project that contains the data related to the DSR.

##### **TIP**

The URL for the site collection in your organization where sites associated with Projects is

`https://<your org>.sharepoint.com/sites/pwa`; for example, <https://contoso.sharepoint.com/pwa>. You can use this specific site collection as the location of your content search and then the name of the Project in the search query.

Additionally, an IT admin can use the Site Collections page in the SharePoint admin center to get a list of PWA site collections in the organization.

##### **Delete**

You can delete information about a user from your Project Online environment. See [Delete user data from Project Online](#).

##### **Export**

You can a specific user's content from your Project Online environment. This data is exported to multiple files in the JSON format. For step-by instructions see, [Export user data from Project Online](#). For detailed information

about the files that are exported, see [Project Online export json object definitions](#).

## **Publisher**

The following sections explain how to use the in-app functionality in Microsoft Publisher to find, access, export, and delete personal data.

### **Discover**

You can use the in-app search feature to find text in a Publisher file the same way as you can in most Office applications. See [Find and replace text](#).

### **Access**

After you find data, you can take a screenshot of it or copy and paste it into a Word or text file and provide that to the data subject. You can also save a publication as a Word, PDF, or XPS file. See:

- [Save a publication as a Word document](#)
- [Save As or convert a publication to .pdf or .xps using Publisher](#)

### **Export**

You can provide a data subject with the actual Publisher file or as previously explained, you can save a publication as a Word, PDF, or XPS file. See:

- [Save a publication as a Word document](#)
- [Save As or convert a publication to .pdf or .xps using Publisher](#)

### **Delete**

You can delete content from a publication, delete entire pages, or delete an entire Publisher file. See [Add or delete pages](#).

## **Stream**

The following sections explain how to use the in-app functionality in Microsoft Stream to find, access, export, and delete personal data.

### **Discover**

To discover content that is generated or uploaded to Stream that may be relevant to a data subject request, a Stream admin can run a user report to determine what videos, video descriptions, groups, channels, or comments a Stream user may have uploaded, created, or posted by a user. For instructions on how to generate a report, see [Managing user data in Microsoft Stream](#). The report output is in HTML format and contains hyperlinks that can be used to navigate to videos of potential interest. If you would like to view a video that has custom permission set and you are not part of the original users for whom the video was intended, you can view in admin mode, See [Admin capabilities in Microsoft Stream](#).

### **Access**

Depending on the nature of the data subject request, a copy of the report described above can be used help satisfy a data subject request. The user report includes the Stream user's name and unique ID, a list of videos the user uploaded, a list of videos the user has access to, a list of channels the user created, a list of all the groups the user is a member of, and a list of all comments the user left on videos. The report further shows whether the user viewed each video listed in the user report. If you would like to provide the data subject with access to a video to satisfy a DSR request, you can share the video.

### **Export**

See the Access section for Stream.

### **Delete**

To delete or edit videos or any other Stream content, a Stream admin can select view in admin mode to perform the necessary function. See [Admin capabilities in Microsoft Stream](#). If a user has left the organization and would like to have their name removed from appearing next to videos that they uploaded, you can remove their name or replace it with another. See [Managing deleted users in Microsoft Stream](#).

## Sway

The following sections explain how to use the in-app functionality in Microsoft Sway to find, access, export, and delete personal data.

### Discover

Content created using Sway (found at [www.sway.com](http://www.sway.com)) can only be seen by the owner and those that the author has permitted to view the Sway. See [Privacy Settings in Sway](#). To determine whether Sway is a place where personal data responsive to your DSR is likely to reside, you can ask the Data Subject and organizational users who are likely to have generated content about the Data Subject to search their Sways and share with you any Sways that are likely to contain personal data responsive to the Data Subject's request. For information on how to share a Sway, see "Share a Sway from your Organizational Account" in this [Share your Sway](#) article.

### Access

If you have found personal data in a Sway that you would like to share with the Data Subject, you can provide the Data Subject with access to the data through one of several means. You can provide the Data Subject a copy of the online version of Sway (as described above); you can take screenshots of the relevant portion of the Sway that you would like to share; or you can print or download the Sway to Word or convert it to a PDF. How to download a Sway is further described in the "export" section below.

### Delete

To learn how to delete a Sway, go to the "How do I delete my Sway?" section in [Privacy settings in Sway](#).

### Export

To export a Sway, open the Sway that you would like to download, select the series of dots (ellipsis) in the upper right corner, select **Export**, and then choose either **Word** or **PDF**.

## Whiteboard

The following sections explain how to use the in-app functionality in Microsoft Whiteboard to find, access, export, and delete personal data.

- [Whiteboard 2016 on Surface Hub](#)
- [Whiteboard on all other platforms](#)

### Whiteboard 2016 on Surface Hub

This section describes responding to DSR requests for data created using the built-in Whiteboard 2016 app on Surface Hub.

#### Discover

Whiteboard files (.wbx files) are stored in users' OneDrive for Business account. You can ask the data subject or other users if whiteboards they created may contain personal data responsive to a DSR request. They can share a whiteboard with you, or you can get a copy of it to give to the data subject.

To access and transfer whiteboards:

1. Give yourself access to the user's OneDrive for Business account. See the "Get access to the former employee's OneDrive for Business documents" section in [Get access to and back up a former user's data](#).
2. Go to the Whiteboard App Data folder in the user's OneDrive for Business account and copy the .wbx files of the whiteboards that you want to transfer.
3. Give yourself access to the data subject's OneDrive for Business account, and then go to Whiteboard App Data folder.
4. Paste the .wbx files that you copied in the previous step.

#### Access

If you find personal data in a whiteboard that's responsive to a DSR access request, you can provide the data subject access to a whiteboard in several ways:

- Take screenshots of the relevant portions of a whiteboard.

- Upload a copy of the .wbx file to the data subject's OneDrive for Business account. See the previous section for steps on accessing and transferring .wbx files.
- Export a copy of whiteboard as a .png file.

#### Export

If you've obtained a copy of a whiteboard, you can export it.

1. Launch Whiteboard on the Surface Hub.
2. Tap the Share button and then select Export a copy. You can export a whiteboard to a OneNote (.one) file or to an image (.png) file.

#### Delete

You can give yourself access to the user's OneDrive for Business account and then delete the whiteboards.

1. Give yourself access to the data subject's OneDrive for Business account. See the "Get access to the former employee's OneDrive for Business documents" section in [Get access to and back up a former user's data](#)
2. Go to the Whiteboard App Data folder and then delete the contents of this folder.

#### Whiteboard for PC, Surface Hub, and other platforms

If an admin receives a DSR request for data in the new Whiteboard app, they can use Whiteboard PowerShell to add themselves (or other users) as an owner of a user's whiteboards. This enables an admin to perform actions including accessing, exporting, and deleting whiteboards. Use either the **Set-WhiteboardOwner** cmdlet to add yourself or another user as the owner of a whiteboard or use the **Invoke-TransferAllWhiteboards** cmdlet to transfer the ownership of all whiteboards for a specific user to a new owner. For information about using these cmdlets and installing the Whiteboard PowerShell module, see [Microsoft Whiteboard cmdlet reference](#). After you or another person has ownership of a whiteboard, see [Microsoft Whiteboard cmdlet reference](#).

After you or another person has ownership of a whiteboard, see the [Whiteboard support article](#) for detailed guidance about accessing, exporting, and deleting whiteboards.

#### Yammer

The following sections explain how to use the in-app functionality in Microsoft Yammer to find, access, export, and delete personal data.

##### Discover

From the Yammer admin center, a Yammer verified admin (global admin or verified admin set up in Yammer) can export data pertaining to a given user. The export includes the messages and files posted and modified by the user, and information about topics and groups created by the user. When a user-specific data export is run, the admin will also receive an inbox message with the user's account activity data that they can provide to the user if they so choose. For detailed instructions, see [Yammer Enterprise: Privacy](#).

User-specific exports are for a single network, so if the user is in an external Yammer network, the admin must export data for that external network, and for the home network.

To access data not included in data export, screenshots can be taken for the user's profile, settings, group memberships, bookmarked messages, followed users, and followed topics. Users or admins can collect this information. For more information, see [Yammer Enterprise: Privacy](#).

##### Access

You can view data in the exported files, including the full text of messages and the contents of files. You can also select links in the exported files to go directly to the posted messages and files in Yammer, and to groups, and topics the user created, messages the user liked, messages where the user is @mentioned, polls the user has voted on, and links the user has added.

Per-user data export does not include:

- The user's profile:

- If the user has a Yammer identity, the user has full control of their profile. For information on how to view and modify the profile, see [Change my Yammer profile and settings](#).
- If the user has an Office 365 identity, the Yammer user profile is pulled automatically from Office 365, which gets the profile information from Azure Active Directory (AAD). Yammer users can temporarily change their profiles in Yammer, but these changes are overwritten when there is a change in AAD, so you must view and change directory data in AAD. See [Manage Yammer users across their lifecycle from Office 365](#) and [Add or change profile information for a user in Azure Active Directory](#).
- The user's settings:
  - The user can view and change their own settings. For information on how to view and modify user settings, see [Change my Yammer profile and settings](#). An admin can view this information and take screenshots, but can't change it. Go to Yammer settings > **People**, and then select the name of the user.
    - The user's group membership, bookmarked messages, followed users, and followed topics.
    - The user can view this information. For information on how, see [Tips for staying organized in Yammer](#). An admin can view this information and take screenshots, but can't change it. Go to Yammer settings > **People**, and then select the name of the user.

### Export

For instructions for how to export data, see [Manage GDPR data subject requests in Yammer Enterprise](#). You must run a per-user export for each Yammer network the user is a member of.

Yammer has data retention settings that either soft-delete or hard-delete data when a user deletes a message or file. If this is set to soft-delete, data a user has deleted will be included in the export. If the Yammer data retention setting is set to hard-delete, the deleted information is no longer stored in Yammer, so will not be included in the export.

### Delete

Yammer allows verified admins to execute a GDPR-compliant delete via the Yammer admin center if they receive a DSR. This option is called Erase User, and it suspends the user for 14 days and then removes all their personal data, excluding files and messages. If the user is a guest user, this must be done for each external network the guest is a member of.

#### NOTE

If an admin wants to remove the files and messages of a user during the 14-day window, they will have to perform a user level export to identify the files and messages, and then decide which ones to delete either by in-product deletion or by using a PowerShell script. After the 14-day window, the admin can no longer associate the user with their files or messages.

When a user is deleted with the Erase User option, notification is sent to the Yammer Inbox of all network admins and verified admins. The Erase User option deletes the user's Yammer profile, but does not delete their Office 365 or Azure Active Directory profile.

For detailed steps to remove a user, see [Manage GDPR data subject requests in Yammer Enterprise](#).

## Responding to DSR rectification requests

If a data subject has asked you to rectify the personal data that resides in your organization's data stored in Office 365, you and your organization have to determine whether it's appropriate to honor the request. If you choose to honor the request, then rectifying the data may include taking actions such as editing, redacting, or removing personal data from a document or other type or item. The most expedient way to do this is to ask the

data/document owner to use the appropriate Office 365 application to make the requested change. An alternative is to have an IT admin in your organization make the change. This will probably require the IT admin (or other people in your organization with the appropriate privileges, such as a SharePoint Online site collection administrator) to assign to themselves or someone else working on the DSR the necessary permissions to gain access to the document or the content location where the document is located to make the change directly to the document.

### **Requesting that the data owner to make the approved change**

The most direct way to rectify personal data is to ask the data owner to make the change. After you locate the data that is the subject of the DSR, you can provide the following information so that they can make the change.

- The location and file name (for documents and other files) of the item that needs to be changed. Locating the data in question is part of the discovery process [discovery process](#) that was previously explained.
- The approved change the data owner should make

You may want to consider implementing a confirmation process where you or another person involved in the DSR investigation verifies that the requested change has been made.

### **Gaining access to a SharePoint Online site or OneDrive for Business account to make changes**

If it's not feasible for the data owner to implement the data subject's request for rectification, an IT admin or SharePoint admin in your organization can get access to the content location and make the required changes. Or, an admin can assign you or another data privacy officer the necessary permissions.

#### **SharePoint Online**

To assign administrator or owner permissions to a SharePoint Online site so that you or someone else can access and edit that document, see

- [Manage administrators for a site collection](#)
- [Edit and manage permissions for a SharePoint list or library](#)

#### **OneDrive for Business**

A global admin can access a user's OneDrive for Business account by using the .

1. Sign in to Office 365 with your global admin credentials.
2. Go to the admin center.
3. Go to **Active users** and select the user.
4. Expand **OneDrive for Business Settings** in the details pane, and then select **Access files**.
5. select the URL to go to the user's OneDrive for Business account.

### **Gaining access to an Exchange Online mailbox to make changes to data**

A global admin can assign themselves the permissions necessary to open and edit (or delete) items in another user's mailbox, as if they were the mailbox owner. A global admin can also assign these permissions to another user. Specifically, the global admin needs to add the **Read and manage** permission, which is the Full Access permission in Exchange Online. For details, see:

- [Give mailbox permissions to another user in Office 365](#)
- [Access another person's mailbox](#)

If the user mailbox is placed on a legal hold or has been assigned to a retention policy, all versions of a mailbox are retained until the retention period expires or the hold is removed from the mailbox. That means if a mailbox item is changed in response to DSR rectification request, a copy of original item (before the change was made) is retained and stored in a hidden folder in the Recoverable Items folder in the user's mailbox.

### **Making changes to content in OneDrive for Business and SharePoint Online**

Admins or data owners can make changes to SharePoint Online documents, lists, and pages. Keep the following

things in mind when making changes to SharePoint content:

- Updating a document saves a new version of the document, which will contain the revision. Older versions of the document will not be updated. That means it's possible that the data that's the subject of a DSR rectification request may persist in older versions of the topic. Older versions of a topic can be deleted and then permanently removed from Office 365. See the [Deleting documents in SharePoint Online and OneDrive for Business](#) section in this guide.
- To completely redact a SharePoint file in a way that removes all traces of a data subject from the file, including all versions of the file and all recorded activity performed by the data subject, you have to perform the following steps:
  1. Download a copy of the file to your local computer.
  2. Permanently delete the file from SharePoint Online, by deleting the file, and then deleting it from the first-stage and second-stage Recycle Bin. See the [Deleting documents in SharePoint Online and OneDrive for Business](#) section in this guide.
  3. Make the revisions to the copy of the document on your local computer.
  4. Upload the revised file to the original SharePoint Online location.
- Data in SharePoint lists can be edited. See [Add, edit, or delete list items](#).

IT admins can also correct certain personal properties associated with a document:

User information from the SharePoint User Profile or Office 365 is often associated with OneDrive for Business and SharePoint Online documents to represent that person. For example, a user's name in a Created By or Modified By People column for a document or list item. This user information can be rectified in several ways, depending on the source:

- Rectify user properties in their own on-premises Active Directory. For customers syncing user properties such as user Display Name, First Name, etc. from an on-premises AD, those properties should be rectified there. Appropriately mapped properties flow into Office 365, and then OneDrive for Business and SharePoint Online.
- Rectify user properties in the admin center. Changes made to account information there will automatically be reflected in OneDrive for Business and SharePoint Online experiences. For info, see [Add or change profile information for a user in Azure Active Directory](#). For properties sourced in Office 365, no changes can be made on the SharePoint side.
- Rectify user properties in the SharePoint user profile experience of the SharePoint admin center. In the user profiles tab of the SharePoint admin center, admins can select **Manage user profiles**, and look up any user's properties. Then they can choose to Edit the user's properties.
- Rectify user properties in a custom source. Custom SharePoint profile properties may be syncing from a custom source via Microsoft Identity Manager (MIM) or another method.

This won't affect all experiences, which may retain the older information. For example, the user's name as text in the document.

### **Making changes to content in Power BI**

Power BI relies on the underlying source data used in its dashboards and reports to be complete and accurate, so correcting inaccurate or incomplete source data must be done there. For example, if you created a Power BI report that is connected to Dynamics 365 for Sales as the live data source, you would have to make any corrections to the data in Dynamics 365 for Sales.

After those changes are made, you can take advantage of the [scheduled data refresh](#) capabilities to update the dataset that is stored in Power BI so that the revised data is reflected in the dependent Power BI assets. To help comply with GDPR requirements, you should have policies in place to ensure that you are refreshing your data at an appropriate cadence.



## Making changes to content in Yammer

For messages, a user can edit a given message to rectify any inaccuracies. They can request a list of all their messages from a Yammer verified admin, and then select a link in the file to review each message.

For files, a user can edit a given file to rectify any inaccuracies. They can request a list of all the files they posted from a Yammer verified admin, and then access the files in Yammer. Files that are exported into the Files folder can be viewed by searching for the file by number. For example, for a file named 12345678.ppx in the export, use the Search box in Yammer to search for 1235678.ppx. Or, go to

[https://www.yammer.com/<network\\_name>/#/files/<file\\_number>](https://www.yammer.com/<network_name>/#/files/<file_number>); for example, <https://www.yammer.com/contosomkt.onmicrosoft.com#/files/12345678>.

For data that the user can access through their profile and settings, the user can make any needed changes.

- The user's profile:
  - If the user has a Yammer identity, the user has full control of their profile. For information on how to view and modify the profile, see [Change my Yammer profile and settings](#).
  - If the user has an Office 365 identity, the Yammer user profile is pulled automatically from Office 365, which gets the profile information from Azure Active Directory (AAD). Yammer users can temporarily change their profiles in Yammer, but these changes are overwritten when there is a change in AAD, so the best place to view and change directory data is AAD. The user needs to request that AAD be updated. See [Manage Yammer users across their lifecycle from Office 365](#) and [Add or change profile information for a user in Azure Active Directory](#).
- The user's settings:
  - The user can change their own settings. For information on how to view and modify user settings, see [Change my Yammer profile and settings](#).
  - The user's group membership, bookmarked messages, followed users, and followed topics. The user can change this information; see [Tips for staying organized in Yammer](#).

## Responding to DSR restriction requests

Here are the ways to restrict the processing of data in Office 365:

- Remove an Office 365 application license to prevent users from accessing data via an application
- Prevent users from accessing their OneDrive for Business account
- Turn off an Office 365 service from processing the data
- Temporarily remove the data from SharePoint Online and OneDrive for Business and retain it on-premises
- Temporarily restrict all access to a SharePoint Online site
- Prevent a user from signing in to Office 365

If your organization determines later that a restriction no longer applies, you can end the restriction by reversing the steps you took to restrict it; such as reassigning licenses, turning a service back on, or allowing a user to sign in to Office 365.

### Removing the license for an Office 365 application

As previously explained, licenses for all Office 365 applications that are included in your organization's Microsoft 365 for business subscription are assigned to all users by default. If necessary to restrict, access to data that's subject to a DSR, an IT admin can use the Office 365 admin portal temporarily turn off a user's license for an application. If a user then tries to use that application, they'll receive an unlicensed product notification or a message saying they no longer have access. For details, see [Remove licenses from users in Office 365 for business](#).

**Notes:**

- To restrict a user from accessing Yammer, you must first [enforce Office 365 identify for a Yammer user](#) and then remove the user's Yammer license.
- For scenarios that take advantage of Power BI Embedded, you can restrict access to the independent software vendor (ISV) application that the content is embedded in.

### Preventing users from accessing their OneDrive for Business account

Removing a user's SharePoint Online license won't prevent them from accessing their OneDrive for Business account if it exists. You have to remove the user's permissions to their OneDrive for Business account to. You can do this by removing the user as a site collection owner of their OneDrive for Business account. Specifically, you have to remove the user from the Primary Site Collection Administrator and Site Collection Administrators groups in their user profile. See the "Add and remove admins on a OneDrive for Business account" section in [Manage user profiles in the SharePoint admin center](#).

### Turning off an Office 365 Service

Another way to address a DSR request to restrict the processing of data is to turn off an Office 365 service. This impacts all users in your entire organization and prevents everyone from using the service or accessing data in the service.

The most expedient way to turn off a service is to use Office 365 PowerShell and remove the corresponding user license from all users in the organization. This will in effect restrict anyone from access data in that service. For detailed instructions, see [Disable access to services with Office 365 PowerShell](#) and follow the procedures to disable Office 365 services for users from a single licensing plan.

#### NOTE

For Yammer, in addition to removing the Yammer license from user accounts, you also must disable users' ability to sign in to Yammer with Yammer credentials (by enforcing the use of their Office 365 credentials when signing in). For detailed instructions, see [Turn off Yammer access for Microsoft 365 users](#).

### Temporarily removing data from SharePoint Online or OneDrive for Business sites

Another way to restrict the processing of personal data is to temporarily remove it from Office 365 in response to a DSR. When your organization determines that the restriction no longer applies, you can import the data back into Office 365.

Because most Office documents are on a SharePoint Online or OneDrive for Business site, here's a high-level process for removing documents from sites and then re-importing them.

1. Get a copy of the document that is the subject of the restriction request. You may have to request either access to the site or ask a global admin or a site collection administrator to provide you with a copy of the document.
2. Store the document in an on-premises location (such as a file server or a file share) or another location other than your Office 365 tenant in the Microsoft cloud.
3. Permanently delete (purge) the original document from Office 365. This is a 3-step process:
  - a. Delete the original copy of the document. When you delete a document from a site, it's sent to the site Recycle Bin (also called the *first-stage Recycle Bin*).
  - b. Go to the site Recycle Bin and delete that copy of the document. When you delete a document from the site Recycle Bin, it's sent to the site collection Recycle Bin (also called the *second-stage Recycle Bin*). See [Delete a file, folder, or link from a SharePoint document library](#).
  - c. Go to the site collection Recycle Bin and delete that copy of the document, which permanently removes it from Office 365. See [Delete items from the site collection recycle bin](#).

4. When the restriction no longer applies, the copy of the document that was stored on-premises can be re-uploaded to the site in Office 365.

#### **IMPORTANT**

The preceding procedure won't work if the document is located on a site that is on hold (with one of the retention or legal hold features in Office 365). In the case where a restriction request for a DSR takes precedence over a legal hold, the hold would have to be removed from the site before a document could be permanently deleted. Additionally, the document history for deleted documents is permanently removed.

### **Temporarily restricting access to SharePoint Online sites**

A SharePoint Online administrator can temporarily prevent all users from accessing a SharePoint Online site collection by locking the site collection (by using the **Set-SPOSite -LockState** command in SharePoint Online PowerShell). This prevents users from accessing the site collection and any content or data that's located in the site. If you then determine that users should be able to access the site, the administrator can unlock the site. See [Set-SPOSite](#) for information about running this PowerShell cmdlet.

### **Preventing a user from signing in to Office 365**

An IT admin can also prevent a user from signing into Office 365, which would prevent the user from accessing any Office 365 online service or processing any data stored in Office 365. See [Block a former employee's access to Office 365 data](#).

## Part 2: Responding to DSRs with Respect to Insights Generated by Office 365

The Microsoft suite of Office 365 services includes online services that provide insights to users and organizations that have opted to use them.

- Delve and MyAnalytics provide insights to individual users
- Workplace Analytics provides insights to organizations.

These services are described in the following sections:

### **Delve**

In Delve, users can manage their Office 365 profile and discover people and documents that may be relevant to them. Users can only see documents that they have access to. For a series of helpful articles about Delve, see [Office Delve](#).

#### **Access and export**

Admins can't access or export a users' Delve data. This means that users have to access and export Delve data themselves. Most of the data types can be accessed and exported directly from Delve, but some data types are only available through other services.

#### **Data available in the Delve user interface**

- **Profile data:** This is the profile information from your organization's Global Address List in Azure Active Directory, and optional information that users have chosen to add about themselves. To access or export profile data in Delve, a user can select **Me > Update profile**. They can either copy the content directly from the page or
- **Blog data:** This is blog posts published by a user. To access or export blog data, a user can select **Me > All posts**. They can either copy the content directly from the page or take a screenshot.
- **Recent people data:** These are the people in the organization that Delve has inferred are most relevant to the user at a given time. When a user selects **Me > See all** in the "select a person to see what they're working on" pane, Delve shows the most relevant people for a user at a given time.

#### **Data available through an export link in Delve**

- **People list data:** These are the people the user has viewed in Delve. The **People** list is shown in the left pane on the home page. Users can export the list of people they have most recently viewed in Delve.
- **Favorites data:** These are boards and documents that the user has marked as their favorite. The **Favorites** page shows boards and documents that the user has added to their favorites. Users can export a list of their current favorite boards and documents.
- **Feature settings data:** These are Delve configurations or actions that result from a user's use of Delve. Users can export a full list of these settings.

To access or export the above data, the user can select the gear icon in the upper-right corner in Delve, and then select **Feature settings > Export data**. Information is exported in JSON format.

#### Data that's available through other services

- **Popular documents data:** These are documents and email attachments that may be relevant to the user. Delve dynamically organizes these documents and email messages based on the user's activities and people they work with in Office 365. When a user opens Delve or selects **Home**, Delve shows the most relevant documents or attachments for the user at a given time. To access or export the actual documents and attachments, the user can go to the Office 365 service through which the document or attachment was made available (such as Office.com, SharePoint Online, OneDrive for Business, or Exchange Online).
- **Recent documents and email attachments data:** These are the most recent documents and email attachments that the user has modified. When a user selects **Me > See all** in the "Get back to your recent documents and email attachments" pane, Delve shows the latest documents and email attachments the user has modified at a given time. To access or export the actual documents and attachments, the user can go to the Office 365 service through which the document or attachment was made available; for example, Office.com, SharePoint Online, OneDrive for Business, or Exchange Online.
- **Documents from people around your data:** These are the documents that Delve has inferred are most relevant to the user at a given time. When a user selects **Me > See all** in the "Discover documents from people around you" pane, Delve shows the most relevant documents for a user at a given time. To access or export the actual documents, the user can go to the Office 365 service through which the document or attachment was made available (for example, Office.com, SharePoint Online, OneDrive for Business, or Exchange Online).

#### Rectify

Users can modify the following information in Delve:

- **Profile information:** A user can select **Me > Update profile** to update their information. Depending on your organization's settings in the Global Address List, users may not be able to modify all their profile information, such as their name or job title.
- **Feature settings:** A user can select the gear icon in the upper-right corner in Delve, and then select **Feature settings >** to change the desired settings.

#### Restrict

To restrict processing in Delve for your organization, you can turn off the Office Graph. Learn more [here](#).

#### Delete

Users can delete the following information in Delve:

- **Profile information:** To delete profile information, a user can select **Me > Update profile** and either delete free-form text. Depending on your organization's settings in the Global Address List, users may not be able to delete all their profile information, such as their name or job title.
- **Documents and email attachments:** To delete a document or attachment, users must go to the service where the document or attachment is stored (such as SharePoint Online, OneDrive for Business, or Exchange Online) and delete the document there.

#### MyAnalytics

MyAnalytics provides statistics to users to help them understand how they spend their time at work. To help

your users better understand the data that is presented to them in their personal dashboard and how that data is calculated, direct your users to [MyAnalytics personal dashboard](#).

#### **Access and export**

If your organization uses MyAnalytics, then Microsoft generates insights for all users. All MyAnalytics insights are derived from email and meeting headers in the user's mailbox. Users can go to the [MyAnalytics dashboard](#) while signed in to their Office 365 account to view the insights that are generated about how they spend their time at work. They can take screenshots of MyAnalytics insights if they want to have permanent copies of their information.

#### **Rectify**

All insights generated by MyAnalytics are derived from the user's mail and calendar items. Therefore, there is nothing to rectify other than the source email or calendar items.

#### **Restrict**

To restrict processing for a specific user, you can opt them out of MyAnalytics. To see how, see [Configure MyAnalytics user settings](#).

#### **Delete**

All mailbox content, including MyAnalytics data, is purged when a user account is "hard-deleted" from Active Directory. For more information, see the [Deleting a user](#) section in this guide.

### **Workplace Analytics**

Workplace Analytics allows organizations to augment Office 365 data with their own business data to gain insights about organizational productivity, collaboration patterns, and employee engagement. [This article](#) explains the control that your organization has over the data that Workplace Analytics processes and who has access to that data.

To assist you with DSRs in Workplace Analytics:

1. Determine whether your organization is using Workplace Analytics. For more information, see [Assign licenses to users](#). If your organization is not using Workplace Analytics, there is no further action.
2. If your organization is using Workplace Analytics, then see who in your organization has been assigned to the role of Workplace Analytics administrator. You should also determine if the data subject's mailbox is licensed for Workplace Analytics. If necessary, have your Workplace Analytics administrator contact Microsoft Support in handling the following DSR requests:

#### **Access and export**

Workplace Analytics insight reports created by you may or may not contain personal data of users that your organization licensed for Workplace Analytics, depending on the information that your organization used to supplement the Office 365 data. Your Workplace Analytics administrator needs to review those reports to determine if they contain a user's personal data. If a report does contain a user's personal data, then you need to decide if you want to provide a copy of that report to the user. Workplace Analytics allows you to export the report.

#### **Rectify**

As explained above, Workplace Analytics uses Office 365 data with the organizational data that you provide to generate reports of interest to you. The Office 365 data can't be rectified; it's based on a user's email and calendar activities. However, the organizational data that you have uploaded into Workplace Analytics to generate the report can be rectified. To do this, you need to correct the source data, upload it, and rerun the report to generate a new Workplace Analytics report.

#### **Restrict**

To restrict processing for a specific user, you can remove their Workplace Analytics license.

#### **Delete**

If a data subject would like to be removed from a Workplace Analytics report or set of reports, you can delete

the report. It is your responsibility to delete users from any organizational data that you used to generate the report, and reupload the data. All data about the user is removed when a user account is "hard-deleted" from Azure Active Directory.

To remove the personal data of a data subject, a global administrator can take the following steps:

1. Remove the Workplace Analytics license from the data subject.
2. Delete the Azure Active Directory (AAD) entry for the data subject. (For more information, see [Delete a user](#).)
3. Contact support and have support open a ticket for a Data Subject Rights (DSR) user-delete request. In this ticket, identify the data subject by using their User Principal Name (UPN).
4. Export a copy of the HR data from the company's HR system (see [Export data](#)), remove the data subject's information from that HR data file, and then upload the edited HR data file in .csv format into Workplace Analytics (see [Upload organizational data](#)).

## Part 3: Responding to DSRs for system-generated Logs

Microsoft also provides you with the ability to access, export, and delete system-generated logs that may be deemed personal under the GDPR's broad definition of "personal data." Examples of system-generated logs that may be deemed personal under GDPR include:

- Product and service usage data such as user activity logs
- User search requests and query data
- Data generated by product and services as a product of system functionality and interaction by users or other systems

The ability to restrict or rectify data in system-generated logs is not supported. Data in system-generated logs constitutes factual actions conducted within the Microsoft cloud and diagnostic data, and modifications to such data would compromise the historical record of actions and increase fraud and security risks.

### Accessing and exporting system-generated logs

The tenant admin is the only person within your organization who can access system-generated logs associated with a particular user's use of Office 365 services and applications. The data retrieved for an export request will be provided in a machine-readable format and will be provided in files that will allow the user to know which services the data is associated with. As noted above, the data retrieved will not include data that may compromise the security or stability of the service.

To access and export system-generated logs:

1. Sign in to the Azure portal and select **All services**.
2. Type **policy** into the filter, and then select **Policy**.
3. In the **Policy** blade, select **User privacy**, select **Manage User Requests**, and then select **Add export request**.
4. Complete the **Export data request**:
  - **User**. Type the email address of the Azure Active Directory user that requested the export.
  - **Subscription**. Select the account you use to report resource usage and to bill for services. This is also the location of your Azure storage account.
  - **Storage account**. Select the location of your Azure Storage (Blob). For more info, see the [Introduction to Microsoft Azure Storage — Blob storage](#) article.
  - **Container**. Create a new (or select an existing) container as the storage location for the user's exported privacy data.
5. Select **Create**.

The export request goes into **Pending** status. You can view the report status on the **User privacy > Overview blade**.

#### **IMPORTANT**

Because personal data can come from multiple systems, it's possible that the export process might take up to one month to complete.

#### **Notify about exporting or deleting issues**

If you run into issues while exporting or deleting data from the Azure portal, go to the Azure portal **Help + Support** blade and submit a new ticket under **Subscription Management > Other Security and Compliance Request > Privacy Blade and GDPR Requests**.

#### **NOTE**

When you export data from the Azure portal, system-generated data for a few applications will not be exported. To export data for these applications, see [Additional steps to export system-generated log data](#).

The following summarizes accessing and exporting system-generated logs:

- **How long does an export request using the Azure portal take to complete a request?:** This can depend on several factors. Usually it should complete in one or two days, but it can take up to 30 days.
- **What format will the output be in?:** The output is structured machine-readable files such as XML, CSV, or JSON.
- **Who has access to Azure portal to submit access requests for system-generated data?:** Office 365 global administrators have access to the Azure portal.
- **What data do the export results return?:** The results contain system-generated logs that Microsoft stores. Exported data spans across various Microsoft services including Office 365, Azure, and Dynamics. The results do not include data that may compromise the security or stability of the service.
- **How is data returned to the user?:** Data is exported to your organization's Azure storage location; it's up to admins in your organization to determine how they will show/return this data to users.
- **What will system-generated log data look like?:** Below is an example, the data are in JSON format:

```
[{
  "DateTime": "2017-04-28T12:09:29-07:00",
  "AppName": "SharePoint",
  "Action": "OpenFile",
  "IP": "154.192.13.131",
  "DevicePlatform": "Windows 1.0.1607"
}]
```

Product and service usage data for some of Microsoft's most often-used services, such as Exchange Online, SharePoint Online, Skype for Business, Yammer, and Office 365 Groups can also be retrieved by searching the Office 365 audit log in the Security & Compliance Center. For more information, see [Use the Office 365 audit log search tool in DSR investigations](#) in Appendix A. Using the audit log may be of interest to you because it's possible to assign permissions to other people in your organization (such as your compliance officer) to search the audit log to access this data.

#### **Deleting system-generated logs**

To delete system-generated logs retrieved through an access request, you must remove the user from the

service and permanently delete their Azure Active Directory account. For instructions about permanently deleting a user, see the [Deleting a user section](#) in this guide. It's important to note that permanently deleting a user account is irreversible once initiated.

Permanently deleting a user account removes the user's data from system-generated logs, except for data that may compromise the security or stability of the service, for nearly all Office 365 services within 30 days.

One exception to this 30-day period is that the permanent deletion of the user account in Exchange Online takes longer than 30 days. This is due to the critical nature of Exchange Online content and to prevent accidental data loss. Exchange Online has been engineered to intentionally place data in a holding state for up to 60 days after a user account has been permanently deleted. To permanently delete a user's Exchange Online data in a 30-day time frame, permanently delete the user account in Azure Active Directory and then contact [Microsoft Support](#) and request that the user's Exchange Online data be manually removed outside the scheduled delete process. For more information, see [Removing Exchange Online data](#), which was previously explained in this guide.

Deleting a user's account will not remove system-generated logs for Yammer and Kaizala. To remove the data from these applications, see one of the following:

- Yammer - [Manage GDPR data subject requests in Yammer Enterprise](#)
- Kaizala - [Export or delete a user's organizational data in Kaizala](#)

#### **National clouds**

A global IT admin needs to do the following to export system-generated log data in the following national clouds:

- **Office 365 Germany:** Follow the steps above.
- **Office 365 US Government:** [Go to the Office 365 admin portal](#) and submit a request to Microsoft Support.
- **Office 365 operated by 21Vianet (China):** [Go to the Office 365 operated by 21Vianet admin portal](#) and then go to **Commerce > Subscription > Privacy > GDPR** and enter the required information.

## Part 4: Additional resources to assist you with DSRs

### **DSR guides for other Microsoft enterprise services**

This guide is dedicated to the topic of how to find and act on personal data to respond to DSRs when using Office 365 products, services, and administrative tools. Go to the [Microsoft Service Trust Portal](#) to access similar guides for other Microsoft enterprise services.

### **Microsoft Support**

"Support Data" is the data you and your users provide to Microsoft if your organization or your users engage with Microsoft to receive product support related to Office 365 or other Microsoft products and services (for example, to troubleshoot unexpected product behavior). Some of this data may contain personal data. For more information, see [Microsoft Support and Professional Services Data Subject Requests for the GDPR](#).

### **Product and services authenticated with an Org ID for which Microsoft is a data controller**

Parts 1–3 of this guide covers products and services for which Microsoft is a data processor to your organization, and thus DSR capability is made available to your tenant administrator. There are various circumstances where your organization's users may use their work or school account (also referred to as "Azure Active Directory ID" or "AAD") to sign in to Microsoft products and services for which Microsoft is a data controller. For all such products and services, your users need to initiate their own data subject requests directly to Microsoft and Microsoft will fulfill the requests directly to the user. By design, products and services involving storage of user-authored content enable users to access, export, rectify, and delete their user-authored content as part of the inherent functionality of the products. Scenarios where this may apply include the following:

- **Optional connected online services:** Microsoft 365 Apps for enterprise makes certain optional



connected online services available to the user. The list of services and related user controls are listed [here](#). You can decide whether you would like to allow your end users to use these services. For more information, see [How admins can manage controller services in Microsoft 365 Apps for enterprise](#). If these optional services process personal data, Microsoft is a data controller for these services.

- **User feedback:** If your users elect to provide feedback on Microsoft products and services, Microsoft is a data controller for such feedback to the extent it contains personal data. Microsoft fulfills any data subject requests for feedback collected by Microsoft (including feedback managed by Microsoft subprocessors) except in cases where Microsoft has instructed users not to include personal data during the feedback collection process. Exceptions: If Microsoft has instructed users not to include personal data during the feedback collection process, Microsoft relies on that instruction and will assume that no personal data has been provided. Users who have created a separate account with third-party feedback service providers need to fulfill their DSR directly with those providers.
- **Windows authenticated via work or school account:** If your organization has purchased Windows licenses, and your users authenticate to organization-provided Windows with their work or school account, Microsoft acts as a data controller.
- **User-acquired products or services:** If you allow your users, acting in their individual capacity, to acquire Microsoft products or services that use AAD for authentication (for example, Office add-ons or applications available in a Microsoft Store), Microsoft may be a data controller. For any such Microsoft products or services, users need to contact Microsoft directly to initiate a DSR.

#### **IMPORTANT**

If you delete a user as enabled via Azure Active Directory, your (former) user will lose the ability to sign in to any products or services for which he or she formerly relied upon for a work or school account. Additionally, Microsoft will no longer be able to authenticate the user in connection with a DSR request for products or services for which Microsoft is a data controller. If you wish to enable a user to initiate DSRs against such services, it is important you instruct your user to do so before you delete the user's AAD account.

#### **Personal accounts**

If your users have used Microsoft accounts (that is, personal accounts) to acquire products and services from Microsoft for their own use and for which Microsoft is a data controller, they may initiate DSR requests by using the [Microsoft privacy dashboard](#).

#### **Third-party products**

If your organization, or your users acting in their individual capacity, have acquired products or services from third parties and use their Microsoft work or school account for authentication, any data subject requests should be directed to the applicable third party.

## Appendix A: Preparing for DSR investigations

To help prepare your organization to undertake DSR investigations using Office 365 services, consider the following recommendations:

- Use the DSR eDiscovery case tool in the Security & Compliance Center to manage DSR investigations
- Set up Compliance Boundaries to limit the scope of Content Searches
- Use the audit log search tool in DSR investigations

#### **Use the DSR case tool to manage DSR investigations**

We recommend that you use the DSR case tool in Security & Compliance Center to manage DSR investigations. By using the DSR case tool, you can:

- Create a separate case for each DSR investigation.

- Use the built-in to search for all content related to a specific data subject. When you create a case and start the search, these content locations are searched:
  - All mailboxes in your organization (including the mailboxes associated with all Microsoft Teams and Microsoft 365 Groups)
  - All SharePoint Online sites and OneDrive for Business accounts in your organization
  - All Microsoft Teams sites and Microsoft 365 group sites in your organization
  - All public folders in Exchange Online
- Revise the default search query and rerun the search to narrow the search results.
- Control who has access to the case by adding people as members of the case; only members can access the case and are only able to see their cases in the list of cases on the DSR cases page in the Security & Compliance Center. Additionally, you can assign different permissions to different members of the same case. For example, you could allow some members to only view the case and the results of a Content Search and allow other members to create searches and export search results.
- Create export jobs to export the search results in response to a DSR export request. You can export all content returned by the Content Search. Other Office 365 data related to a data subject is also exported.
- Create export jobs to export the search results in response to a DSR export request. You can export all content returned by the Content Search. You can also export system-generated logs for Office Roaming service.
- Delete cases when the DSR investigation process is complete. This removes all the content searches and export jobs associated with the case.

To get started with using DSR cases, see [Manage GDPR data subject requests with the DSR case tool in the Security & Compliance Center](#).

#### **IMPORTANT**

An eDiscovery Administrator can view and manage all DSR cases in your organization. For more information about the different roles related to eDiscovery, see [Assign eDiscovery permissions to potential case members](#).

### **Set up Compliance Boundaries to limit the scope of Content Searches**

Compliance Boundaries are implemented by using the search permissions filtering functionality in the Security & Compliance Center. Compliance Boundaries create logical search boundaries within an organization that control/limit which content locations (for example Exchange Online mailboxes and SharePoint Online sites) that an IT admin or compliance officer can search. Compliance Boundaries are useful for multi-national organizations that need to respect geographical boundaries, governmental organizations that need to separate different agencies, and business organizations that segregated into business unit or department. For all these scenarios, Compliance Boundaries can be used in DSR investigations to limit which mailboxes and sites can be searched by people involved in the investigation.

You can use Compliance Boundaries together with eDiscovery cases to limit the content locations that can be searched in an investigation to those locations only within the agency or business unit.

Here's a high-level overview of how to implement Compliance Boundaries (together with eDiscovery cases) for DSR investigations.

1. Determine the agencies in your organization that will be designated as a compliance boundary.
2. Determine which user object attribute in Azure Active Directory will be used to define the compliance boundary. For example, you might choose the Country, CountryCode, or Department attribute, so that members of the admin role group that you create in the next step can only search the content locations of the users that have a specific value for that attribute. This is how you limit who can search for content in a

specific agency.

#### NOTE

Currently, you must perform an additional step for OneDrive for Business and file a Microsoft Support request to have the attribute synchronized to OneDrive for Business accounts.

3. Create an admin role group in the Security & Compliance Center for each compliance boundary. We recommend that you create these role groups by copying the built-in eDiscovery Manager role group and then removing any roles as necessary.
4. Add members to each of the specific role groups as eDiscovery Managers. Members are the people responsible for investigating and responding to DSRs, and will typically consist of IT admins, data privacy officers, compliance managers, and human resource representatives.
5. Create a search permissions filter for each compliance boundary so that the members of the corresponding admin role group can only search mailboxes and sites for users within that agency/compliance boundary. The search permissions filter allows members of the corresponding role group to search only the content locations with user object attribute value that corresponds to the agency/compliance boundary.

For step-by-step instructions, see [Set up compliance boundaries for eDiscovery investigations in Office 365](#).

#### Use the audit log search tool in DSR investigations

IT admins can use the audit log search tool in the Security & Compliance Center to identify documents, files, and other Office 365 resources that users have created, accessed, changed, or deleted. Searching for this kind of activity can be useful in DSR investigations. For example, in SharePoint Online and OneDrive for Business, auditing events are logged when users perform these activities:

- Accessed a file
- Modified a file
- Moved a file
- Uploaded or downloaded a file

You can search the audit log for specific activities, types of activities, activities performed by a specific user, and other search criteria. In addition to SharePoint Online and OneDrive for Business activities, you can also search for activities in Flow, Power BI, and Microsoft Teams. Auditing records are retained for 90 days. Therefore, you won't be able to search for user activities that occurred more than 90 days ago. For a complete list of audited activities and how to search the audit log, see [Search the audit log in the Security & Compliance Center](#).

#### TIP

To work around the 90-day limitation discussed above and maintain a running history of your organization's auditing records, you could export all activities on a recurring schedule (for example, every 30 days) to have a continuous record of your organization's auditing records.

## Appendix B: Change log

The following table lists the changes to the Office 365 DSR guide since its initial publication on May 25, 2018.

DATE	SECTION/APP	CHANGE
------	-------------	--------

DATE	SECTION/APP	CHANGE
9/18/2018	<a href="#">Whiteboard</a>	Whiteboard Preview is no longer in preview and has been released to general availability. Therefore, the section on Whiteboard Preview was renamed to "Whiteboard for PC, Surface Hub, and other platforms"; procedures to access, export, and delete data were removed from this section and replaced with a link to the Whiteboard support article.
11/08/2018	<a href="#">Workplace Analytics</a>	Added step-by-step guidance to the Delete section about removing a data subject from Workplace Analytics and removing information about a data subject from a Workplace Analytics report.
11/12/2018	All	Fixed broken bookmarks and broken links to external topics.
1/9/2019	StaffHub	In the Delete section, updated the description of what happens when a user account is permanently deleted.
5/8/2019	<a href="#">Publisher</a>	Added content about responding to DSRs for Publisher.
7/11/2019	<a href="#">MyAnalytics</a>	The ability for an admin to use the DSR case tool in the Security & Compliance Center to export MyAnalytics data was removed because all users can now view their data in the MyAnalytics app.
11/6/2019	<a href="#">Education</a>	Linked to new topics on using PowerShell scripts to get a list of classes for a specific student and then exporting or deleting their data.
1/28/2020	All	Removed StaffHub from document, StaffHub is retired.

# Visual Studio Family Data Subject Requests for the GDPR and CCPA

2/5/2021 • 10 minutes to read • [Edit Online](#)

The European Union [General Data Protection Regulation \(GDPR\)](#) gives rights to people (known in the regulation as *data subjects*) to manage their personal data. Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of personal data, requesting corrections to it, restricting the processing of it, deleting it, or receiving it in an electronic format. A formal request by a data subject to a data controller (an employer or other type of agency or organization that has control over personal data) to take an action on that data subject's personal data is called a *data subject request* or DSR.

Similarly, the California Consumer Privacy Act (CCPA), provides privacy rights and obligations to California consumers, including rights similar to GDPR's Data Subject Rights, such as the right to delete, access and receive (portability) their personal information. The CCPA also provides for certain disclosures, protections against discrimination when electing exercise rights, and "opt-out/ opt-in" requirements for certain data transfers classified as "sales". Sales are broadly defined to include the sharing of data for a valuable consideration. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

For general information about GDPR, see the [GDPR section of the Service Trust portal](#).

## Products covered by this guide

This guide discusses how to use Microsoft tools to export or delete personal data collected during authenticated (signed-in) session usage of Visual Studio and Visual Studio for Mac and Microsoft extensions to them and to Visual Studio Code. This guide also covers how to make data subject requests for personal data collected when using Visual Studio Developer Community, NuGet.org, and the ASP.NET website. These products may enable the use of non-Microsoft tools and extensions, and Microsoft is not a data processor or controller for these tools and extensions. Users should contact the tool or extension provider to understand the personal data and collection policies for these tools and extensions.

## Additional privacy information

The Microsoft Software License Terms accompanying the products, the [Microsoft Privacy Statement](#), and [Microsoft's GDPR Commitments](#) describe our data processing practices.

## Visual Studio, Visual Studio for Mac, and Visual Studio Code

### Personal data we collect

As a data processor under the GDPR, Microsoft collects the data we need from users to provide experiences for and improve Visual Studio and Visual Studio for Mac and Microsoft extensions to them and to Visual Studio Code. There are two categories of data: customer data and system-generated logs. Customer data includes user-identifiable transactional and interactional data that these products need to perform the service they provide. For example, to provide users with personalized experiences such as roaming settings, we need to collect user account information and settings data. System-generated logs are usage or diagnostic data that are used to help identify and troubleshoot problems and improve our products and services, and may also contain identifiable information about end users, such as a user name. System-generated logs are retained for no more than 18 months. As an example, system-generated logs are aggregated for each day of product usage and include the

usage date, the product used (for example, "Visual Studio 2017"), the action you took (for example, "vs/core/packagecostsummary/solutionload"), and the number of times the action was taken, as shown in this sample:

```
{Time:"2/23/2018 12:00:00 AM","AppName":"Visual Studio
2017","Action":"vs/core/packagecostsummary/solutionload","Target":"1 times",
"DevicePlatform":"Windows 10 Enterprise","IP":null,"InputMethod":null,
"SearchTerm":null,"SearchResult":null}

{Time:"2/23/2018 12:00:00 AM","AppName":"Visual Studio
2017","Action":"vs/ide/connected/accountmanagement/account","Target":"1 times",
"DevicePlatform":"Windows 10 Enterprise","IP":null,"InputMethod":null,
"SearchTerm":null,"SearchResult":null}

{"Time":"2/27/2018 12:00:00 AM","AppName":"Visual Studio
2017","Action":"vs/core/perf/satellitepagefileusage","Target":"23 times",
"DevicePlatform":"Windows 10 Enterprise","IP":null,"InputMethod":null,
"SearchTerm":null,"SearchResult":null}
```

For more information, see [System-generated logs collected by Visual Studio](#).

Only personal data that is attached to authenticated identities can be serviced by a DSR. So, for example, because Visual Studio Code does not support sign-in, system-generated logs from it are not attached to an authenticated identity and cannot be serviced. However, some Microsoft extensions for Visual Studio Code may provide authenticated data, and this data can be serviced by a DSR. For more information, see [GDPR and Visual Studio Code](#). In general, we do not store data for Visual Studio 2013 and earlier; however, certain extensions and components may provide data attached to authenticated identities and can be serviced by a DSR as outlined below.

### How users can control personal data

Visual Studio 2015 and later, Visual Studio for Mac, and Visual Studio Code provide the following means for your users to stop data collection, and for you as controller to export, or delete data that has already been gathered.

#### In-app settings

Users can control the privacy settings for these products. For more information, see the following

- [How to manage privacy settings in Visual Studio](#).
- [How to manage privacy settings in Visual Studio for Mac](#).
- [How to disable telemetry reporting in Visual Studio Code](#).

#### Exporting or deleting data

Controllers can manage customer data and system-generated logs collected from their data subjects by one of two methods, depending upon how their Visual Studio Family product or Microsoft extensions were registered. In some cases, both methods must be used. Both methods allow Controllers to download a copy of their activity history managed by that method. Closure of an AAD or MSA account deletes associated Visual Studio customer data, and anonymizes personally identifiable data in system-generated logs pertaining to these products. Anonymized system-generated logs are retained for no more than 18 months.

- Users that have registered a Visual Studio Family product by using an account that is backed by an Azure tenant — for example, AAD account or MSA account associated with an Azure subscription — can follow the instructions in [Azure Data Subject Requests for the GDPR](#).
- Users that have registered a Visual Studio Family product without an account that is backed by an Azure tenant — for example many accounts using a Microsoft Account (MSA) — can use [the web-based Microsoft Privacy Response Center](#) available through their Microsoft account to view, control, and delete activity data tied to their Microsoft account across multiple Microsoft services. In this scenario, the user is a controller for their own personal data.

#### NOTE

When an MSA account holder deletes their account, all their personally identifiable data pertaining to these products is deleted, whether the account is backed by an Azure tenant or not, and system-generated logs are anonymized.

For Visual Studio 2013, the data we collect is anonymized. For Visual Studio 2012 and prior releases, we immediately delete the data upon receipt. In both cases, there is nothing to view, export, or delete at a later time.

## Visual Studio Developer Community

We support [General Data Protection Regulation \(GDPR\)](#) requests through the [Developer Community](#) website. You can View, Export, or Delete your feedback data.

### Personal data we collect

Microsoft collects data to help us reproduce and troubleshoot issues you report with Visual Studio Family products. This data includes personal data and public feedback. Personal data includes:

- Your [Developer Community](#) profile information;
- Preferences and notifications;
- Attachments and system-generated logs you provided by [reporting a problem in Visual Studio](#) or through [Developer Community](#);
- Your votes.

Public feedback includes: reported problems, comments, and solutions.

### How users can control personal data

#### View

To View your feedback-related data, follow these steps:

1. Sign into [Developer Community](#). From the top-right corner, click on your profile and select **Profile and Preferences**.
2. Click on any of the **Profile**, **Notifications**, **Activity**, and **Attachments** tabs to view the data submitted to the feedback systems.
  - a. **Profile** refers to your [Developer Community](#) profile, including user name, email address, about, etc.
  - b. **\*\*Notifications** are how you control the email notifications you receive.
  - c. **Activity** will give you the feedback items you have been active on (posted, commented, etc.), and the activities performed.
  - d. **Attachments** is a list of your attachment history in a format like

```
FileName was attached to the problem "ProblemName" Tue, Apr 10, 18 2:27 PM.
```

#### Export

You can export your feedback data as part of DSR. We will create one or more .zip archives that will include:

- Your [Developer Community](#) profile information;
- Preferences and notification settings;
- Attachments you provided by [reporting a problem in Visual Studio](#) or through [Developer Community](#).

#### NOTE

We will exclude the following public feedback you have provided from your archive: comments, solutions, reported problems.

To start an Export, follow these steps:

1. Sign into [Developer Community](#). From the top-right corner, click on your profile and select **Profile and Preferences**.
2. Click the **Privacy** tab, and then click **Create an archive** to request exporting your data.
3. The **Archive Status** will update to show that we are preparing the data. The length of time before the data is available depends on the amount of data we need to export.
4. Once the data is ready, we will send you an email.
5. Click **Download Archive** in the email, or go back to the Privacy tab to download your data.

#### NOTE

- We will not send email if you chose not to receive notifications in the Notifications tab.
- If you request Export again, we will remove your old archive and create a new one.

#### Delete

Deleting will remove the following information about you from [Developer Community](#):

- Profile information;
- Preferences and notification settings;
- Attachments you provided by [reporting a problem in Visual Studio](#) or through [Developer Community](#).
- Your votes

#### NOTE

We will not delete, but will anonymize, the following public information: your comments, your solutions, problems that you reported.

#### IMPORTANT

Delete of an AAD or MSA account triggers the Delete process for [Developer Community](#).

To initiate a Delete, follow these steps:

1. Sign into [Developer Community](#). From the top-right corner, click on your profile and select **Profile and Preferences**.
2. Click the **Privacy** tab, and then click **Delete your data and account** to start deleting your data.
3. A confirmation screen will appear.
4. Type "delete" in the box, and then click **Delete my account**.

Once you click **Delete my account**:

- We will sign you out.
- We will delete your [Developer Community](#) account, your personal data, and attachments.
- We will anonymize your public feedback. Your public feedback will remain available on Developer Community, and will be indicated as reported by an Anonymous user.
- We won't email you after we delete your account, because you will no longer be present in the system.
- If you report a new problem or log into [Developer Community](#), you will be identified as a new user.
- If you delete your account from [Developer Community](#), we will not delete it from other Microsoft services.

## Xamarin Forums

### Personal Data We Collect



Through the [Xamarin Forums](#) user community, Microsoft collects data you provide to help us reproduce and troubleshoot issues you may have with Microsoft products and services. This data includes personal data and public feedback. The personal data we collect is user account data (for example, user names and email addresses associated with your Xamarin Forums), and the public feedback we collect includes bugs, problems, comments, and solutions you provide via the Xamarin Forums.

### How You Can Control Your Data

#### Xamarin Forums

##### View

Users with active Xamarin Forums accounts may view their personal data and public feedback (for example, all of their posted threads and posts) from their Xamarin Forums account page. Users may also edit their personal data through their account page.

##### Export

Xamarin Forums are hosted by a third party, Vanilla Forums. To request export of your public data, users should contact [forums@xamarin.com](mailto:forums@xamarin.com) (monitored by the Xamarin team). We will then work directly with Vanilla Forums to process this request.

##### Delete

Xamarin Forums are hosted by a third party, Vanilla Forums. To request deletion of your personal and public data, users should contact [forums@xamarin.com](mailto:forums@xamarin.com) (monitored by the Xamarin team). We will then manually service the user's personal data deletion request.

#### NOTE

Bugzilla for Xamarin no longer accepts new issues. Former Xamarin Bugzilla accounts holders can view an archive of all bugs they've reported and all comments they've added to bugs at <https://xamarin.github.io/bugzilla-archives/>. To request deletion of personal data contained in the archive, users can file and issue at <https://github.com/xamarin/bugzilla-archives/issues/new/choose>. Public feedback (for example, bugs, problems, comments, and solutions) that users have posted to the Xamarin Bugzilla will not be deleted after receipt of a delete request. Public feedback will instead be anonymized by removing the name and email address associated with any public feedback created by the user submitting the delete request.

## NuGet

For more information on DSR for NuGet.org, see [NuGet User Data Requests](#).

## ASP.NET

For information on DSR for the ASP.NET website, see [The ASP.NET Website and GDPR Data Subject Request processing](#).

## IIS.NET

For information on DSR for the IIS.NET website, see [The IIS.NET Website and GDPR Data Subject Request processing](#).

## Other Visual Studio Family Services

### SurveyMonkey

From time to time, we invite customers to provide feedback on these products via SurveyMonkey. This data is deleted within 28 days. When servicing data subject requests for these products, if we have authenticated survey responses we include them in export and delete data subject requests.

## Learn more

- [Microsoft's GDPR Commitments to Customers of our Generally Available Enterprise Software Products](#)
- [Microsoft Trust Center](#)
- [Service Trust portal](#)
- [Microsoft Privacy Dashboard](#)
- [Microsoft Privacy Response Center](#)
- [Azure Data Subject Requests for the GDPR](#)

# Data processor service for Windows Enterprise Data Subject Requests for the GDPR and CCPA

2/5/2021 • 6 minutes to read • [Edit Online](#)

## NOTE

This topic is intended for participants in the data processor service for Windows Enterprise preview program and requires acceptance of specific terms of use. To learn more about the program and agree to the terms of use, see <https://aka.ms/WindowsEnterprisePublicPreview>.

## Introduction to Data Subject Requests (DSRs)

The EU General Data Protection Regulation (GDPR) gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of personal data, requesting corrections to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request* or DSR.

Similarly, the California Consumer Privacy Act (CCPA), provides privacy rights and obligations to California consumers, including rights similar to GDPR's Data Subject Rights, such as the right to delete, access, and receive (portability) their personal information. The CCPA also provides for certain disclosures, protections against discrimination when electing exercise rights, and "opt-out/ opt-in" requirements for certain data transfers classified as "sales". Sales are broadly defined to include the sharing of data for a valuable consideration. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

The guide discusses how to use Microsoft products, services, and administrative tools to help our controller customers find and act on personal data to respond to DSRs. Specifically, this includes how to find, access, and act on personal data that reside in the Microsoft cloud. Here's a quick overview of the processes outlined in this guide:

1. **Access**—Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it that can be available to the data subject.
2. **Delete**—Permanently remove personal data that resided in the Microsoft cloud.
3. **Export**—Provide an electronic copy (in a machine-readable format) of personal data to the data subject. Personal information under the CCPA is any information relating to an identified or identifiable person.

Personal information under the CCPA is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. The defined term "personal information" roughly aligns with "personal data" under GDPR. However, the CCPA also includes family and household data. For more information about the CCPA, see the [California Consumer Privacy Act](#) and the [California Consumer Privacy Act FAQ](#).

Each section in this guide outlines the technical procedures that a data controller organization can take to respond to a DSR for personal data in the Microsoft cloud.

# Terminology

The following list provides definitions of terms that are relevant to this guide.

- *Controller*—The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller, or the specific criteria for its nomination may be provided for by Union or Member State law.
- *Personal data and data subject*—Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- *Processor*—A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.
- *Customer Data*—All data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, a customer through use of the enterprise service.
- *Windows Diagnostic Data*—Vital technical data from Windows devices about the device and how Windows and related software are performing. It is used to keep Windows up to date, secure, reliable, performant, and improves Windows through the aggregate analysis of the use of Windows. Some examples of Windows Diagnostic Data are the type of hardware being used, applications installed with their respective usage, and reliability information on device drivers. Some Windows components and apps connect to Microsoft services directly, but the data they exchange is not Windows Diagnostic Data. For example, exchanging a user's location for local weather or news is not an example of Windows Diagnostic Data.

## How to use this guide

When you use data processor service for Windows Enterprise enrolled devices, Windows generates some information, known as Windows Diagnostic Data, in order to provide the service.

## Windows Diagnostic Data

Microsoft provides you with the ability to access, delete, and export Windows Diagnostic Data associated with a user's use of the data processor service for Windows Enterprise.

### IMPORTANT

The ability to rectify Windows Diagnostic Data is not supported. Windows Diagnostic Data constitutes factual actions conducted within Windows, and modifications to such data would compromise the historical record of actions, increasing security risks and harming reliability. All data covered in this document is considered Windows Diagnostic Data.

## Executing DSRs against Windows Diagnostic Data

Microsoft provides the ability to access, delete, and export certain Windows diagnostic data through the Azure portal, and also directly via pre-existing application programming interfaces (APIs).

### Step 1: Access

The tenant admin is the only person within your organization who can access Windows Diagnostic Data associated with a particular user's use of a data processor service for Windows Enterprise enrolled device. The data retrieved for an access request will be provided, via export, in a machine-readable format and will be

provided in files that will allow the user to know which devices and services the data is associated with. As noted previously, the data retrieved will not include data that may compromise the security or stability of the Windows device.

Microsoft offers a portal experience, providing the enterprise customer's tenant administrator the capability to manage DSR access requests. [Azure DSR, Part 2, Step 3: Export](#), describes how to execute a DSR access request, via export, through the Azure portal.

### Step 2: Delete

Microsoft provides a way to execute user-based DSR delete requests based on a particular user's Azure Active Directory object.

For user-based delete requests, Microsoft offers a portal experience, providing the enterprise customer's tenant administrator the capability to manage DSR delete requests. [Azure DSR, Part 1, Step 5: Delete](#), describes how to execute a DSR delete request through the Azure portal.

Microsoft provides the ability to delete users, which in turn will delete Customer Data, directly via a pre-existing application programming interface (API). Details are described in the [API reference documentation](#).

#### IMPORTANT

Deleting collected data does not stop further collection. To turn off data collection follow the procedure described in the [respective service's reference documentation](#).

Additionally, user-based delete requests require deleting the user account itself.

### Step 3: Export

The tenant admin is the only person within your organization who can access Windows diagnostic data associated with a particular user's use of a data processor service for Windows Enterprise enrolled device. The data retrieved for an export request will be provided in a machine-readable format and will be provided in files that will allow the user to know which devices and services the data is associated with. As noted previously, the data retrieved will not include data that may compromise the security or stability of the Windows device. [Azure DSR, Part 2, Step 3: Export](#), describes how to execute a DSR export request through the Azure portal.

Microsoft provides the ability to export Customer Data directly via a pre-existing application programming interface (API). Details are described in the [API reference documentation](#).

## Notify about exporting or deleting issues

If you run into issues while exporting or deleting data from the Azure portal, go to the Azure portal **Help + Support** blade and submit a new ticket under **Subscription Management > Other Security and Compliance Request > Privacy Blade and GDPR Requests**.

# GDPR Breach Notification

2/5/2021 • 4 minutes to read • [Edit Online](#)

The General Data Protection Regulation (GDPR) introduces new rules for organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents no matter where you or your enterprise are located. Additional details can be found in the [GDPR Summary topic](#). This document leads you to information on the completion of Breach Notifications under the GDPR using Microsoft products and services.

## What constitute a breach of personal data under the GDPR?

Personal data means any information related to an individual that can be used to identify them directly or indirectly. A personal data breach is 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed'.

## Terminology

Helpful definitions for GDPR terms used in this document:

- *Data Controller (Controller)*: A legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- *Personal data and data subject*: Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly.
- *Processor*: A natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller.
- *Customer Data*: Data produced and stored in the day-to-day operations of running your business.

## Microsoft and Breach Notification

Microsoft takes its obligations under the General Data Protection Regulation (GDPR) seriously. A security incident/data breach refers to events such as unlawful access to customer's data stored on Microsoft equipment or in Microsoft facilities, or unauthorized access to such that has the potential to result in the loss, disclosure, or alteration of customer data.

As a data processor, Microsoft ensures that service customers are able to meet the GDPR's breach notification requirements as data controllers. Our notification provides the information needed to make that assessment. Microsoft notifies customers of any personal data breach, except for those cases where personal data is confirmed to be unintelligible (for example, encrypted data where integrity of the keys is confirmed).

Data controllers are responsible for assessing risks to data privacy and determining whether a breach requires notification of a customer's DPA. Microsoft provides the information needed, along with your GDPR compliance policy, to make that assessment.

Initial notification includes a description of the nature of the breach, approximate user impact, and mitigation steps (if applicable). If our investigation is not complete at the time of initial notification, we will indicate next steps and timelines for subsequent communication. For more information about how Microsoft detects and responds to a breach of personal data, see [Data Breach Notification Under the GDPR](#) in the Service Trust Portal.

Details regarding breach notification for specific Microsoft products and services is given below.

### 1. [Office 365](#)

Microsoft invests extensively in systems, processes, and personnel to reduce the likelihood of personal data breach and to quickly detect and mitigate consequence of breach if it does occur. Additional details can be read at [Office 365 Investments in Data Security](#).

A customer may become aware of a breach and wish to contact Microsoft. In this case, notify Microsoft Support, which will then interface with engineering teams for more information.

## 2. [Azure & Dynamics 365](#)

Microsoft has a global, 24x7 incident response service that works to mitigate the effects of attacks against Microsoft Azure and Dynamics 365.

- *Detection of Breaches:* Since both Microsoft and the customer have security obligations, Azure services employ a shared responsibility model to define security and operational accountabilities. Microsoft does not monitor or respond to security incidents within the customer's realm of responsibility. Customer incident response may involve collaboration with Azure [customer support](#), given appropriate service contracts. Microsoft Azure also offers various services (for example, [Azure Security Center](#)) that customers can utilize for developing and managing security incident response.

For a list of events that trigger a breach investigation in Microsoft Azure, see [Detection of Potential Breaches. Azure and Breach Notification under the GDPR](#) further details how Microsoft investigates, manages, and responds to security incidents within Azure.

- *Data Breach Response:* Microsoft determines appropriate priority and severity levels of a breach by investigating the functional impact, recoverability, and information impact of the incident. Priority and severity may change over the course of the investigation, based on new findings and conclusions. Microsoft's security response team works closely with global legal advisors to help ensure that forensics are performed in accordance with legal obligations and commitments to customers. These processes are detailed in [Azure's Data Breach Response](#).
- *Customer Notification:* Microsoft Azure notifies customers and regulatory authorities of data breaches as required. Customer notices are delivered in no more than 72 hours from the time we declared a breach except for the following circumstances:
  - Microsoft believes the act of performing a notification increases the risk to other customers.
  - The 72-hour timeline may leave some incident details available. These details will be provided to you as the investigation proceeds.

Further details can be found in [Customer Notification](#).

## 3. [Microsoft Support and Professional Services](#)

The nature of professional services means that some data protection incidents may fall within the customer's realm of responsibility. When Microsoft Professional Services identifies a data protection incident, it follows documented industry standard response plan as outlined in [Scope & Limits of Data Protection Incident Response Process](#).

## Breach notification admin tools

- **Set your organization's privacy contact:** Tenant Administrators can use the [Azure Active Directory Admin Portal](#) to define your organization's privacy contact should Microsoft need to communicate with them.

## Learn more

- [Microsoft Trust Center](#)

# Azure and Dynamics 365 breach notification under the GDPR

2/9/2021 • 9 minutes to read • [Edit Online](#)

Microsoft takes its obligations under the General Data Protection Regulation (GDPR) seriously. Microsoft takes extensive security measures within its online services to protect against data breaches. These measures include both physical and logical security controls, as well as automated security processes, comprehensive information security and privacy policies, and security and privacy training for all personnel.

Security is built into Microsoft Azure from the ground up, starting with the [Security Development Lifecycle](#), a mandatory development process that incorporates privacy-by-design and privacy-by-default methodologies. The guiding principle of Microsoft's security strategy is to 'assume breach,' which is an extension of the defense-in-depth strategy. By constantly challenging the security capabilities of Azure, Microsoft can stay ahead of emerging threats. For more information on Azure security, review these [resources](#).

Microsoft has a dedicated global, 24x7 incident response service that works to mitigate the effects of attacks against Microsoft Azure. Attested by multiple security and compliance audits (for example, [ISO/IEC 27018](#)), Microsoft employs rigorous operations and processes at its data centers to prevent unauthorized access, including 24x7 video monitoring, trained security personnel, smart cards, and biometric controls.

## Detection of potential breaches

Due to the nature of modern cloud computing, not all data breaches occurring in a customer cloud environment involve Microsoft Azure services. Microsoft employs a shared responsibility model for Azure services to define security and operational accountabilities. Shared responsibility is important when discussing security of a cloud service, because both the cloud services provider and the customer are accountable for portions of cloud security.

Microsoft does not monitor for or respond to security incidents within the customer's realm of responsibility. A customer-only security compromise would not be processed as an Azure security incident and would require the customer tenant to manage the response effort. Customer incident response may involve collaboration with Microsoft Azure [customer support](#), given appropriate service contracts. Microsoft Azure also offers various services (for example, [Azure Security Center](#)) that customers can utilize for developing and managing security incident response.

Azure responds to a potential data breach according to the security incident response process, which is a subset of the Microsoft Azure incident management plan. Microsoft's Azure security incident response is implemented using a five-stage process: Detect, Assess, Diagnose, Stabilize, and Close. The Security Incident Response Team may alternate between the diagnose and stabilize stages as the investigation progresses. An overview of the security incident response process is below:

STAGE	DESCRIPTION
<i>1: Detect</i>	First indication of a potential incident.
<i>2: Assess</i>	An on-call incident response team member assesses the impact and severity of the event. Based on evidence, the assessment may or may not result in further escalation to the security response team.



STAGE	DESCRIPTION
<i>3: Diagnose</i>	Security response experts conduct the technical or forensic investigation, identify containment, mitigation, and workaround strategies. If the security team believes that customer data may have become exposed to an unlawful or unauthorized individual, execution of the Customer Incident Notification process begins in parallel.
<i>4: Stabilize and Recover</i>	The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps such as quarantining impacted systems may occur immediately and in parallel with diagnosis. Longer term mitigations may be planned which occur after the immediate risk has passed.
<i>5: Close and Post-mortem</i>	The incident response team creates a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a recurrence of the event.

The [Microsoft Azure Security Response in the Cloud](#) white paper further details how Microsoft investigates, manages, and responds to security incidents within Azure.

The detection processes used by Microsoft Azure are designed to discover events that risk the confidentiality, integrity, and availability of Azure services. Several events can trigger an investigation:

- Automated system alerts via internal monitoring and alerting frameworks. These alerts could come in the way of signature-based alarms such as anti-malware, intrusion detection or via algorithms designed to profile expected activity and alert upon anomalies.
- First party reports from Microsoft Services running on Microsoft Azure and Azure Government.
- Security vulnerabilities are reported to the [Microsoft Security Response Center \(MSRC\)](#) via [secure@microsoft.com](mailto:secure@microsoft.com). MSRC works with partners and security researchers around the world to help prevent security incidents and to advance Microsoft product security.
- Customer reports via the [Customer Support Portal](#) or Microsoft Azure and Azure Government Management Portal, that describe suspicious activity attributed to the Azure infrastructure (as opposed to activity occurring within the customer's scope of responsibility).
- Security [Red Team and Blue Team](#) activity. This strategy uses a highly skilled Red Team of offensive Microsoft security experts to uncover and attack potential weaknesses in Azure. The security response Blue Team must detect and defend against the Red Team's activity. Both Red and Blue Team actions are used to verify that Azure security response efforts are effectively managing security incidents. Security Red Team and Blue Team activities are operated under rules of engagement to help ensure the protection of customer data.
- Escalations by operators of Azure Services. Microsoft employees are trained to identify and escalate potential security issues.

## Azure's data breach response

Microsoft assigns the investigation appropriate priority and severity levels by determining the functional impact, recoverability, and information impact of the incident. Both the priority and severity may change over the course of the investigation, based on new findings and conclusions. Security events involving imminent or confirmed risk to customer data are treated as high severity and worked around the clock to resolution.

Microsoft Azure categorizes the information impact of the incident into the following breach categories:

CATEGORY	DEFINITION
<i>None</i>	No information was exfiltrated, changed, deleted, or otherwise compromised.
<i>Privacy Breach</i>	Sensitive personal data of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated.
<i>Proprietary Breach</i>	Unclassified proprietary information, such as protected critical infrastructure information (PCI), was accessed or exfiltrated.
<i>Integrity Loss</i>	Sensitive or proprietary information was changed or deleted.

The Security Response Team works with Microsoft Azure Security Engineers and SMEs to classify the event based on factual data from the evidence. A security event may be classified as:

- **False Positive:** An event that meets detection criteria but is found to be part of a normal business practice and may need to be filtered. The service team identifies the root cause for false positives and will address them in a systematic way using detection sources and fine-tuning them as needed.
- **Security Incident:** An incident when unlawful access to any Customer Data or Support Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data or Support Data has occurred.
- **Customer Reportable Security/Privacy Incident (CRSPI):** An unlawful or unauthorized access to or use of Microsoft's systems, equipment, or facilities resulting in disclosure, modification, or loss of customer data.
- **Privacy Breach:** A subtype of Security Incident involving personal data. Handling procedures are no different than a security incident.

For a CRSPI to be declared, Microsoft must determine that unauthorized access to customer data has or has likely occurred and/or that there is a legal or contractual commitment that notification must occur. It is desired, but not required, that specific customer impact, resource access, and repair steps be known. An incident is generally declared a CRSPI after the conclusion of the Diagnose stage of a security incident. However, the declaration may happen at any point that all pertinent information is available. The security incident manager must establish evidence beyond reasonable doubt that a reportable event has occurred to begin execution of the Customer Incident Notification Process.

Microsoft verifies that customer and business risk is successfully contained, and that corrective measures are implemented. If necessary, emergency mitigation steps to resolve immediate security risks associated with the event are taken.

Microsoft also completes an internal post-mortem for data breaches. As a part of this exercise, sufficiency of response and operating procedures are evaluated, and any updates that may be necessary to the Security Incident Response SOP or related processes are identified and implemented. Internal postmortems for data breaches are highly confidential records not available to customers. Postmortems may, however, be summarized and included in other customer event notifications. These reports are provided to external auditors for review as part of Azure's routine audit cycle.

## Customer notification

Microsoft notifies impacted customers and regulatory authorities of data breaches as required. Microsoft relies on heavy internal compartmentalization in the operation of Azure. Data flow logs are also robust. As a benefit of this design, most incidents can be scoped to specific customers. The goal is to provide impacted customers with an accurate, actionable, and timely notice when their data has been breached.

After the declaration of a CRSPI, the notification process takes place as expeditiously as possible while still

considering the security risks of moving quickly. Generally, the process of drafting notifications occurs as the incident investigation is ongoing. Customer notices are delivered in no more than 72 hours from the time we declared a breach *except* in the following circumstances:

- Microsoft believes that the act of performing a notification increases the risk to other customers. For example, the act of notifying may tip off an adversary causing an inability to remediate.
- Other unusual or extreme circumstances vetted by Microsoft's legal department and the Executive Incident Manager.
- The 72-hour timeline may leave some incident details available. These details are provided to customers and regulatory authorities as the investigation proceeds.

Microsoft provides impacted customers with detailed information enabling them to perform internal investigations and assisting them in meeting end-user commitments, while not unduly delaying the notification process.

Notification of a personal data breach will be delivered to the impacted customer by any means Microsoft selects, including via email. Notification of a data breach will be delivered to the list of security contacts provided in Azure Security Center, which can be configured by following the [implementation guidelines](#). If contact information is not provided in Azure Security Center, the notification is sent to one or more administrators in an Azure subscription. To ensure that notification can be successfully delivered, it is the customer's responsibility to ensure that the administrative contact information on each applicable subscription and online services portal is correct.

The Microsoft Azure or Azure Government team may also elect to notify other Microsoft personnel such as members of Microsoft's Customer Support Service (CSS) team and the customer's Account Manager(s) (AM) or Technical Account Manager(s) (TAM). These individuals often have close relationships with the customer and can facilitate faster remediation

## Microsoft Dynamics 365 built-in security features

Microsoft Dynamics 365 takes advantage of the cloud service infrastructure and built-in security features to keep data safe using security measures and mechanisms to protect data. In addition, Dynamics 365 provides efficient data access and collaboration with data integrity and privacy in the following areas: [secure identity, data protection, role based security, and threat management](#).

The Microsoft Dynamics 365 offering follows the same Technical and Organizational measures one or more Microsoft Azure service teams take for securing against data breach processes. Therefore, any information documented in the 'Microsoft Azure Data Breach' notification document here is analogous to Microsoft Dynamics 365 as well.

## Learn more

[Microsoft Trust Center](#)

# Microsoft Support and Professional Services and Breach Notification Under the GDPR

11/30/2020 • 7 minutes to read • [Edit Online](#)

Microsoft Support and Professional Services take its obligations under the General Data Protection Regulation (GDPR) seriously.

Microsoft Professional Services includes a diverse group of technical architects, engineers, consultants, and support professionals dedicated to delivering on the Microsoft mission of empowering customers to do more and achieve more. Our Professional Services team includes more than 21,000+ total consultants, Digital Advisors, Premier Support, engineers, and sales professionals working across 191 countries, supporting 46 different languages, managing several million engagements per month, and engaging in customer and partner interactions through on-premise, phone, web, community, and automated tools. The organization brings broad expertise across the Microsoft portfolio, leveraging an extensive network of partners, technical communities, tools, diagnostics, and channels that connect us with our enterprise customers.

The drive for Microsoft Professional Services' global data protection incident response team is to (a) employ rigorous operations and processes to prevent data protection incidents from occurring, (b) manage them professionally and efficiently when they do occur, and (c) learn from these data protection incidents through regular post-mortem and program improvements. Microsoft's Professional Services data protection incident response team's processes and results are reviewed and attested to by multiple security and compliance audits (for example, ISO/IEC 27001).

## Data Protection incident response overview

Microsoft Professional Services is committed to protecting its customers and takes considerable measures to prevent data protection incidents from occurring as a means of maintaining customer trust. A data protection incident in the Professional Services organization is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, or Support or Consulting Data, while processed by Microsoft. For Commercial customers that have purchased Premier Support, Unified Support or Microsoft Consulting Services, you should refer to your data protection incident response language in the Professional Services Data Protection Addendum located at <https://aka.ms/professionalservicesdpa/>.

## Scope & limits of data protection incident response process

Our personal data breach notification process begins when we declare that a [personal data breach] has occurred.

To be declared, the Microsoft data protection incident response team must determine that a data protection incident as defined previously has occurred. Declaration will occur as soon as all pertinent information is available to determine that a data protection incident has occurred.

Due to the nature of professional services, some events that seem like Microsoft data protection incidents are not because they occurred through customer's actions or on customer's systems. Microsoft does not monitor for or respond to data protection incidents within the customer's realm of responsibility. However, when Microsoft becomes aware of a customer-driven data protection incident we will classify this incident as a customer-driven data protection incident, which the data protection incident response team calls an 'event', inform the customer of our observation, and as requested will assist them on their response effort, to the extent required by their interaction with Microsoft. Some examples of customer-driven data protection incidents include inadvertent sending Microsoft the customer's passwords and other sensitive data to Microsoft, requests to delete data and

being the victim of fraud.

Some actions are out of scope for this process completely, including general questions about our data protection policies or standards, data subject right requests, opt-out requests, product wish lists, or bug reports not related to data protection, data protection incidents not involving customer's data, and fraud against Microsoft.

## Types of data protection incidents

The data protection incident response team has identified a set of scenarios that may occur in professional services. While adhering to the basic data protection incident response framework, procedures have been developed and customized to expedite the response process. For instance, a misdirected email may require little investigation. On the other hand, identifying malicious personnel may require a complete forensic investigation due to the surreptitious nature of an offender's activities. This set of scenarios may provide insight into the data protection incident response process for professional services.

## Data protection incident response process

When Microsoft Professional Services identifies a data protection incident, a triage process occurs that (a) assesses the event, (b) determines whether it is in-scope for this process, (c) determines whether it was malicious, (d) performs a preliminary investigation and assigns a severity level, and (e) alerts and coordinates with appropriate stakeholders within Microsoft. The team also begins recording details for tracking purposes and the post-mortem exercise.

### **Detection**

Microsoft Professional Services continuously monitors for emerging data protection incidents across all data stores containing personal data—both online and offline. We use different methods to detect data protection incidents, including automated alerts, customer reports, reports from external parties, observation of anomalies, and indications of malicious or hacker activity.

The detection processes used by Microsoft Professional Services are designed to discover data protection incidents and trigger investigations. For example:

- Security vulnerabilities are reported to the Microsoft-wide reporting system for referral or reported directly to the Professional Services data protection incident response team.
- Customers submit reports via the [Customer Support Portal](#) that describe suspicious activity.
- Professional Services personnel submit escalations. Microsoft employees are trained to identify and escalate potential security issues.
- For tools and systems used in the process of providing Professional Services, the operations teams use automated system alerts via internal monitoring and alerting frameworks. These alerts could come in the way of signature-based alarms such as antimalware, intrusion detection or via algorithms designed to profile expected activity and alert upon anomalies.

### **Data protection incident response drills, testing of data protection incident response plan**

In addition to ongoing training, each year Professional Services executes drills in partnership with appropriate internal departments to communicate the data protection incident escalation procedures, roles, and responsibilities to all stabilization team members. This training prepares key stakeholders for real-world data protection incidents—whether security, physical, or privacy in nature. This training includes exercises with representatives of the data protection incident response team, security team, legal teams, and communications team.

After the exercises, we document the outcome and remediation methods we have decided to use.

### **Data protection incident response training**

A key component of data protection incident response is personnel training to identify and report data

protection incidents. Personnel in the Professional Services organization are required to take training that covers privacy fundamentals, GDPR regulations, and best practices on how to identify and report data protection incidents.

Regular online training is available, and completion is mandatory for all personnel. The training program employs testing, ongoing surveys, awareness, and follow-up designed to ensure that training is being understood and retained.

## **Process**

When Microsoft Professional Services organization identifies a data protection incident, it follows a documented industry standard response plan, beginning with determination that the data protection incident criteria are met. Where a data protection incident occurs, it is generally declared immediately after Triage but, depending on complexity, the declaration may happen at any point when a level of necessary information is available, including after the investigation stage. On the other hand, the team has discretion to declare a data protection incident based only on reasonable suspicion of occurrence. The team may also alternate between the various stages as the investigation progresses.

Based on the severity level, Microsoft may also complete an internal post-mortem for data protection incidents. As a part of this exercise, sufficiency of response and operating procedures are evaluated, and any updates that may be necessary to the *Data Protection Incident Response Standard Operating Procedure* or related processes are identified and implemented. Internal postmortems for data breaches are highly confidential records not available to customers. Postmortems may, however, be summarized and included in customer event notifications. As part of a routine audit cycle, post-mortem processes are reviewed by external auditors to ensure follow-up occurs.

## **Notification**

When Microsoft Professional Services declares a data protection incident under the GDPR, we target notification to our customers within 72 hours.

After the declaration of a data protection incident, the notification process takes place as expeditiously as possible while still considering the security risks of moving quickly. To ensure that notification can be successfully delivered, it is the customer's responsibility to ensure that the administrative contact information on each applicable account, subscription, and online services portal is correct. While the goal is to provide impacted customers with an accurate, actionable, and timely notice, to achieve the 72-hour notification commitment the initial notification may not include complete details as all details may not be available during the early stages of a data protection incident. In addition, Microsoft may need to withhold some details due to the circumstances of the data protection incident. For instance, it may be necessary to withhold details if the act of providing notification increases risk to other customers or interferes with Microsoft's or law enforcement's ability to catch a malicious actor.

In its capacity as a data processor, Microsoft recognizes that customers are responsible for determining whether notification is appropriate and, if so, notifying the competent Data Protection Authority (DPA) and the customer's own data subjects of any personal data breach. Microsoft Professional Services will work to provide customers the information needed to proceed with notice in these circumstances.

When providing notice to customers of a personal data breach, Microsoft will include the following information, if applicable and known:

- Nature of the breach
- Mitigation measures Microsoft is taking or proposing
- Product, service, application involved
- Length of time personal data was exposed, if known
- Volume of affected/exposed personal data records, if known
- Sub-processor/supplier details, if one is involved in the breach

## Learn more

Find out more about Microsoft Professional Services (<https://aka.ms/pstrust>).

# Breach Notification Under the GDPR

1/5/2021 • 7 minutes to read • [Edit Online](#)

As a data processor, Office 365 will ensure that our customers are able to meet the GDPR's breach notification requirements as data controllers. To that end, we are committed to the following actions:

- Providing customers with an ability to specify a dedicated privacy contact who will be notified in the event of a breach. Customers can specify this contact using the Privacy reader role settings for Message Center.
- Notifying customers of a personal data breach within 72 hours of a breach being declared. Notifications will be published to the Message Center, which is accessible through the Microsoft 365 admin center. Secondly, email notifications are sent to specified contacts indicating a new Message Center post has been published.
- Initial notification will include, at the least, a description of the nature of the breach, approximation of user impact, and mitigation steps (if applicable). If our investigation is not complete at the time of initial notification, we will indicate next steps and timelines for subsequent communication in our initial notification

Microsoft recognizes that data controllers are responsible for conducting risk assessments and determining whether a breach requires notification of the customer's DPA, and our notification to customers will provide the information needed to make that assessment. Microsoft will therefore notify customers of any personal data breach, except for those cases where personal data is confirmed to be unintelligible (for example, encrypted data where integrity of the keys is confirmed).

## Office 365 investments in data security

In addition to our commitment to provide timely notification of breach, Office 365 strongly invests in systems, processes, and personnel to reduce the likelihood of personal data breach and to quickly detect and mitigate consequence of breach if it does occur.

Here is a description of some of our investments in this space:

- **Access Control Systems.** Office 365 maintains a "zero-standing access" policy, which means that engineers do not have access to the service unless it is explicitly granted in response to a specific incident that requires elevation of access. Whenever access is granted it is done under the principle of least privilege: permission granted for a specific request only allows for a minimal set of actions required to service that request. To do this, Office 365 maintains strict separation between "elevation roles", with each role only allowing certain pre-defined actions to be taken. The "Access to Customer Data" role is distinct from other roles that are more commonly used to administer the service and is scrutinized most heavily before approval. Taken together, these investments in access control greatly reduce the likelihood that an engineer in Office 365 inappropriately accesses customer data.
- **Security Monitoring Systems and Automation:** Office 365 maintains robust, real-time security monitoring systems. Among other issues, these systems raise alerts for attempts to illicitly access customer data, or for attempts to illicitly transfer data out of our service. Related to the points about access control mentioned previously, our security monitoring systems maintain detailed records of elevation requests that are made, and the actions taken for a given elevation request. Office 365 also maintains automatic resolution investments that automatically act to mitigate threats in response to issues we detect, and dedicated teams for responding to alerts that cannot be resolved automatically. To validate our security monitoring systems, Office 365 regularly conducts red-team exercises in which an internal penetration testing team simulates attacker behavior against the live environment. These exercises lead to regular improvements to our security monitoring and response capabilities.
- **Personnel and Processes:** In addition to the automation described previously, Office 365 maintains



processes and teams responsible for both educating the broader organization about privacy and incident management processes, and for executing those processes during a breach. For example, a detailed privacy breach Standard Operating Procedure (SOP) is maintained and shared with teams throughout the organization. This SOP describes in detail the roles and responsibilities both of individual teams within Office 365 and centralized security incident response teams. These responsibilities span both what teams need to do to improve their own security posture (conduct security reviews, integrate with central security monitoring systems, and other best practices), and what teams would need to do if an actual breach (rapid escalation to incident response, maintain and provide specific data sources that will be used to expedite the response process). Teams are also regularly trained on data classification, and correct handling and storage procedures for personal data.

The major takeaway is that Office 365 strongly invests in reducing the likelihood and consequences of personal data breach impacting our customers. If personal data breach does occur, we are committed to rapidly notifying our customers once that breach is confirmed.

## What to expect in the event of breach

The section above describes the investments Office 365 takes to reduce the likelihood of data breach. In the unlikely event that breach does occur, customers should expect a predictable experience in terms of the following responses:

- Consistent incident response lifecycle within Office 365. As described above, Office 365 maintains detailed incident response SOPs describing how teams should prepare for breach and how they should operate if a breach does occur. This ensures that our protections and processes apply throughout the service.
- Consistent criteria for notifying customers. Our notification criteria focus on Confidentiality, Integrity, and Availability of customer data. Office 365 will directly notify customers if either the confidentiality or integrity of customer data is impacted. That is, we will notify customers if their data is accessed without proper authorization, or if there is inappropriate destruction or loss of data. Office 365 will also report issues impacting data availability, although this action is usually done through the Service Health Dashboard (SHD).
- Consistent notification details. When Office 365 does communicate regarding data breach, customers can expect specific details to be communicated: at minimum, we will provide the following details:
  - Timing of the breach and timing of breach awareness
  - The approximate number of users impacted
  - The type of user data that was breached
  - Actions needed to mitigate the breach, either by the controller or by the processor

Customers should also note that Office 365, as a data processor, will not determine the risk of data breach. Whenever personal data breach is detected, we will notify our customers and provide them with the details they need to accurately determine risk to impacted users and to decide whether further reporting to regulatory authorities is required. To that end, data controllers are expected to determine the following about the incident:

- Breach severity (that is, risk determination)
- Whether end users need to be notified
- Whether regulators (DPAs) need to be notified
- Specific steps that will be taken by the controller to mitigate the consequences of breach

## Contacting Microsoft

In some scenarios, a customer may become aware of a breach and may wish to notify Microsoft. The current protocol is for customers to notify Microsoft Support, which will then interface with engineering teams for more

information. In this scenario, Microsoft engineering teams are similarly committed to providing the information customers need, through their support contact, in a timely fashion.

## Call to action for customers

As noted previously, Office 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified. Additionally, Office 365 recommends that customers designate a Global Privacy Contact alias, which can be done in the Azure Active Directory portal. In the event of personal data breach, this alias may be e-mailed in addition to the notification that will be sent to administrators.

The customer's privacy contact can be an individual within the organization, a distribution list (DL), or someone entirely outside of the organization. Office 365 only asks that customers provide an e-mail address for this contact, and customers will be able to specify this address in the Azure Active Directory portal, under the "Global Privacy Contact" field. This field is related to, but distinct from, the existing "Technical Contact" field in Azure Active Directory. If customers choose to specify a DL for this contact, they should ensure that the DL is configured to enable receipt of messages from external senders.

To summarize, Office 365 asks customers to do the following to receive the benefits of our breach notification processes:

- Decide on a contact to receive e-mail notifications regarding personal data breach. This contact should be aware of the controller's requirements under GDPR and should be prepared to interface with the organization's DPO and potentially the DPA shortly after receiving notification. Tenant administrators will also receive breach notifications and should similarly be aware of the controller's requirements under GDPR.
- Enter the privacy contact's e-mail address into the Azure Active Directory portal. If no Global Privacy Contact information is provided, Microsoft will only notify the tenant administrator

# Data processor service for Windows Enterprise breach notification under the GDPR

2/5/2021 • 8 minutes to read • [Edit Online](#)

## NOTE

This topic is intended for participants in the data processor service for Windows Enterprise preview program and requires acceptance of specific terms of use. To learn more about the program and agree to the terms of use, see <https://aka.ms/WindowsEnterprisePublicPreview>.

Microsoft data processor service for Windows Enterprise takes its obligations under the General Data Protection Regulation (GDPR) seriously. Microsoft data processor service for Windows Enterprise takes extensive security measures to protect against data breaches. These include dedicated threat management teams that proactively anticipate, prevent, and mitigate malicious access. Internal security measures such as port scanning, perimeter vulnerability scanning, and intrusion detection detect and prevent malicious access, as well as automated security processes, comprehensive information security and privacy policies, and security and privacy training for all personnel.

Security is built into the Microsoft data processor service for Windows Enterprise from the ground up, starting with the [Security Development Lifecycle](#), a mandatory development process that incorporates privacy-by-design and privacy-by-default methodologies. The guiding principle of Microsoft's security strategy is to 'assume breach', which is an extension of the defense-in-depth strategy. By constantly challenging the security capabilities of the data processor service for Windows Enterprise, Microsoft can stay ahead of emerging threats. For more information on the data processor service for Windows Enterprise security, please review these [resources](#) the data processor service for Windows Enterprise responds to a potential data breach according to the security incident response process. The data processor service for Windows Enterprise security incident response is implemented using a five-stage process: Detect, Assess, Diagnose, Stabilize, and Close. The Security Incident Response Team may alternate between the diagnose and stabilize stages as the investigation progresses. An overview of the security incident response process is below:

STAGE	DESCRIPTION
<i>1: Detect</i>	First indication of a potential incident.
<i>2: Assess</i>	An on-call incident response team member assesses the impact and severity of the event. Based on evidence, the assessment may or may not result in further escalation to the security response team.
<i>3: Diagnose</i>	Security response experts conduct the technical or forensic investigation, identify containment, mitigation, and workaround strategies. If the security team believes that customer data may have become exposed to an unlawful or unauthorized individual, execution of the Customer Incident Notification process begins in parallel.

STAGE	DESCRIPTION
<b>4: Stabilize and Recover</b>	The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps such as quarantining impacted systems may occur immediately and in parallel with diagnosis. Longer term mitigations may be planned which occur after the immediate risk has passed.
<b>5: Close and Post-mortem</b>	The incident response team creates a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence of the event.

The detection processes used by Microsoft data processor service for Windows Enterprise are designed to discover events that risk the confidentiality, integrity, and availability of the data processor service for Windows Enterprise. Several events can trigger an investigation:

- Automated system alerts via internal monitoring and alerting frameworks. These alerts could come in the way of signature-based alarms such as anti-malware, intrusion detection or via algorithms designed to profile expected activity and alert upon anomalies.
- First party reports from Microsoft Services running on Microsoft Azure and Azure Government.
- Security vulnerabilities are reported to the [Microsoft Security Response Center \(MSRC\)](#) via [secure@microsoft.com] ([secure@microsoft.com](mailto:secure@microsoft.com)). MSRC works with partners and security researchers around the world to help prevent security incidents and to advance Microsoft product security.
- Customer reports via the Customer Support Portal or Microsoft Azure and Azure Government Management Portal, that describe suspicious activity attributed to the Azure infrastructure (as opposed to activity occurring within the customer's scope of responsibility).
- Security [Red Team and Blue Team](#) activity. This strategy uses a highly skilled Red Team of offensive Microsoft security experts to uncover and attack potential weaknesses in Azure. The security response Blue Team must detect and defend against the Red Team's activity. Both Red and Blue Team actions are used to verify that Azure security response efforts are effectively managing security incidents. Security Red Team and Blue Team activities are operated under rules of engagement to help ensure the protection of customer data.
- Escalations by operators of Azure Services. Microsoft employees are trained to identify and escalate potential security issues.

## Data processor service for Windows Enterprise Data Breach Response

Microsoft assigns the investigation appropriate priority and severity levels by determining the functional impact, recoverability, and information impact of the incident. Both the priority and severity may change over the course of the investigation, based on new findings and conclusions. Security events involving imminent or confirmed risk to customer data are treated as high severity and worked around the clock to resolution. Microsoft data processor service for Windows Enterprise categorizes the information impact of the incident into the following breach categories:

CATEGORY	DEFINITION
<b>None</b>	No information was removed, changed, deleted, or otherwise compromised.
<b>Privacy Breach</b>	Sensitive personal data of taxpayers, employees, beneficiaries, etc. was accessed or removed.

CATEGORY	DEFINITION
<i>Proprietary Breach</i>	Unclassified proprietary information, such as protected critical infrastructure information (PCI), was accessed or removed.
<i>Integrity Loss</i>	Sensitive or proprietary information was changed or deleted.

The Security Response Team works with Microsoft data processor service for Windows Enterprise Security Engineers and SMEs to classify the event based on factual data from the evidence. A security event may be classified as:

- **False Positive:** An event that meets detection criteria but is found to be part of a normal business practice and may need to be filtered. The service team will identify the root cause for false positives and will address them in a systematic way using detection sources and fine-tuning them as needed.
- **Security Incident:** An incident where unlawful access to any Customer Data or Support Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data or Support Data has occurred.
- **Customer-Reportable Security Incident (CRSI):** An unlawful or unauthorized access to or use of Microsoft's systems, equipment, or facilities resulting in disclosure, modification, or loss of customer data.
- **Privacy Breach:** A subtype of Security Incident involving personal data. Handling procedures are no different than a security incident.

For a CRSI to be declared, Microsoft must determine that unauthorized access to customer data has or has likely occurred and/or that there is a legal or contractual commitment that notification must occur. It is desired, but not required, that specific customer impact, resource access, and repair steps be known. An incident is generally declared a CRSI after the conclusion of the Diagnose stage of a security incident; however, the declaration may happen at any point that all pertinent information is available. The security incident manager must establish evidence beyond reasonable doubt that a reportable event has occurred to begin execution of the Customer Incident Notification Process.

Throughout the investigation, the security response team works closely with global legal advisors to help ensure that forensics are performed in accordance with legal obligations and commitments to customers. There are also significant restrictions on system and customer data viewing and handling in various operating environments. Sensitive or confidential data, and Customer Data, are not transferred out of the production environment without explicit written approval from the Incident Manager recorded in the corresponding incident ticket.

Microsoft verifies that customer and business risk is successfully contained, and that corrective measures are implemented. If necessary, emergency mitigation steps to resolve immediate security risks associated with the event are taken.

Microsoft also completes an internal post-mortem for data breaches. As a part of this exercise, sufficiency of response and operating procedures are evaluated, and any updates that may be necessary to the Security Incident Response SOP or related processes are identified and implemented. Internal postmortems for data breaches are highly confidential records not available to customers. Postmortems may, however, be summarized and included in other customer event notifications. These reports are provided to external auditors for review as part of the data processor service for Windows Enterprise routine audit cycle.

## Customer notice

Microsoft data processor service for Windows Enterprise notifies customers and regulatory authorities of data breaches as required. Microsoft relies on heavy internal compartmentalization in the operation of the data processor service for Windows Enterprise. Data flow logs are also robust. As a benefit of this design, most

incidents can be scoped to specific customers. The goal is to provide impacted customers with an accurate, actionable, and timely notice when their data has been breached.

After the declaration of a CRSI, the notification process takes place as expeditiously as possible while still considering the security risks of moving quickly. Generally, the process of drafting notifications occurs as the incident investigation is ongoing. Customer notices are delivered in no more than 72 hours from the time we declared a breach except for the following circumstances:

- Microsoft believes the act of performing a notification will increase the risk to other customers. For example, the act of notifying may tip off an adversary causing an inability to remediate.
- Other unusual or extreme circumstances vetted by Microsoft's legal department Corporate External and Legal Affairs (CELA) and the Executive Incident Manager.

Microsoft data processor service for Windows Enterprise provides customers with detailed information enabling them to perform internal investigations and assisting them in meeting end-user commitments, while not unduly delaying the notification process.

Notification of a personal data breach will be delivered to the customer by any means Microsoft selects, including via email. Notification of a data breach will be delivered to the list of security contacts provided in Azure Security center, which can be configured by following the [implementation guidelines](#). If contact information is not provided in Azure Security Center, the notification is sent to one or more administrators in an Azure subscription. To ensure that notification can be successfully delivered, it is the customer's responsibility to ensure that the administrative contact information on each applicable subscription and online services portal is correct.

The data processor service for Windows Enterprise team may also elect to notify additional Microsoft personnel such as Customer Service (CSS) and the customer's Account Manager(s) (AM) or Technical Account Manager(s) (TAM). These individuals often have close relationships with the customer and can facilitate faster remediation.

For more information about how Microsoft detects and responds to a breach of personal data, see [Data Breach Notification Under the GDPR](#) in the Service Trust Portal.

# Data Protection Impact Assessment for the GDPR

2/5/2021 • 3 minutes to read • [Edit Online](#)

The General Data Protection Regulation (GDPR) introduces new rules for organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents no matter where you or your enterprise are located. Additional details can be found in the [GDPR Summary topic](#). This document guides you to information regarding Data Protection Impact Assessments (DPIAs) under the GDPR when using Microsoft products and services.

## Terminology

Helpful definitions for GDPR terms used in this document:

- *Data Controller (Controller)*: A legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- *Personal data* and *data subject*: Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly.
- *Processor*: A natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller.
- *Customer Data*: Data produced and stored in the day-to-day operations of running your business.

## What is a DPIA?

The GDPR requires controllers to prepare a Data Protection Impact Assessment (DPIA) for operations that are 'likely to result in a high risk to the rights and freedoms of natural persons.' There is nothing inherent in Microsoft products and services that need the creation of a DPIA. However, because Microsoft products and services are highly customizable, a DPIA may be needed depending on the details of your Microsoft configuration. Microsoft has no control over, and little or no insight into such information. You, as a data controller must determine appropriate uses of their data.

## DPIA in Action

The DPIA guidance applies to Office 365, Azure, Dynamics 365, and Microsoft Support and Professional Services. That guidance includes consideration of:

### When is a DPIA needed?

The risk factors listed below should be addressed when considering whether to complete a DPIA. Other potential factors and further details are found in Part 1 of each of the guidelines.

- A systematic and extensive evaluation of data based on automated processing.
- Processing on a large scale of special categories of data (data revealing information uniquely identifying a natural person), or of personal data relating to criminal convictions and offenses.
- Systematic monitoring of a publicly accessible area on a large scale.

The GDPR clarifies 'The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional, or lawyer. In such cases, a data protection impact assessment should not be mandatory.'

### What is required to complete a DPIA?

A DPIA should provide specific information about the intended processing, which is detailed in Part 2 of the guidance. That information includes:

- Assessment of the necessity, and proportionality of data processing in relation to the purpose of the DPIA.
- Assessment of the risks to the rights and freedoms of natural persons.
- Intended measures to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and demonstrate compliance with the GDPR.
- Purposes of processing
- Categories of personal data processed
- Data retention
- Location and transfers of personal data
- Data sharing with third-party subprocessors
- Data sharing with independent third-parties
- Data subject rights

## Additional Considerations

Specific details that may be relevant to your Microsoft implementation are below.

- [Office 365](#): This document applies to Office 365 applications and services, including but not limited to Exchange Online, SharePoint Online, Yammer, Skype for Business, and Power BI. Refer to Tables 1 and 2 for more details.
- [Azure](#): Customers are encouraged to work with their privacy officers and legal counsel to determine the necessity and content of any DPIAs related to their use of Microsoft Azure.
- [Dynamics 365](#): The contents of a DPIA may vary according to which Dynamics 365 tools you are employing. For specific details refer to [Part 2 Contents of a DPIA](#).
- [Microsoft Support and Professional Services](#): Professional Services does not conduct certain routine or automated data processing, nor is it intended to process special categories or perform tasks that facilitate or require monitoring of publicly accessible data. For details see [Part 1 — Determining Whether a DPIA is needed](#). Controllers must consider the DPIA elements outlined above, along with any other relevant factors, in the context of the controller's specific implementations and uses of Professional Services. For Professional Services information, see [Part 2 — Contents of a DPIA](#).

## Learn more

- [Microsoft Trust Center](#)



# Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Azure

2/9/2021 • 11 minutes to read • [Edit Online](#)

Under the General Data Protection Regulation (GDPR), data controllers are required to prepare a Data Protection Impact Assessment (DPIA) for processing operations that are "likely to result in a high risk to the rights and freedoms of natural persons." There is nothing inherent in Microsoft Azure itself that would necessarily require the creation of a DPIA by a data controller using it. Rather, whether a DPIA is required will be dependent on the details and context of *how* the data controller deploys, configures, and uses Microsoft Azure.

The purpose of this document is to provide data controllers with information about Microsoft Azure that will help them to determine whether a DPIA is needed and, if so, what details to include.

## NOTE

Microsoft is not providing any legal advice in this document. This document is being provided for informational purposes only. Customers are encouraged to work with their privacy officers and legal counsel to determine the necessity and content of any DPIAs related to their use of Microsoft Azure or any other Microsoft online service.

## Part 1: Determining whether a DPIA is needed

Article 35 of the GDPR requires a data controller to create a Data Protection Impact Assessment (DPIA) "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons." It further sets out particular factors that would indicate such a high risk, which is discussed in the following table: To determine whether a DPIA is needed, a data controller should consider these factors, along with any other relevant factors, in light of the controller's specific implementation(s) and use(s) of Microsoft Azure.

HIGH RISK FACTOR	RELEVANT INFORMATION ABOUT MICROSOFT AZURE
A systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.	Microsoft Azure does not provide capabilities to perform certain automated processing of data.  <i>However, because Azure is a highly customizable service, a data controller could potentially configure it to be used for such processing. Controllers should make this determination based on their usage of Azure.</i>
Processing on a large scale of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offenses.	Microsoft Azure is not designed to process special categories of personal data and the usage of Azure does not increase the inherent risk of a controller's processing.  <i>However, a data controller could use Microsoft Azure to process the enumerated special categories of data. Microsoft Azure is a highly customizable service that enables the customer to track or otherwise process any type of data, including special categories of personal data. But as the data processor, Microsoft has no control over such use and has little or no insight into such use. It is incumbent upon the data controller to determine appropriate uses of the data controller's data.</i>

HIGH RISK FACTOR	RELEVANT INFORMATION ABOUT MICROSOFT AZURE
<p>A systematic monitoring of a publicly accessible area on a large scale.</p>	<p>Microsoft Azure is not designed to conduct or facilitate such monitoring.</p> <p><i>However, a data controller could use Azure to process data collected through such monitoring. Microsoft Azure is a highly customizable service that enables the customer to track or otherwise process any type of data, including monitoring data. But as the data processor, Microsoft has no control over such use and has little or no insight into such use. It is incumbent upon the data controller to determine appropriate uses of the data controller's data.</i></p>

## Part 2: Contents of a DPIA

Article 35(7) mandates that a Data Protection Impact Assessment specifies the purposes of processing and a systematic description of the envisioned processing. A systematic description of a comprehensive DPIA might include factors such as the types of data processed, how long data is retained, where the data is located and transferred, and what third parties may have access to the data. In addition, the DPIA must include:

- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of natural persons; and
- the measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The following table contains information about Microsoft Azure that is relevant to each of those elements. As in Part 1, data controllers must consider the details provided in the table, along with any other relevant factors, in the context of the controller's specific implementation(s) and use(s) of Microsoft Azure.

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT MICROSOFT AZURE
-------------------	--

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT MICROSOFT AZURE
<p>Purpose(s) of processing</p>	<p>The purpose(s) of processing data using Microsoft Azure is determined by the controller that implements, configures, and uses it.</p> <p>As specified by the <a href="#">Online Services Terms</a> and <a href="#">Data Protection Addendum</a>, Microsoft, as a data processor, processes Customer Data to provide Customer the Online Services in accordance with Customer's documented instructions.</p> <p>As detailed in the standard <a href="#">Online Services Terms</a> and <a href="#">Data Protection Addendum</a>, Microsoft also uses Personal Data to support a limited set of legitimate business operations consisting of: (1) billing and account management; (2) compensation (for example, calculating employee commissions and partner incentives); (3) internal reporting and modeling (for example, forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy, or energy efficiency; and (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Customer Data outlined in the Online Service Terms).</p> <p>Microsoft is controller of the processing of personal data to support these specific legitimate business operations. Generally, Microsoft aggregates Personal Data before using it for our legitimate business operations, removing Microsoft's ability to identify specific individuals, and uses personal data in the least identifiable form that will support processing necessary for legitimate business operations.</p> <p>Microsoft will not use Customer Data or information derived from it for profiling or for advertising or similar commercial purposes.</p>

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT MICROSOFT AZURE
<p>Categories of personal data processed</p>	<p>*Customer Data—All data, including all text, sound, video, or image files, and software, that is provided to Microsoft by, or on behalf of, a customer through use of the enterprise service. Customer Data includes both (1) identifiable information of end users (for example, user names and contact information in Azure Active Directory) and customer content that a customer uploads into or creates in specific services (for example, customer content in an Azure Storage account, customer content of an Azure SQL Database, or a customer’s virtual machine image in Azure Virtual Machines).</p> <p>*Service-Generated Data—Logs and related data generated by Microsoft that help Microsoft provide enterprise services to users. Service-generated logs contain primarily pseudonymized data, associated with unique identifiers generated by the system, that cannot on their own identify an individual person but are used to deliver the enterprise services to users. These service-generated logs may also contain identifiable information about end users, such as a username.</p> <p>*Support Data—This is data provided to Microsoft by or on behalf of Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain technical support for Online Services.</p> <p>For more information regarding data processed by Azure, see the <a href="#">Online Services Terms</a>, including the Data Processing Agreement and <a href="#">Microsoft Trust Center</a>.</p>
<p>Data retention</p>	<p>Microsoft will retain and process Customer Data during the Customer’s right to use the Online Service and until all Customer Data is retrieved by Customer or deleted in accordance with the terms of the OST. During the term of Customer’s subscription, the Customer will have the ability to access and extract Customer Data stored in each Online Service. Except for free trials and LinkedIn services, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer’s subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer’s account and delete the Customer Data. The customer can delete personal data pursuant to a Data Subject Request using the capabilities described in the <a href="#">Azure Data Subject Request GDPR Documentation</a>.</p>

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT MICROSOFT AZURE
<p>Location and transfers of personal data</p>	<p>Customers have the ability to provision Customer Data at rest within specified <a href="#">geographic regions</a>, subject to certain exceptions as set out in the OST. Additional details regarding service deployments and data residency can also be found in the <a href="#">Microsoft Data Protection Addendum (DPA)</a> to the Online Services Terms (OST) and on the <a href="#">Azure Global Infrastructure</a> webpage.</p> <p>For personal data from the European Economic Area, Switzerland, and the United Kingdom, Microsoft will ensure that transfers of Personal Data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. In addition to Microsoft's commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft continues to abide by the terms of the <a href="#">Privacy Shield framework</a> but will no longer rely on it as a basis for the transfer of personal data from the EU/EEA to the United States.</p>
<p>Data sharing with third-party subprocessors</p>	<p>Microsoft shares data with third parties acting as our subprocessors to support functions such as customer and technical support, service maintenance, and other operations. Any subcontractors to which Microsoft transfers Customer Data, Support Data, or Personal Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the <a href="#">Online Services Terms</a>. All third-party subprocessors with which Customer Data from Microsoft's Core Online Services is shared are included in the Online Services Subcontractor list. All third-party subprocessors that may access Support Data (including Customer Data that customers choose to share during their support interactions) are included in the <a href="#">Microsoft Commercial Support Contractors</a> list.</p>

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT MICROSOFT AZURE
<p>Data subject rights</p>	<p>When operating as a processor, Microsoft makes available to the customer (also known as the data controller) the personal data of its data subjects and the ability to fulfill data subject requests when they exercise their rights under the GDPR. Microsoft does so in a manner consistent with the functionality of the product and its role as a data processor. If Microsoft receives a request from the customer's data subjects to exercise one or more of its rights under the GDPR, the request will be redirected to the data controller.</p> <p>The Azure Data Subject Requests Guide provides a description to the data controller on how to support data subject rights using the capabilities in Azure.</p> <p>Requests from a data subject to exercise rights under the GDPR for personal data processed to support the legitimate business processes should be directed to Microsoft, as clarified in the Microsoft Privacy Statement.</p> <p>Microsoft generally aggregates personal before using it for our legitimate business operations and is not in a position to identify personal data for a specific individual in the aggregate. This action significantly reduces the privacy risk to the individual. Where Microsoft is not in a position to identify the individual, it cannot support data subject rights for access, erasure, portability, or the restriction or objection of processing.</p> <p>The <a href="#">Azure Data Subject Request GDPR Documentation</a> provides a description of how to support data subject rights using the capabilities in Azure.</p>
<p>An assessment of the necessity and proportionality of the processing operations in relation to the purposes</p>	<p>Such an assessment will depend on the data controller's needs and purposes of processing.</p> <p>Microsoft takes measures such as the anonymization or aggregation of personal data used by Microsoft to support legitimate business operations to support provision of the services, minimizing the risk of such processing to data subjects that use the service.</p> <p>Regarding the processing carried out by Microsoft, such processing is necessary and proportional for providing the services to the data controller. Microsoft makes this commitment in the OST.</p>
<p>An assessment of the risks to the rights and freedoms of data subjects</p>	<p>The key risks to the rights and freedoms of data subjects from the use of Microsoft Azure will be a function of how and in what context the data controller implements, configures, and uses Microsoft Azure.</p> <p>However, as with any service, personal data held in the service may be at risk of unauthorized access or inadvertent disclosure. Measures Microsoft takes to address such risks are discussed in the OST, as further detailed later in this article.</p>

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT MICROSOFT AZURE
<p>The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned</p>	<p>Microsoft is committed to helping protect the security of Customer Data. The security measures Microsoft takes are described in detail in the OST.</p> <p>Microsoft complies with strict security standards and industry-leading data protection methodology. Microsoft is continually improving its systems to deal with new threats. More information regarding cloud governance and privacy practices is available at <a href="#">Trust Center's Cloud Governance &amp; Privacy</a> page.</p> <p>Microsoft takes reasonable and appropriate technical and organizational measures to safeguard the personal data that it processes. These measures include, but are not limited to, internal privacy policies and practices, contractual commitments, and international and regional standard certifications. More information is available at <a href="#">Trust Center's Privacy Standards</a> page.</p> <p>Microsoft provides significant, transparent customer facing security and privacy materials to help explain Microsoft's use and processing of personal data. Customers are encouraged to contact Microsoft with questions.</p> <p>Further, Microsoft complies with all other GDPR obligations that apply to data processors, including but not limited to, data protection impact assessments and record keeping.</p> <p>Where Microsoft processes personal data for its legitimate business operations, it complies with GDPR obligations that apply to data controllers.</p>

## Learn more

- [Microsoft Trust Center](#)

# Data Protection Impact Assessments: Guidance for Data Controllers Using Dynamics 365

2/18/2021 • 13 minutes to read • [Edit Online](#)

Under the General Data Protection Regulation (GDPR), data controllers are required to prepare a Data Protection Impact Assessment (DPIA) for processing operations that are 'likely to result in a high risk to the rights and freedoms of natural persons.' There is nothing inherent in Dynamics 365 that would necessarily require the creation of a DPIA by a Data Controller using it. Rather, whether a DPIA is required will be dependent on the details and context of *how* the data controller deploys, configures, and uses Dynamics 365

The purpose of this document is to provide data controllers with information about Dynamics 365 that will help them to determine whether a DPIA is needed and, if so, what details to include.

## Part 1: Determining whether a DPIA is needed

Article 35 of the GDPR requires a data controller to create a Data Protection Impact Assessment '[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.' It further sets out particular factors that would indicate such a high risk, which are discussed in the following table: In determining whether a DPIA is needed, a data controller should consider these factors, along with any other relevant factors, in light of the controller's specific implementation(s) and use(s) of Dynamics 365.

RISK FACTOR	RELEVANT INFORMATION ABOUT DYNAMICS 365
A systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;	Dynamics 365 does perform certain automated processing of data, such as lead or opportunity scoring (for example, predicting how likely a sale is to occur). But it is not designed to perform processing on which decisions are based that produce legal or similarly significant effects on individuals.  However, because Dynamics 365 is a highly customizable service, a data controller could potentially configure it to be used for such processing, such as scoring for employment decisions or credit applications.
Processing on a large scale <sup>1</sup> of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offenses;	Dynamics 365 is not specifically designed to process special categories of personal data.  However, a data controller <i>could</i> use Dynamics 365 to process the enumerated special categories of data. For instance, Dynamics 365 offers healthcare industry templates which could be used to process personal data associated with a health condition. Further, Dynamics 365 is a highly customizable service that enables the customer to track or otherwise process any type of personal data, including special categories of personal data. But as the data processor, Microsoft has no control over such use and typically would have little or no insight into such use.



RISK FACTOR	RELEVANT INFORMATION ABOUT DYNAMICS 365
A systematic monitoring of a publicly accessible area on a large scale	<p>Dynamics 365 is not designed to conduct or facilitate such monitoring.</p> <p>However, a data controller could use it to process data collected through such monitoring.</p>

#### NOTE

<sup>1</sup> With respect to the criteria that the processing be on a 'large scale,' Recital 91 of the GDPR clarifies that: 'The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional, or lawyer. In such cases, a data protection impact assessment should not be mandatory.'

## Part 2: Contents of a DPIA

Article 35(7) mandates that a Data Protection Impact Assessment specifies the purposes of processing and a systematic description of the envisioned processing. A systematic description of a comprehensive DPIA might include factors such as the types of data processed, how long data is retained, where the data is located and transferred, and what third parties may have access to the data. In addition, the DPIA must include:

- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of natural persons; and
- the measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The table below contains information about Dynamics 365 that is relevant to each of those elements. As in Part 1, data controllers must consider the details provided below, along with any other relevant factors, in the context of the controller's specific implementation(s) and use(s) of Dynamics 365.

ELEMENTS OF A DPIA	RELEVANT INFORMATION ABOUT DYNAMICS 365
Purpose(s) of processing	<p>The purpose(s) of processing data using Dynamics 365 is determined by the controller that implements, configures, and uses it.</p> <p>Dynamics 365 is an online platform for processing that is made up of several discrete online services, each of which has distinct purposes of processing. Below are the types of services offered by Dynamics365:</p> <p><b>Customer Engagement</b> at its core is a customer relationship management service. It includes the following online services: Dynamics 365 for Sales, Dynamics 365 for Marketing, Dynamics 365 for Customer Service, Dynamics 365 for Project Service, and Dynamics 365 for Field Service.</p> <p><b>Dynamics 365 for Finance and Operations, Enterprise edition (D365FOEE)</b> is an enterprise resource planning suite offered as a software as a service (SaaS), that is provided primarily to enterprise customer management of Sales, Service, Finance and Operations, Manufacturing and Human Resources.</p> <p><b>Dynamics 365 for Retail (D365FR)</b> is offered as a software as a service (SaaS) with integrated on-premise point-of-sale</p>

**Dynamics 365 Lifecycle Services (LCS)** is an ancillary online service, used primarily by enterprise customers in the deployment, management, and maintenance of the customer's D365FOEE, D365FR implementations.

**Dynamics 365 for Business Central** is an enterprise resource planning offering, provided as a Software as a Service (SaaS) by Microsoft to small and medium-sized enterprises. The service processes personal data to assist with finance, manufacturing, customer relationship management, supply chains, analytics, and electronic commerce.

**Dynamics 365 for Talent** is offered as a software as a service (SaaS), that provides customers with the management of Human resources and consists of the following services:

*Core HR*— A service to streamline recordkeeping tasks and automate processes related to staffing an organization. These processes include employee retention, benefits administration, compensation, training, performance reviews, and change management.

*Attract* - a service to find, interview, and hire personnel.

*Onboarding* - a service to help onboard new hires into their job\*.

**Microsoft Social Engagement (MSE)** is an ancillary service to Dynamics 365 offered to enterprise customers to (i) enable processing of public social media posts and personal data posted by data subjects in a limited number of social media outlets to help them analyze and identify topics of interest (for example, trends), and manage corporate or institutional presence in these virtual places (for example, fan pages), including publishing content to specific social media outlets (listen); and (ii) engage directly with data subjects via private communications in social media (engage).

In its processor capacity operating the services enumerated above, Dynamics 365 processes personal data only to provide customers its online services as described, including purposes compatible with providing those services such as personalization, security, fraud and malware prevention, troubleshooting and improvement.

As specified by the [Online Services Terms](#) and [Data Protection Addendum](#), Microsoft, as a data processor, processes Customer Data to provide Customer the Online Services in accordance with Customer's documented instructions.

As detailed in the standard [Online Services Terms](#) and [Data Protection Addendum](#), Microsoft also uses Personal Data to support a limited set of legitimate business operations consisting of: (1) billing and account management; (2) compensation (for example, calculating employee commissions and partner incentives); (3) internal reporting and modeling (for example, forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy, or energy efficiency; and (6) financial

ELEMENTS OF A DPIA	<p>reporting and compliance with legal obligations (subject to the limitations on disclosure of Customer Data outlined in the Online Service Terms).</p>
	<p>Microsoft is controller of the processing of personal data to support these specific legitimate business operations. Generally, Microsoft aggregates Personal Data before using it for our legitimate business operations, removing Microsoft's ability to identify specific individuals, and uses personal data in the least identifiable form that will support processing necessary for legitimate business operations.</p> <p>Microsoft will not use Customer Data or information derived from it for profiling or for advertising or similar commercial purposes.</p>
Categories of personal data processed	<p><b>Customer Data:</b> This is all data, including text, sound, video, or image files and software, that customers provide to Microsoft or that is provided on customers' behalf through their use of Microsoft online services. It includes data that customers upload for storage or processing, as well as customizations. Examples of Customer Data processed in Office 365 include email content in Exchange Online, and documents or files stored in SharePoint Online or OneDrive for Business.</p> <p><b>Service-Generated Data:</b> This is data that is generated or derived by Microsoft through operation of the service, such as use or performance data. Most of these data contain pseudonymous identifiers generated by Microsoft.</p> <p><b>Support Data:</b> This is data provided to Microsoft by or on behalf of Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain technical support for Online Services.</p> <p>Customer Data, System-generated Log Data, and Support Data do not include administrator and billing data, such as customer administrator contact information, subscription information, and payment data, which Microsoft collects and processes in its capacity as a data controller and which is outside the scope of this document.</p>
Data retention	<p>Microsoft will retain Customer Data for the duration of the customer's right to use the service and until all Customer Data is deleted or returned in accordance with the customer's instructions or the terms of the Online Services Terms. At all times during the term of the customer's subscription, the customer will have the ability to access and extract Customer Data stored in the service. Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the Customer Data.</p> <p>The customer can delete Customer Data and Pseudonymous data at any time using the capabilities described in the Dynamics' <a href="#">Data Subject Rights Guide</a>.</p>

ELEMENTS OF A DPIA	RELEVANT INFORMATION ABOUT DYNAMICS 365
<p>Location and transfers of personal data</p>	<p>If Customer provisions its instance of Dynamics 365 Core Services in Australia, Canada, the European Union, India, Japan, the United Kingdom, or the United States, Microsoft will store Customer Data at rest within the specified geographic area, subject to certain exceptions as set out in the Online Services Terms. Detailed information about Customer Data storage can be found in the <a href="#">Trust Center</a>.</p> <p>For personal data from the European Economic Area, Switzerland, and the United Kingdom, Microsoft will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. In addition to Microsoft's commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft continues to abide by the terms of the <a href="#">Privacy Shield framework</a> but will no longer rely on it as a basis for the transfer of personal data from the EU/EEA to the United States.</p>
<p>An assessment of the necessity and proportionality of the processing operations in relation to the purposes</p>	<p>Such an assessment will depend on the controller's needs and purposes of processing.</p> <p>In its processor capacity, Microsoft offers D365 to process personal data only to provide customers its online services, including purposes compatible with providing those services such as personalization to the customer, security, fraud and malware prevention, troubleshooting and improvement. Microsoft processes data on behalf of the customer (tenant) as necessary to provide the requested service as set forth in our Online Services Terms found at <a href="https://microsoft.com/licensing/contracts">https://microsoft.com/licensing/contracts</a>.</p>
<p>An assessment of the risks to the rights and freedoms of data subjects</p>	<p>The key risks to the rights and freedoms of data subjects from the use of Dynamics 365 will be a function of how and in what context the data controller implements, configures, and uses it.</p> <p>Microsoft takes measures such as the anonymization or aggregation of personal data used by Microsoft to support legitimate business operations to support provision of the services, minimizing the risk of such processing to data subjects that use the service.</p> <p>However, as with any service, personal data held in the service may be at risk of unauthorized access or inadvertent disclosure. Measures Microsoft takes to address such risks are discussed below.</p>

ELEMENTS OF A DPIA	RELEVANT INFORMATION ABOUT DYNAMICS 365
Data sharing with third-party subprocessors	<p>Microsoft shares data with third parties acting as our subprocessors to support functions such as customer and technical support, service maintenance, and other operations. Any subcontractors to which Microsoft transfers Customer Data, Support Data or Personal Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the Online Services Terms. All third-party subprocessors with which Customer Data from Microsoft's Core Online Services is shared are included in the Online Services Subcontractor list. All third-party subprocessors that may access Support Data (including Customer Data that customers choose to share during their support interactions) are included in the Microsoft Commercial Support Contractors list.</p>
Data subject rights	<p>When operating as a processor, Microsoft makes available to customers (data controllers) the personal data of its data subjects and the ability to fulfill data subject requests when they exercise their rights under the GDPR. We do so in a manner consistent with the functionality of the product and our role as a processor. If we receive a request from the customer's data subjects to exercise one or more of its rights under the GDPR, we redirect the data subject to make its request directly to the data controller. The Dynamics 365 Data Subject Requests for the GDPR and CCPA provides a description to the data controller on how to support data subject rights using the capabilities in Dynamics 365.</p> <p>Requests from a data subject to exercise rights under the GDPR for personal data processed to support the legitimate business processes should be directed to Microsoft, as clarified in the Microsoft Privacy Statement.</p> <p>Microsoft generally aggregates personal before using it for our legitimate business operations and is not in a position to identify personal data for a specific individual in the aggregate. This significantly reduces the privacy risk to the individual. Where Microsoft is not in a position to identify the individual, it cannot support data subject rights for access, erasure, portability, or the restriction or objection of processing.</p>

ELEMENTS OF A DPIA	RELEVANT INFORMATION ABOUT DYNAMICS 365
<p>The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned</p>	<p>Microsoft is committed to helping protect the security of Customer's information. In compliance with the provisions of Article 32 of the GDPR, Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data and Support Data against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction.</p> <p>For detailed list of Microsoft-managed controls (technical and business process controls) for security implemented by Dynamics 365 please visit the <a href="#">Service Trust Portal</a>. Further, Microsoft complies with all other GDPR obligations that apply to data processors, including but not limited to, providing data protection impact assessments and accurate record keeping.</p> <p>Where Microsoft processes personal data for its legitimate business operations, it complies with GDPR obligations that apply to data controllers.</p>

## Learn more

- [Microsoft Trust Center](#)

# Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Professional Services

2/18/2021 • 11 minutes to read • [Edit Online](#)

## Introduction to Microsoft Professional Services

Microsoft Professional Services includes a diverse group of technical architects, engineers, consultants, and support professionals dedicated to delivering on Microsoft's mission of empowering customers to do more and achieve more. Find out more about Microsoft Professional Services by visiting the [Microsoft Professional Services Trust page](#).

Microsoft Professional Services takes its obligations under the General Data Protection Regulation (GDPR) seriously. The information in this document is designed to provide information about how Microsoft's support and consulting offerings that customers can use when preparing Data Protection Impact Assessments (DPIAs) under GDPR.

### Introduction to DPIAs

Under the General Data Protection Regulation (GDPR), data controllers are required to prepare a DPIA for processing operations that are "likely to result in a high risk to the rights and freedoms of natural persons." There is nothing inherent in Microsoft Professional Services that would necessarily require the creation of a DPIA by a data controller using it. Rather, whether a DPIA is required will be dependent on the details and context of the type of services and how the data controller uses the professional services.

The purpose of this document is to provide data controllers with information about Professional Services that will help them to determine whether a DPIA is needed and, if so, what details to include.

## Part 1: Determining whether a DPIA is needed

Article 35 of the GDPR requires a data controller to create a Data Protection Impact Assessment "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons." It further sets out particular factors that would indicate such a high risk, which is discussed in the following table: In determining whether a DPIA is needed, a data controller should consider these factors, along with any other relevant factors, in light of the data controller's specific implementation(s) and use(s) of Professional Services.

RISK FACTOR	RELEVANT INFORMATION ABOUT PROFESSIONAL SERVICES
A systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;	Professional Services does perform certain routine or automated processing of data, such as break/fix support (for example, assisting customers when their computer breaks), account migration, and analysis of system vulnerabilities. Professional Services solutions, excluding customer development covered under the note later in this table, are not intended to perform processing on which decisions are based that produce legal or similarly significant effects on individuals.

RISK FACTOR	RELEVANT INFORMATION ABOUT PROFESSIONAL SERVICES
<p>Processing on a large scale <sup>1</sup> of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offenses;</p>	<p>Professional Services are not intended to be utilized in work that requires the processing of special categories of personal data, excluding customer development covered under the note later in this table.</p> <p>However, a data controller could use Professional Services consulting solutions to process the enumerated special categories of data. For instance, Professional Services offers healthcare industry database development that could be used by a data controller to process personal data associated with a health condition. It is the responsibility of the controller to assess and either restrict or document this usage as appropriate.</p>
<p>A systematic monitoring of a publicly accessible area on a large scale</p>	<p>Professional Services are not intended to be utilized in work that requires or facilitates such monitoring, excluding customer development covered under the note later in this table.</p> <p>If a data controller used Professional Services to develop this type of system or used IT systems to process data collected through such monitoring, then it would be the responsibility of the data controller as described later in this table.</p>

**NOTE**

<sup>1</sup> With respect to the criteria that the processing be on a "large scale," Recital 91 of the GDPR clarifies that: "The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional, or lawyer. In such cases, a data protection impact assessment should not be mandatory."

[Custom Development Note] Professional Services offers a wide variety of consulting solutions. A data controller could potentially request a solution that, in accordance with the above criteria, would be a high-risk solution. For instance, a data controller may request that Professional Services create a solution to develop a business intelligence engine for employment decisions or credit applications or a solution that involves user tracking, specialized use of Artificial Intelligence (AI)/Analytics, or processing of special categories of personal data.

At the start of an engagement, Professional Services has processes to evaluate and address high-risk solutions it may be asked to work on. As part of this, Professional Services may require assurances from the data controller on GDPR compliance (for example, contractual terms), a plan for development of a DPIA, or other criteria (for example, agreed operating guidelines) as required of a data processor under the GDPR. However, regardless of Microsoft's actions it is the responsibility of the data controller to develop the DPIA with input where applicable from the processor of the customer's data.

## Part 2: Contents of a DPIA

Article 35(7) mandates that a Data Protection Impact Assessment specifies the purposes of processing and a systematic description of the envisioned processing. A systematic description of a comprehensive DPIA might include factors such as the types of data processed, how long data is retained, where the data is located and transferred, and what third parties may have access to the data. In addition, the DPIA must include:

- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;



- an assessment of the risks to the rights and freedoms of natural persons; and
- the measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The following table contains information about Professional Services that is relevant to each of those elements. As in Part 1, data controllers must consider the details provided in the table, along with any other relevant factors, in the context of the controller’s specific implementation(s) and use(s) of Professional Services.

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT PROFESSIONAL SERVICES
Purpose(s) of processing	<p>The purpose(s) of processing data using Professional Services is determined by the controller that implements, configures, and uses it.</p> <p>As specified by the <a href="#">Microsoft Professional Services Data Protection Addendum (MPSDPA)</a>, Microsoft, as a data processor, processes Support and Consulting Data only to provide the requested services to our customer, the data controller. Microsoft will not use Support and Consulting Data or information derived from it for any advertising or similar commercial purposes.</p>
The purpose(s) of processing data using Professional Services is determined by the controller that implements, configures, and uses it.	<p>As specified by the <a href="#">Microsoft Professional Services Data Protection Addendum (MPSDPA)</a>, Microsoft, as a data processor, processes Support and Consulting Data only to provide the requested services to our customer, the data controller. Microsoft will not use Support and Consulting Data or information derived from it for any advertising or similar commercial purposes.</p>
Categories of personal data processed	<p>Support and Consulting data means all data, including all text, sound, video, image files, or software, that are provided to Microsoft by, or on behalf of, Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain Professional Services or Support. This may include information collected over phone, chat, e-mail, or web form. It may include description of problems, files transferred to Microsoft to resolve support issues, automated troubleshooters, or by accessing customer systems remotely with customer permission.</p> <p>Customer Data and Support Data do not include customer contact or billing data, such as subscription information, and payment data, which Microsoft collects and processes in its capacity as a data controller and which is outside the scope of this document.</p>

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT PROFESSIONAL SERVICES
Data retention	<p>Microsoft will retain Support and Consulting Data for the duration of the customer engagement plus a retention period after the engagement ends as necessary to ensure quality and continuity of service. As an example, after a support case is closed the data is normally retained for a period to ensure the ability to reference it if the issue re-emerges and the case is reopened.</p> <p>When Professional Services provides support, the engagement length is defined when the support case is closed. When Professional Services provides consulting services, the engagement length is often defined by the work order. In other cases, the engagement length is defined by the maintenance of the business relationship. In all cases, Support and Consulting Data will be deleted or returned on request or in accordance with the customer's instructions without undue delay using the capabilities described in the Professional Services <a href="#">Data Subject Rights Guide</a>.</p>
Location and transfers of personal data	<p>Due to the nature of Professional Services, including the need to provide round-the-clock support, data may be transferred worldwide. A list of locations Microsoft operates in is available on request. For consulting services, data may be held in-country if agreed to within the work order.</p> <p>For personal data from the European Economic Area, Switzerland, and the United Kingdom, Microsoft will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. In addition to Microsoft's commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft continues to abide by the terms of the <a href="#">Privacy Shield framework</a> but will no longer rely on it as a basis for the transfer of personal data from the EU/EEA to the United States.</p>

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT PROFESSIONAL SERVICES
Data sharing with third parties	<p>Microsoft shares data with third parties acting as our sub-processors to support functions such as customer and technical support, service maintenance, and other operations. Any subcontractors to which Microsoft transfers Support and Consulting Data will have entered into written agreements with Microsoft that are no less protective than the data protection terms of the <a href="#">MPSDPA</a>. All third-party sub-processors with which Support and Consulting Data is shared under the <a href="#">MPSDPA</a> are included in the <a href="#">Microsoft Commercial Support Contractors List</a>.</p> <p>Microsoft will not disclose Support and Consulting Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Support and Consulting Data, Microsoft will attempt to redirect the law enforcement agency to request the data directly from the customer. If compelled to disclose Support and Consulting Data to law enforcement, Microsoft will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so.</p> <p>Upon receipt of any other third-party request for Support and Consulting Data, Microsoft will promptly notify the customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from the customer.</p>
Data subject rights	<p>When operating as a processor, Microsoft makes available to customer (data controllers) the personal data of its data subjects and the ability to fulfill data subject requests when they exercise their rights under the GDPR. We do so in a manner consistent with the functionality of the product and our role as a processor. If we receive a request from the customer's data subject to exercise one or more of its rights under the GDPR, we redirect the data subject to make its request directly to the data controller.</p> <p>The <a href="#">Professional Services Data Subject Request GDPR Documentation</a> provides a description of how the customer can address their data subject rights obligations in Professional Services.</p>
An assessment of the necessity and proportionality of the processing operations in relation to the purposes	<p>Such an assessment will depend on the controller's needs and purposes of processing.</p> <p>With regard to the processing carried out by Microsoft, such processing is necessary and proportional for the purpose of providing the services to the data controller. Microsoft commits to this in the <a href="#">MPSDPA</a>.</p>

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT PROFESSIONAL SERVICES
<p>An assessment of the risks to the rights and freedoms of data subjects</p>	<p>The key risks to the rights and freedoms of data subjects from the use of Professional Services will be a function of how and in what context the data controller implements, configures, and uses the professional services and any solutions provided by Professional Services.</p> <p>However, as with any service, personal data held in the service may be at risk of unauthorized access or inadvertent disclosure. Measures Microsoft takes to address such risks are discussed later in this article.</p>
<p>The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.</p>	<p>Microsoft is committed to helping protect the security of customer information. In compliance with the provisions of Article 32 of the GDPR, Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Support and Consulting Data against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction.</p> <p>Further, Microsoft complies with all other GDPR obligations that apply to data processors, including but not limited to, data protection impact assessments and record keeping.</p>

## Learn more

- [Microsoft Professional Services Trust](#)

# Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Office 365

2/18/2021 • 14 minutes to read • [Edit Online](#)

Under the General Data Protection Regulation (GDPR), data controllers are required to prepare a Data Protection Impact Assessment (DPIA) for processing operations that are 'likely to result in a high risk to the rights and freedoms of natural persons'. There is nothing inherent in Microsoft Office 365 that would necessarily require the creation of a DPIA by a data controller using it. Rather, whether a DPIA is required will be dependent on the details and context of how you, as the data controller, deploy, configure, and use Office 365.

Part 1 of this document provides information about Office 365 to help you, as a data controller, determine whether a DPIA is needed. If the answer is 'yes,' Parts 2 and 3 of this document provide key information from Microsoft that can help draft it. Specifically, Part 2 provides answers applicable to all Office 365 services for each of the required elements of a DPIA. Part 3 provides additional product-specific information for a number of the most relevant information needs of our customers for purposes of drafting their own DPIAs. Part 3 also includes an illustrative DPIA document that you can download and modify to make drafting DPIAs easier for you.

Office 365 applications and services, include, but are not limited to, Exchange Online, SharePoint Online, OneDrive for Business, Yammer, and Microsoft Teams. A more complete list of services available through Office 365 can be seen in Tables 1 and 2 of the [Office 365 Data Subject Request Guide](#).

## Part 1: Determining whether a DPIA is needed

Article 35 of the GDPR requires a data controller to create a Data Protection Impact Assessment 'where a type of processing in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.' It further sets out particular factors that would indicate such a high risk, which are discussed in the following table. In determining whether a DPIA is needed, you, as a data controller should consider these factors, along with any other relevant factors, in light of the controller's specific implementation(s) and use(s) of Office 365.

RISK FACTOR	RELEVANT INFORMATION ABOUT OFFICE 365
A systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person	<p>Depending upon the data controller's configuration, Office 365 may perform certain automated processing of data, such as the analysis performed by Workplace Analytics that allows the data controller to derive insights on how people collaborate within an organization based on email and calendar header information from user's mailboxes.</p> <p>Office 365 is not designed to perform automated processing as the basis for decisions that produce legal or similarly significant effects on individuals. However, because Office 365 is a highly customizable service, a data controller could potentially use it for such processing.</p>

RISK FACTOR	RELEVANT INFORMATION ABOUT OFFICE 365
<p>Processing on a large scale <sup>1</sup> of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offenses</p>	<p>Office 365 is not designed to process special categories of personal data.</p> <p>However, a data controller could use Office 365 to process the enumerated special categories of data. Office 365 is a highly customizable service that enables the customer to track or otherwise process any type of personal data, including special categories of personal data. Any such use is relevant to a controller's determination of whether a DPIA is needed. But as the data processor, Microsoft has no control over such use and typically would have little or no insight into such use.</p>
<p>A systematic monitoring of a publicly accessible area on a large scale</p>	<p>Office 365 is not designed to conduct or facilitate such monitoring.</p> <p>However, a data controller could use it to process data collected through such monitoring.</p>

**NOTE**

<sup>1</sup> With respect to the criteria that the processing be on a "large scale," Recital 91 of the GDPR clarifies that: "The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional, or lawyer. In such cases, a data protection impact assessment should not be mandatory."

## Part 2: Contents of a DPIA

GDPR Article 35(7) mandates that a Data Protection Impact Assessment specifies the purposes of processing and a systematic description of the envisioned processing. In Microsoft's DPIAs, such systematic description includes factors such as the types of data processed, how long data is retained, where the data is located and transferred, and what third parties may have access to the data. In addition, the DPIA must include:

- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of natural persons; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the General Data Protection Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The following table provides key information from Microsoft that can help with your DPIA drafting. It contains information about Office 365 that is relevant to each of the required elements of a DPIA. As in Part 1, data controllers must consider the details provided below, along with the details of its own specific implementation(s) and use(s) of Office 365.

RISK FACTORS	RELEVANT INFORMATION ABOUT OFFICE 365

RISK FACTORS	RELEVANT INFORMATION ABOUT OFFICE 365
<p>Purpose(s) of processing</p>	<p>The purpose(s) of processing data using Office 365 is determined by the controller that implements, configures, and uses it.</p> <p>As specified by the <a href="#">Online Services Terms</a> and <a href="#">Data Protection Addendum</a>, Microsoft, as a data processor, processes Customer Data to provide Customer the Online Services in accordance with Customer's documented instructions.</p> <p>As detailed in the standard <a href="#">Online Services Terms</a> and <a href="#">Data Protection Addendum</a>, Microsoft also uses Personal Data to support a limited set of legitimate business operations consisting of: (1) billing and account management; (2) compensation (for example, calculating employee commissions and partner incentives); (3) internal reporting and modeling (for example, forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy, or energy efficiency; and (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Customer Data outlined in the Online Service Terms).</p> <p>Microsoft is controller of the processing of personal data to support these specific legitimate business operations. Generally, Microsoft aggregates Personal Data before using it for our legitimate business operations, removing Microsoft's ability to identify specific individuals, and uses personal data in the least identifiable form that will support processing necessary for legitimate business operations.</p> <p>Microsoft will not use Customer Data or information derived from it for profiling or for advertising or similar commercial purposes.</p>

RISK FACTORS	RELEVANT INFORMATION ABOUT OFFICE 365
Categories of personal data processed	<p><b>Customer Data:</b> This is all data, including text, sound, video, or image files and software, that customers provide to Microsoft or that is provided on customers' behalf through their use of Microsoft online services. It includes data that customers upload for storage or processing, as well as customizations. Examples of Customer Data processed in Office 365 include email content in Exchange Online, and documents or files stored in SharePoint Online or OneDrive for Business.</p> <p><b>Service-generated Data:</b> This is data that is generated or derived by Microsoft through operation of the service, such as use or performance data. Most of these data contain pseudonymous identifiers generated by Microsoft.</p> <p><b>Diagnostic Data:</b> This data is collected or obtained by Microsoft from software that is locally installed by Customer in connection with the Online Service and may also be referred to as telemetry. This data is commonly identified by attributes of the locally installed software or the machine that runs that software.</p> <p><b>Support Data:</b> This is data provided to Microsoft by or on behalf of Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain technical support for Online Services.</p> <p>Customer Data, System-generated Log Data, and Support Data do not include administrator and billing data, such as customer administrator contact information, subscription information, and payment data, which Microsoft collects and processes in its capacity as a data controller and which is outside the scope of this document.</p>



RISK FACTORS	RELEVANT INFORMATION ABOUT OFFICE 365
<p>Data retention</p>	<p><b>Customer Data:</b> As set out in the Data Protection Terms in the Online Services Terms, Microsoft will retain Customer Data for the duration of the customer's right to use the service and until all Customer Data is deleted or returned in accordance with the customer's instructions or the terms of the Online Services Terms.</p> <p>At all times during the term of the customer's subscription, the customer will have the ability to access, extract, and delete Customer Data stored in the service, subject in some cases to specific product functionality intended to mitigate the risk of inadvertent deletion (for example, Exchange recovered items folder), as further described in product documentation.</p> <p>Except for free trials and LinkedIn services, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the Customer Data.</p> <p><b>Service-generated Data:</b> This data is retained for a default period of up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.</p> <p>For further information about service capability that enables the customer to delete personal data maintained in the service at any time, see the <a href="#">Office 365 Data Subject Requests Guide</a>.</p>
<p>Location and transfers of personal data</p>	<p>As described in Attachment 1 of the Online Services Terms, if Customer provisions its instance of Office 365 in Australia, Canada, the European Union, France, India, Japan, South Korea, the United Kingdom, or the United States, Microsoft will store the following Customer Data at rest only within that location: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, (3) files uploaded to OneDrive for Business, and (4) project content uploaded to Project Online.</p> <p>For personal data from the European Economic Area, Switzerland, and the United Kingdom, Microsoft will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. In addition to Microsoft's commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft continues to abide by the terms of the <a href="#">Privacy Shield framework</a> but will no longer rely on it as a basis for the transfer of personal data from the EU/EEA to the United States.</p>

RISK FACTORS	RELEVANT INFORMATION ABOUT OFFICE 365
<p>Data sharing with third-party subprocessors</p>	<p>Microsoft shares data with third parties acting as our subprocessors to support functions such as customer and technical support, service maintenance, and other operations. Any subcontractors to which Microsoft transfers Customer Data, Support Data, or Personal Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the <a href="#">Online Services Terms</a>. All third-party subprocessors with which Customer Data from Microsoft's Core Online Services is shared are included in the <a href="#">Online Services Subcontractor list</a>. All third-party subprocessors that may access Support Data (including Customer Data that customers choose to share during their support interactions) are included in the <a href="#">Microsoft Commercial Support Contractors list</a>.</p>
<p>Data sharing with independent third-parties</p>	<p>Some Office 365 products include extensibility options that enable, at the controller's election, sharing of data with independent third parties. For example, Exchange Online is an extensible platform that allows third-party add-ins or connectors to integrate with Outlook and extend Outlook's feature sets. These third-party providers of add-ins or connectors act independently of Microsoft, and their add-ins or connectors must be enabled by the users or enterprise administrators, who authenticate with their add-in or connector account.</p> <p>Microsoft will not disclose Customer Data or Support Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data or Support Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data or Support Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.</p> <p>Upon receipt of any other third-party request for Customer Data or Support Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from the customer.</p>

RISK FACTORS	RELEVANT INFORMATION ABOUT OFFICE 365
Data subject rights	<p>When operating as a processor, Microsoft makes available to customers (data controllers) the personal data of its data subjects and the ability to fulfill data subject requests when they exercise their rights under the GDPR. We do so in a manner consistent with the functionality of the product and our role as a processor. If we receive a request from the customer's data subjects to exercise one or more of its rights under the GDPR, we redirect the data subject to make its request directly to the data controller. The Office 365 Data Subject Requests Guide provides a description to the data controller on how to support data subject rights using the capabilities in Office 365.</p> <p>Requests from a data subject to exercise rights under the GDPR for personal data processed to support the legitimate business processes should be directed to Microsoft, as clarified in the <a href="#">Microsoft Privacy Statement</a>.</p> <p>Microsoft generally aggregates personal before using it for our legitimate business operations and is not in a position to identify personal data for a specific individual in the aggregate. This significantly reduces the privacy risk to the individual. Where Microsoft is not in a position to identify the individual, it cannot support data subject rights for access, erasure, portability, or the restriction or objection of processing.</p>
An assessment of the necessity and proportionality of the processing operations in relation to the purposes	<p>Such an assessment will depend on the controller's needs and purposes of processing.</p> <p>With regard to the processing carried out by Microsoft, such processing is necessary and proportional for the purpose of providing the services to the data controller.</p>
An assessment of the risks to the rights and freedoms of data subjects	<p>The key risks to the rights and freedoms of data subjects from the use of Office 365 will be a function of how and in what context the data controller implements, configures, and uses it.</p> <p>Microsoft takes measures such as the anonymization or aggregation of personal data used by Microsoft to support legitimate business operations to support provision of the services, minimizing the risk of such processing to data subjects that use the service.</p> <p>However, as with any service, personal data held in the service may be at risk of unauthorized access or inadvertent disclosure. Measures Microsoft takes to address such risks are discussed in the following sections.</p>

RISK FACTORS	RELEVANT INFORMATION ABOUT OFFICE 365
<p>The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned</p>	<p>Microsoft is committed to helping protect the security of Customer's information. In compliance with the provisions of Article 32 of the GDPR, Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data and Support Data against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction.</p> <p>Further, Microsoft complies with all other GDPR obligations that apply to data processors, including but not limited to, data protection impact assessments and record keeping.</p> <p>Where Microsoft processes personal data for its legitimate business operations, it complies with GDPR obligations that apply to data controllers.</p>

## Part 3: DPIAs are hard, but this may help

If you have determined that your organization needs to draft a DPIA, the information in this section is designed to help make that process easier for you.

This section:

- provides Office 365 and product-specific information relevant service elements, and
- provides you with a blank model DPIA template that you can download, modify, and use to draft your own DPIAs.

### DPIA service elements matrix

The [DPIA Service Elements Matrix](#) is an organization of content that you might find helpful as you start the process of documenting your DPIA. It's organized by service and provides product-specific information and links to documentation that may help you draft responsive answers to the required DPIA elements more easily.

### Customizable DPIA document

We realize that drafting DPIAs can be a time-consuming effort. Although each customer's DPIA will differ based on how each organization configures and uses Office 365, the following document may save you time. You can download the [Customizable DPIA document](#) as a modifiable illustrative template to get quickly get started. It is free for you to use and adapt to your specific implementation of the service. This document should not be construed as legal advice provided by Microsoft or any of its affiliates. If you have any questions regarding the DPIA drafting process, we urge you to consult with your attorney.

## Learn more

- [Microsoft Trust Center](#)

# Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft data processor service for Windows Enterprise

12/7/2020 • 9 minutes to read • [Edit Online](#)

## NOTE

This topic is intended for participants in the data processor service for Windows Enterprise preview program and requires acceptance of specific terms of use. To learn more about the program and agree to the terms of use, see <https://aka.ms/WindowsEnterprisePublicPreview>.

Under the General Data Protection Regulation (GDPR), data controllers are required to prepare a Data Protection Impact Assessment (DPIA) for processing operations that are 'likely to result in a high risk to the rights and freedoms of natural persons'. There is nothing inherent in the data processor service for Windows Enterprise itself that would necessarily require the creation of a DPIA by a data controller using it. Rather, whether a DPIA is required will be dependent on the details and context of how the data controller deploys, configures, and uses the data processor service for Windows Enterprise.

The purpose of this document is to provide data controllers with information about the data processor service for Windows Enterprise that will help them to determine whether a DPIA is needed and, if so, what details to include.

## NOTE

Microsoft is not providing any legal advice in this document. This document is being provided for informational purposes only. Customers are encouraged to work with their privacy officers and legal counsel to determine the necessity and content of any DPIAs related to their use of the data processor service for Windows Enterprise or any other Microsoft online service.

## Part 1: Determining whether a DPIA is needed

Article 35 of the GDPR requires a data controller to create a Data Protection Impact Assessment (DPIA) '[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons'. It further sets out particular factors that would indicate such a high risk, which is discussed in the following table. To determine whether a DPIA is needed, a data controller should consider these factors, along with any other relevant factors, in light of the controller's specific implementation(s) and use(s) of the data processor service for Windows Enterprise.

### Table 1: Data processor service for Windows Enterprise DPIA risk factors

HIGH RISK FACTOR	RELEVANT INFORMATION ABOUT THE DATA PROCESSOR SERVICE FOR WINDOWS ENTERPRISE
<p>A systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.</p>	<p>The data processor service for Windows Enterprise does not provide capabilities to perform certain automated processing of data.</p> <p>However, because other services use the data processor service for Windows Enterprise as a data source, a data controller could potentially configure those services to be used for such processing. Controllers should make this determination based on their usage of services connected to the data processor service for Windows Enterprise.</p>
<p>Processing on a large scale of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offenses.</p>	<p>The data processor service for Windows Enterprise is not specifically designed to process special categories of personal data and the usage of the data processor service for Windows Enterprise does not increase the inherent risk of a controller's processing.</p> <p>However, a data controller could use services connected to the data processor service for Windows Enterprise to process the enumerated special categories of data. Services that use the data processor service for Windows Enterprise as a data source may enable the customer to track or otherwise process any type of data, including special categories of personal data. But as the data processor, Microsoft has no control over such use and has little or no insight into such use. It is incumbent upon the data controller to determine appropriate uses of the data controller's data.</p>

## Part 2: Contents of a DPIA

Article 35(7) mandates that a Data Protection Impact Assessment specifies the purposes of processing and a systematic description of the envisioned processing. A systematic description of a comprehensive DPIA might include factors such as the types of data processed, how long data is retained, where the data is located and transferred, and what third parties may have access to the data. In addition, the DPIA must include:

an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

an assessment of the risks to the rights and freedoms of natural persons; and

the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The following table contains information about the data processor service for Windows Enterprise that is relevant to each of those elements. As in Part 1, data controllers must consider the details provided in the table, along with any other relevant factors, in the context of the controller' specific implementation(s) and use(s) of the data processor service for Windows Enterprise.

**Table 2: Data processor service for Windows Enterprise DPIA elements**

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT DATA PROCESSOR SERVICE FOR WINDOWS ENTERPRISE
-------------------	--

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT DATA PROCESSOR SERVICE FOR WINDOWS ENTERPRISE
Purpose(s) of processing	<p>The purpose(s) of processing diagnostic data using the data processor service for Windows Enterprise is determined by the controller that implements, configures, and uses it.</p> <p>As specified by the <a href="#">Online Services Terms (OST)</a>, Microsoft, as a data processor, processes Customer Data only to provide the requested services to our customer, the data controller. Microsoft will not use Customer Data or information derived from it for any advertising or similar commercial purposes.</p>
Categories of personal data processed	<p><b>Customer Data</b> - All data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, a customer through use of the enterprise service. Customer Data includes identifiable information of end users (for example, user names and contact information in Azure Active Directory or device information through Windows Diagnostic Data).</p> <p><b>System-Generated Data</b> - Data generated by Microsoft that helps Microsoft provide enterprise services to users. System-generated data contain primarily pseudonymized data, such as unique identifiers generated by the system, that cannot on their own identify an individual person but are used to deliver the enterprise services to users. System-generated data may also contain identifiable information about end users, such as a user name.</p> <p><b>Support Data</b> - Data provided to Microsoft by or on behalf of Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain technical support for Online Services.</p> <p>For more information regarding data processed by the data processor service for Windows Enterprise, see the <a href="#">Online Services Terms</a>, as well as <a href="#">Microsoft Trust Center</a>.</p>
Data retention	<p>Microsoft will retain and process Customer Data for the duration of the Customer's right to use the Online Service and until all Customer Data is retrieved by Customer or deleted in accordance with the terms of the OST. At all times during the term of Customer's subscription, the Customer will have the ability to export Customer Data stored in the data processor service for Windows Enterprise. The customer can delete personal data pursuant to a Data Subject Request using the capabilities described in the <a href="#">data processor service for Windows Enterprise Data Subject Request GDPR Documentation</a>.</p>
Location and transfers of personal data	<p>Data processor service for Windows Enterprise customers' data resides in Microsoft data centers in the United States.</p>

ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT DATA PROCESSOR SERVICE FOR WINDOWS ENTERPRISE
Data sharing with third parties	<p>Microsoft shares data with third parties acting as our subprocessors (that is, subcontractors which process personal data) to support functions such as customer and technical support, service maintenance, and other operations. Any subcontractors to which Microsoft transfers Customer Data or Support Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the <a href="#">Online Services Terms</a>. All third-party subcontractors with which Customer Data or Support Data is shared are included in the <a href="#">Lists of subcontractors</a> (see 'We limit access by subprocessors').</p> <p>Information regarding Microsoft's response to law enforcement and third-party requests for Customer Data and Support Data is located in the Online Services Terms. Unless Microsoft is legally prohibited from doing so, Microsoft will attempt to redirect the law enforcement agency or third party directly to the Customer.</p>
Data subject rights	<p>When operating as a processor, Microsoft makes available to the customer (the controller) the personal data of its data subjects and the ability to fulfill data subject requests when they exercise their rights under the GDPR. Microsoft does so in a manner consistent with the functionality of the product and its role as a data processor. If Microsoft receives a request from the customer's data subjects to exercise one or more of its rights under the GDPR, the request will be redirected to the data controller.</p> <p>The <a href="#">data processor service for Windows Enterprise Data Subject Request GDPR Documentation</a> provides a description of how to support data subject rights using the capabilities in the data processor service for Windows Enterprise.</p>
An assessment of the necessity and proportionality of the processing operations in relation to the purposes	<p>Such an assessment will depend on the data controller's needs and purposes of processing.</p> <p>With regard to the processing carried out by Microsoft, such processing is necessary and proportional for the purpose of providing the services to the data controller. Microsoft makes this commitment in the OST.</p>
An assessment of the risks to the rights and freedoms of data subjects	<p>The key risks to the rights and freedoms of data subjects from the use of the data processor service for Windows Enterprise will be a function of how and in what context the controller implements, configures, and uses the data processor service for Windows Enterprise.</p> <p>However, as with any service, personal data held in the service may be at risk of unauthorized access or inadvertent disclosure. Measures Microsoft takes to address such risks are discussed in the OST, as further detailed later in this table.</p>



ELEMENT OF A DPIA	RELEVANT INFORMATION ABOUT DATA PROCESSOR SERVICE FOR WINDOWS ENTERPRISE
<p>The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned</p>	<p>Microsoft is committed to helping protect the security of Customer Data. The security measures Microsoft takes are described in detail in the OST.</p> <p>Microsoft takes reasonable and appropriate technical and organizational measures to safeguard the personal data that it processes. These measures include, but are not limited to, internal privacy policies and practices, contractual commitments, and international and regional standard certifications. More information is available at <a href="#">Trust Center's Privacy Standards page</a>.</p> <p>Microsoft provides significant, transparent customer facing security and privacy materials to help explain Microsoft's use and processing of personal data. Customers are encouraged to contact Microsoft with questions.</p> <p>Further, Microsoft complies with all other GDPR obligations that apply to data processors, including but not limited to, data protection impact assessments and record keeping.</p>

# GDPR for Office on-premises Servers

11/30/2020 • 2 minutes to read • [Edit Online](#)

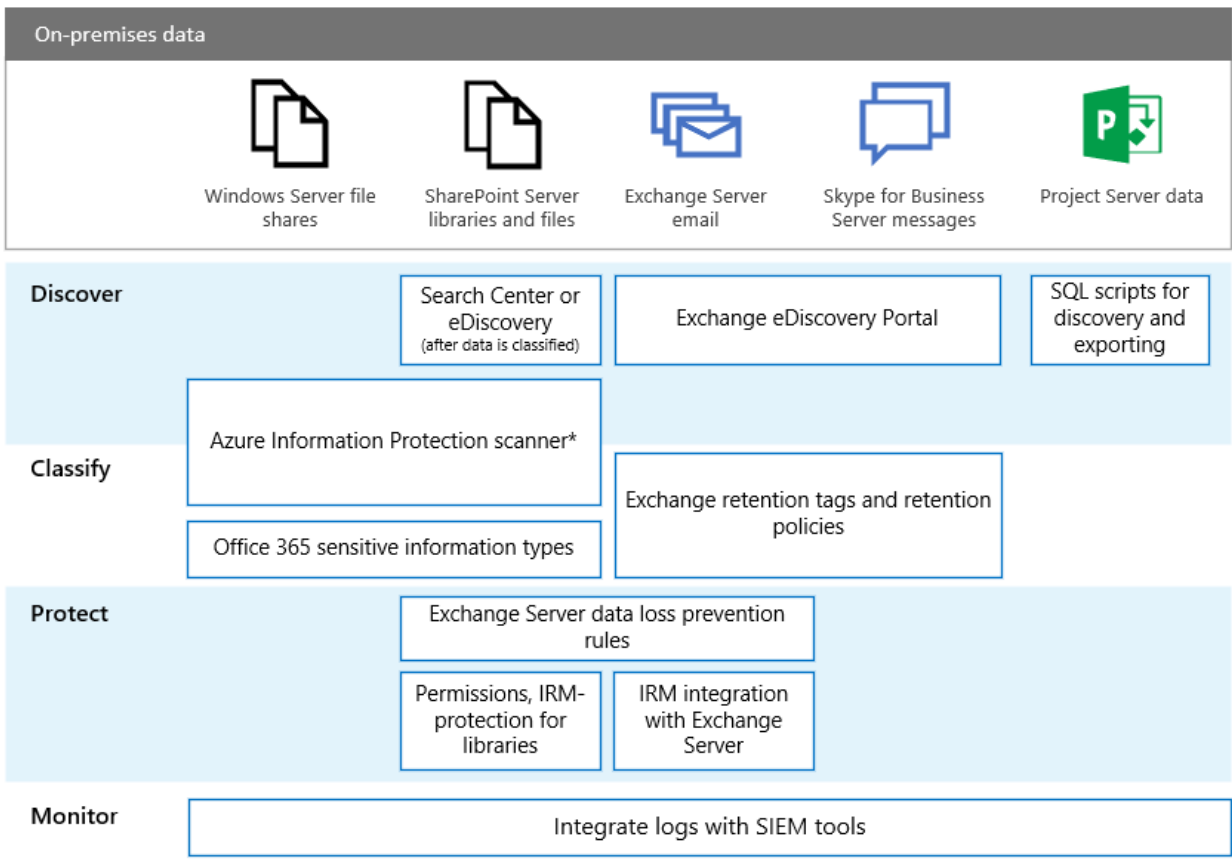
The General Data Protection Regulation (GDPR) introduces requirements for organizations to protect personal data and respond appropriately to data subject requests. This series of articles provides recommended approaches for on-premises workloads:

- [SharePoint Server](#)
- [Exchange Server](#)
- [Skype for Business Server](#)
- [Project Server](#)
- [Office Web Apps Server and Office Online Server](#)
- [On-premises file shares](#)

For more information about the GDPR and how Microsoft can help you, see the [Microsoft Trust Center](#).

Before doing any work with on-premises data, consult with your legal and compliance teams to seek guidance and to learn about existing classification schemas and approaches to working with personal data. Microsoft provides recommendations for developing and extending classifications schemas in the Microsoft GDPR Data Discovery Toolkit at <https://aka.ms/gdprpartners>. This toolkit also describes approaches for moving on-premises data to the cloud where you can use more sophisticated data governance capabilities, if this is desired. The articles in this section provide recommendations for data that is intended to remain on premises.

The following illustration lists recommended capabilities to use across each of these workloads to discover, classify, protect, and monitor personal data. See the articles in this section for more information.



\* Note that protection encrypts the file. Consequently, SharePoint Server can't find the sensitive information types in protected files.

## Illustration description

For accessibility, the following table provides the same examples in the illustration.

ACTION	WINDOWS SERVER FILE SHARES	SHAREPOINT SERVER	EXCHANGE SERVER	SKYPE FOR BUSINESS	PROJECT SERVER
Discover	Azure Information Protection scanner*	Search Center or eDiscovery (after data is classified)  Azure Information Protection scanner*	Exchange eDiscovery Portal	Exchange eDiscovery portal	SQL scripts for discovery and exporting
Classify	Azure Information Protection scanner*  Office 365 sensitive information types	Azure Information Protection scanner*  Office 365 sensitive information types	Exchange retention tags and retention policies	Exchange retention tags and retention policies	

ACTION	WINDOWS SERVER FILE SHARES	SHAREPOINT SERVER	EXCHANGE SERVER	SKYPE FOR BUSINESS	PROJECT SERVER
Protect		Exchange Server data loss prevention rules  Permissions, IRM-protection for libraries	Exchange Server data loss prevention rules  IRM integration with Exchange Server		
Monitor	Integrate logs with SIEM tools	Integrate logs with SIEM tools	Integrate logs with SIEM tools	Integrate logs with SIEM tools	Integrate logs with SIEM tools

\* Note that protection encrypts the file. Consequently, SharePoint Server can't find the sensitive information types in protected files.

# GDPR for SharePoint Server

2/5/2021 • 9 minutes to read • [Edit Online](#)

Applies to:

- SharePoint Server 2013
- SharePoint Server 2016
- SharePoint Server 2019

As part of safeguarding personal information, we recommend the following:

- Classify your data, using Azure Information Protection.
- Run SharePoint Server in a least-privileged configuration. See [Plan for least-privileged administration in SharePoint Server](#) and [Security for SharePoint Server](#) for more information.
- [Enable BitLocker encryption on your servers.](#)

## User Generated content

The basic recommended approach for user generated content contained in SharePoint Server sites and libraries is:

- Use Azure Information Protection to label sensitive data.
- Use [SharePoint Server search](#) and [eDiscovery](#) to retrieve sensitive data.

The recommended approach for files shares and SharePoint sites and libraries includes these steps:

1. **Install and configure Azure Information Protection scanner.**
  - Decide which sensitive data types to use.
  - Specify which SharePoint sites to use.
2. **Complete a discovery cycle.**
  - Run the scanner in discovery mode and validate the findings.
  - If needed, optimize the conditions and sensitive information types.
  - Assess the expected impact of automatically applying labels.
3. **Run the Azure Information Protection scanner to apply labels to qualifying documents.**
4. **For protection:**
  - a. Configure Exchange data loss prevention rules to protect documents with the desired label.
  - b. Be sure permissions to limit who can access files.
  - c. For SharePoint, use IRM-protection for libraries.
5. **For monitoring, integrate Windows Server logs with a SIEM tool.**
  - a. To find personal data for data subject requests, use Search Center or eDiscovery.

When applying labels to sensitive data, be sure to use a label that is not configured with protection. Protection

includes encryption which prevents services from detecting sensitive data in the files.

For more information on using Azure Information Protection scanner to find and label personal data, see the [Microsoft GDPR Data Discovery Toolkit \(https://aka.ms/gdprpartners\)](https://aka.ms/gdprpartners).

For information on configuring the scanner for conditions and using the Office 365 data loss prevention (DLP) sensitive information types, see [How to configure conditions for automatic and recommended classification for Azure Information Protection](#). Note that new Office 365 sensitive information types will not be immediately available to use with the scanner and custom sensitive information types cannot be used with the scanner.

## Removing personal information from Office files

Removing personal information (such as metadata or comments in a Word document) from Office files that are stored in a SharePoint document library must be done manually. Follow these steps:

1. Download a copy of the document from SharePoint Server to your local disk.
2. Delete the document from the SharePoint document library.
3. Follow the steps in [Remove hidden data and personal information by inspecting documents](#).
4. Upload the document back to the SharePoint document library.

## Telemetry and log files

### ULS Logs

Unified Logging Service (ULS) and Usage logging in SharePoint Server track a variety of system functions and can contain user information. ULS logs and usage logs are text files and can be searched using a variety of searching tools. The [Merge-SPLLogFile PowerShell cmdlet](#) provides a way to return records from the ULS logs on multiple servers in a farm.

Consider setting log retention policies to the minimum value needed for your business purposes. For information about configuring logging in SharePoint Server, see [Configure diagnostic logging in SharePoint Server](#).

Note that some system events are also logged to the Windows Event Log.

### Usage Database

The SharePoint Server Usage database (default name WSS\_Logging) contains a subset of the information found in the ULS logs. The maximum retention of data in this database is 30 days. We recommend that you configure it for the shortest duration allowable by your business needs. For more information, see [Configure diagnostic logging in SharePoint Server](#).

## Personal information and search

The search query history and usage records contain references to user names.

### Query history and favorite queries

In SharePoint Server, query histories and 'favorite' queries automatically expire after 365 days. If a user leaves your organization, it is possible to remove references to a user's name from the query history using the steps below.

The following SQL queries apply to SharePoint Server and make it possible to:

- Export a user's query history or favorite queries
- Remove references to user names in the query history

### Export a user's queries since a specific date

Use the following procedure to export queries from the Link Store query log tables, performed by @UserName since @StartTime.

```
[In dbo].[LinkStore_<ID>]:
CREATE PROCEDURE proc_MSS_GetQueryTermsForUser
(
@UserName nvarchar(256),
@StartTime datetime
)
AS
BEGIN
SET NOCOUNT ON;
SELECT searchTime, queryString
FROM
dbo.MSSQLogPageImpressionQuery
WITH
(NOLOCK)
WHERE
userName = @UserName AND
searchTime > @StartTime
END
GO
```

### Export a user's queries from the past 100 days

```
DECLARE @FROMDATE datetime
SET @FROMDATE = DATEADD(day, -100, GETUTCDATE())
EXECUTE proc_MSS_GetQueryTermsForUser '0#.w|domain\username', @FROMDATE
```

### Export a user's favorite queries

Use the following procedure to export a user's favorite queries from the Search Admin DB personal result tables, performed by @UserName, since .

```
In [dbo].[Search_<ID>]:
CREATE PROCEDURE proc_MSS_GetPersonalFavoriteQueries
(
@UserName nvarchar(256),
@SearchTime datetime
)
AS
BEGIN
SET NOCOUNT ON;
SELECT max(queries.SearchTime) as SearchTime,
max(queries.querystring) as queryString,
max(url.url) as URL
FROM MSSQLogOwner owners WITH(NOLOCK)
JOIN MSSQLogPersonalResults results WITH(NOLOCK) on owners.OwnerId = results.OwnerId
JOIN MSSQLogUrl url WITH(NOLOCK) on results.ClickedUrlId = url.urlId
JOIN MSSQLogPersonalQueries queries WITH(NOLOCK) on results.OwnerId = queries.OwnerId
WHERE queries.SearchTime > @SearchTime
AND queries.UserName = @UserName
GROUP BY queries.QueryString,url.url
END
GO
```

### Export a user's favorite queries from the past 100 days

```
DECLARE @FROMDATE datetime
SET @FROMDATE = DATEADD(day, -100, GETUTCDATE())
EXECUTE proc_MSS_GetPersonalFavoriteQueries '0#.w|domain\username', @FROMDATE
```

### Remove references to user names that are more than X days old

Use the following procedure to remove references to *all* user names that are more than @Days old, from the Links Store query log tables. The procedure only removes references backwards in time until it reaches the @LastCleanupTime.

```
In [dbo].[LinksStore_<ID>]:
CREATE PROCEDURE proc_MSS_QLog_Cleanup_Users
(
    @LastCleanupTime datetime,
    @Days int
)
AS
BEGIN
    DECLARE @TooOld datetime
    SET @TooOld = DATEADD(day, -@Days, GETUTCDATE())
    DECLARE @FromLast datetime
    SET @FromLast = DATEADD(day, -@Days, @LastCleanupTime)
    BEGIN TRANSACTION
        UPDATE MSSQLLogPageImpressionQuery
    SET userName = 'NA'
    WHERE @FromLast <= searchTime AND searchTime < @TooOld
    UPDATE MSSQLLogO14PageClick
    SET userName = 'NA'
    WHERE @FromLast <= searchTime AND searchTime < @TooOld
    COMMIT TRANSACTION
END
GO
```

### Remove references to a specific user name that's more than X days old

Use the following procedure to remove references to a *specific* user name from the Links Store query log tables, where the references are more than @Days old. The procedure only removes references backwards in time until it reaches the @LastCleanupTime.

```
In [dbo].[LinksStore_<ID>]:
CREATE PROCEDURE proc_MSS_QLog_Cleanup_Users
(
    @UserName nvarchar(256),
    @LastCleanupTime datetime,
    @Days int
)
AS
BEGIN
    DECLARE @TooOld datetime
    SET @TooOld = DATEADD(day, -@Days, GETUTCDATE())
    DECLARE @FromLast datetime
    SET @FromLast = DATEADD(day, -@Days, @LastCleanupTime)
    BEGIN TRANSACTION
        UPDATE MSSQLLogPageImpressionQuery
    SET userName = 'NA'
        WHERE @FromLast <= searchTime AND searchTime < @TooOld AND userName = @UserName
    UPDATE MSSQLLogO14PageClick
    SET userName = 'NA'
        WHERE @FromLast <= searchTime AND searchTime < @TooOld AND userName = @UserName
    COMMIT TRANSACTION
END
GO
```

### Remove references to all user names in the query history from a date and up to the past 30 days

```
EXECUTE proc_MSS_QLog_Cleanup_Users '1-1-2017', 30
```

### Delete usage records



SharePoint Server automatically deletes usage records after 3 years. You can manually delete such records using the procedure below:

To delete all usage records associated with deleted documents:

1. Ensure that you have the latest SharePoint update installed.
2. Start a SharePoint Management shell.
3. Stop and Clear the Usage Analytics analysis:

```
$tj = Get-SPTimerJob -Type Microsoft.Office.Server.Search.Analytics.UsageAnalyticsJobDefinition
$tj.DisableTimerjobSchedule()
$tj.StopAnalysis()
$tj.ClearAnalysis()
$tj.EnableTimerjobSchedule()
```

4. Wait for the analysis to start again (might take up to 24 hours).
5. On the next run of the analysis, it will dump all records from the Analytics Reporting database. This full dump may take a while for a large database with many entries.
6. Wait for 10 days. The analysis runs daily, and records associated with deleted documents will be removed after the 10<sup>th</sup> run. This run may take longer than normal if many records need to be deleted.

## Personal information and search in SharePoint Server 2010

### FAST Search Server 2010 for SharePoint

In addition to storing files in the index, the FAST Search Server 2010 Add-On also stores files in an intermediate format called FiXML. FiXML files are compacted regularly, by default between 3 am and 5 am every night. Compaction removes deleted files from the FiXML files automatically. To ensure timely removal of information belonging to deleted users or documents, ensure that compaction is always enabled.

### Hybrid Search

The recommended actions for hybrid search solutions are the same as for search in SharePoint Server or SharePoint Online. There are two hybrid search solutions:

**The cloud hybrid search solution** - With the cloud hybrid search solution for SharePoint, you index all your crawled content, including on-premises content, in your search index in Office 365. When users query your search index in Office 365, they get search results from both on-premises and Office 365 content. When documents are deleted from the SharePoint Server environment, they are also deleted from the search index in Office 365. [Read more about the cloud hybrid search solution](#) and [how search components and databases interact in cloud hybrid search](#) to understand better how GDPR affects the hybrid environment.

**The hybrid federated search solution** - With the hybrid federated search solution, you use both your index in SharePoint Server and your index in Office 365. Both SharePoint Server and SharePoint Online Search services can query the search index in the other environment and return federated results. When users search from a Search Center, the search results come from both your search index in SharePoint Server and your search index in Office 365. [Read more about the hybrid federated search solution](#) to understand better how GDPR affects the hybrid environment.

## On Prem to Cloud Migrations

While migrating data from SharePoint Server to SharePoint Online, duplicate data may exist in both locations for a time. If you have data that you need to delete that is in mid-migration, we recommend that you complete the migration first, and then delete the data from both locations. You can query data for export from either location.

## User Profile data

The User Profile Service allows for import of profile data from a variety of external sources. Queries for and update of such user profile data should be handled in the systems in which the data is mastered. If you make updates to the external system, be sure to synchronize the user profiles in SharePoint Server again.

Follow these basic steps to remove a user's personal information from their SharePoint Server user profile:

1. Remove the user information from any external systems that feed into the SharePoint Server user profile. If you are using directory synchronization, the user must be removed from the on-premises Active Directory environment.
2. Run a [profile synchronization](#) on SharePoint Server.
3. Delete the profile from SharePoint Server. Once this is done, SharePoint Server will fully remove the profile from the User Profile Database in 30 days. The user's profile page and personal site will be deleted.

After deleting a user's profile, some limited information (such as user ID) may still be recorded in site collections that the user has visited. If you choose to delete this data from a given site collection, this can be done using CSOM. A sample script is provided below:

```
$username = "<admin@company.sharepoint.com>"
$password = "password"
$url = "<https://site.sharepoint.com>"
$securePassword = ConvertTo-SecureString $Password -AsPlainText -Force

# the path here may need to change if you used e.g. C:Lib.
Add-Type -Path "c:\Program Files\Common Files\microsoft shared\Web Server
Extensions\16ISAPIMicrosoft.SharePoint.Client.dll"
Add-Type -Path "c:\Program Files\Common Files\microsoft shared\Web Server
Extensions\16ISAPIMicrosoft.SharePoint.Client.Runtime.dll"

# connect/authenticate to SharePoint Online and get ClientContext object.
$clientContext = New-Object Microsoft.SharePoint.Client.ClientContext($url)
$credentials = New-Object Microsoft.SharePoint.Client.SharePointOnlineCredentials($username,
$securePassword)
$clientContext.Credentials = $credentials
if (!$clientContext.ServerObjectIsNull.Value)
{
    Write-Host "Connected to SharePoint Online site: '$url'" -ForegroundColor Green
}

# Get user
$user = $clientContext.Web.SiteUsers.GetByLoginName("i:0#.f|membership|user@company.sharepoint.com")

# Redact user
$user.Email = "Redacted"
$user.Title = "Redacted"
$user.Update()
$clientContext.Load($user)
$clientContext.ExecuteQuery()

# Get users
$users = $clientContext.Web.SiteUsers

# Remove user from site
$users.RemoveById($user.Id)
$clientContext.Load($users)
$clientContext.ExecuteQuery()
```

# GDPR for Exchange Server

2/5/2021 • 4 minutes to read • [Edit Online](#)

As part of safeguarding personal information, we recommend the following:

- Use [Retention Tags and Policies](#) in Exchange Server to implement an email life cycle policy.
- Deploy [Information Rights Management](#) to limit who has access to information stored in Exchange Server.
- Enable [BitLocker encryption](#) on your servers.

## Identifying In-scope Content

Exchange uses two primary storage repositories for end user generated content: mailboxes and public folders. Content stored in an individual user's mailbox is uniquely associated to that user and represents their default repository within Exchange. The data stored in a user mailbox includes content created using Outlook, Outlook on the web (formerly known as Outlook Web App), Exchange ActiveSync, Skype for Business clients and other third-party tools that connect to Exchange servers using POP, IMAP or Exchange Web Services (EWS). Examples of these items include: messages, calendar items (meetings and appointments), contacts, notes and tasks. Deleting an individual user's mailbox removes content generated by or sent directly to the user in the context of their mailbox. You can delete user mailboxes by using the Exchange admin center (EAC) or the [Remove-Mailbox](#) cmdlet in the Exchange Management Shell.

Note: The Permanent parameter on the Remove-Mailbox cmdlet should be used with caution as the data will not be recoverable if this option is used.

Exchange also provides shared mailboxes that allow one or more users access to send and receive content that's stored in a common mailbox. The shared mailbox is a unique entity that's not associated with a single account. Instead, multiple users are granted access to send, receive and review email content in the shared mailbox. Shared mailboxes are administered using the Exchange admin center and the same cmdlets used to manage regular user mailboxes. If you need to remove individual messages from a mailbox, there are different options available depending upon the version of Exchange. In Exchange Server 2010 and 2013, you can use the [Search-Mailbox](#) cmdlet with the DeleteContent parameter to identify and remove messages from a mailbox. In Exchange Server 2016 and later, you need to use the [New-ComplianceSearch](#) functionality.

Public folders are a shared storage implementation that's not associated with a specific user. Instead, users are granted access to public folders to generate content. The actual implementation of public folders varies depending upon the version of Exchange (Exchange Server 2010 uses a different implementation than Exchange Server 2013 and later). Limited tools exist to manage the content in public folders. Client tools (for example, Outlook) are the primary mechanism for managing content in public folders. There are cmdlets for managing public folder objects, but not for managing individual content items within the public folder. A custom script that leverages Exchange Web Services (EWS) or other third-party tools will likely be needed to manage individual public folder items.

The primary requirement will likely be managing individual user mailbox content. This requirement will be easily addressed through the graphical or cmdlet-based tools that you regularly use to manage mailboxes. If you need to process content across multiple mailboxes or types of resources, [eDiscovery](#) is the preferred mechanism within Exchange to identify in-scope content.

## Deleted Item Retention

When you delete individual messages or items from a mailbox (not the entire mailbox or public folder resource itself) the content is retained in a recoverable form based on the value of the DeletedItemRetention parameter

for the mailbox database or public folder database. The default value is 14 days, but this value is configurable by an Exchange administrator.

## Removing Soft-Deleted and Disconnected Mailboxes

When an Exchange mailbox is disabled, deleted or moved between databases (for example, as a part of load balancing), the mailbox is placed into a disabled, soft-deleted or disconnected state depending on the operation. While the mailbox is in any of these states, Exchange maintains the mailbox (which includes its contents) based on the current value of the MailboxRetention parameter that's specified on the mailbox database. The default value is 30 days, but this value is configurable by an Exchange administrator. You can use the [Remove-StoreMailbox](#) cmdlet to force Exchange to permanently remove (purge) all data associated with a mailbox prior to the retention period expiring naturally.

### **IMPORTANT**

Use the `Remove-StoreMailbox` cmdlet with caution as it results in an unrecoverable loss of data for the target mailbox.

## On-Prem to Cloud Migrations

While migrating data from Exchange Server to Exchange Online, migrated data may continue to reside on the source on-premises Exchange Server in a form that's recoverable by an Exchange administrator. By default, this data will be automatically removed from the database within 30 days (see the Removing Soft-Deleted and Disconnected Mailboxes section above).

## Automatic Data Collection Reported to Microsoft by Exchange Server

Exchange Servers deployed in on-premises environments do not provide any type of automated reporting or end user data capture to Microsoft. Exchange Servers that have Watson crash dump reporting enabled in the Windows Operating System may receive limited contents of memory at the time the crash report is produced.

# GDPR for Skype for Business Server and Lync Server

2/5/2021 • 2 minutes to read • [Edit Online](#)

Most Skype for Business Server and Lync Server data is stored in Exchange Server. This includes:

- Conversation history
- Voicemail notifications and transcriptions
- Meeting invites

Use the procedures outlined for [GDPR for Exchange Server](#) to find, export, or delete these types of data for GDPR requests.

Contact lists are stored in the SQL Server database. They can be exported in the following ways:

- End users themselves can export the contacts by right clicking the group header and selecting Copy. This will copy all the contacts in that group into the clipboard, which can then be pasted into any app.
- You can use the [Export-CsUserData](#) cmdlet to export this data.

Content uploaded into meetings (such as PowerPoint files or handouts) or content generated in a meeting (such as whiteboard, polls, or Q/A) is stored in the filer. This can also be exported if end users log back into any meeting that has not expired and download any uploaded content or take screenshots in the case of generated content.

MeetNow meetings that are not in the Exchange Calendar and Contact List and contact rights (family, co-worker, etc.) are in the User Database. In Lync Server 2013 and later, you can use the [Export-CsUserData](#) cmdlet to export this data.

# GDPR for Project Server

11/30/2020 • 2 minutes to read • [Edit Online](#)

Project Server uses custom scripts to export and redact user data in Project Web App. The basic process is:

1. Find the Project Web App sites in your farm.
2. Find the projects in each site that contain the user.
3. Export and review the types of data that you want to review.
4. Redact data as needed.

These steps are covered in detail in the following articles:

- [Export user data from Project Server](#)
- [Delete user data from Project Server](#)

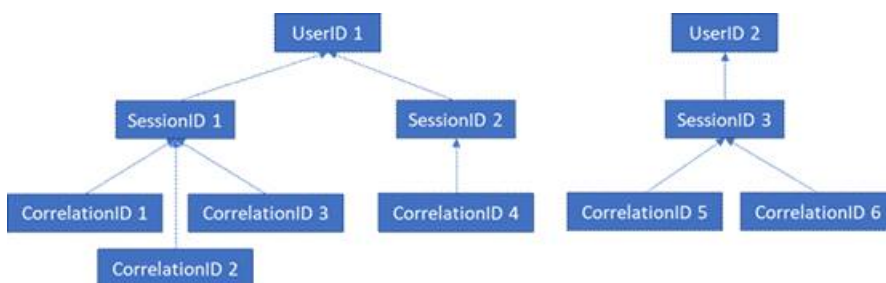
Note that Project Server is built on top of SharePoint Server and logs events to the SharePoint ULS logs and Usage database. See [GDPR for SharePoint Server](#) for more information.

# GDPR for Office Web Apps Server and Office Online Server

11/30/2020 • 2 minutes to read • [Edit Online](#)

Office Online Server and Office Web Apps Server telemetry data is stored in the form of ULS logs. You can use [ULS Viewer](#) to view ULS logs from your on-premises tenant.

Every log line contains a CorrelationID. Related log lines share the same CorrelationID. Each CorrelationID is tied to a single SessionID, and one SessionID may be related to many CorrelationIDs. Each SessionID may be related to a single UserID, although some sessions can be anonymous and therefore not have an associated UserID. In order to determine what data is associated with a particular user, it is therefore possible to map from a single UserID to the SessionIDs associated with that user, from those SessionIDs to the associated CorrelationIDs, and from those CorrelationIDs to all the logs in those correlations. See the below diagram for the relationship between the different IDs.



## Gathering Logs

In order to gather all logs associated with UserID 1, for example, the first step would be to gather all sessions associated with UserID 1 (i.e. SessionID 1 and SessionID2). The next step would be to gather all correlations associated with SessionID 1 (i.e. CorrelationIDs 1, 2, and 3) and with SessionID 2 (i.e. CorrelationID 4). Finally, gather all logs associated with each of the correlations in the list.

1. Launch UlsViewer
2. Open up the uls log corresponding to the intended timeframe; ULS logs are stored in  
`%PROGRAMDATA%\Microsoft\OfficeWebApps\Data\Logs\ULS`
3. Edit | Modify Filter
4. Apply a filter that is:
  - EventID equals apr3y
  - Or
  - EventID equals bp2d6
5. Hashed UserIds will be in the Message of either one of these two events
6. For apr3y, the Message will contain a UserID value and a PUID value
7. For bp2d6, the Message will contain quite a bit of information. The LoggableUserId Value field is the hashed UserID.
8. Once the hashed UserId is obtained from either of these two tags, the WacSessionId value of that row in

ULSViewer will contain the WacSessionId associated with that user

9. Collect all of the WacSessionId values associated with the user in question
10. Filter for all EventId equals "xmnv", Message equals "UserSessionId= <WacSessionId>" for the first WacSessionId in the list (replacing the <WacSessionId> part of the filter with your WacSessionId)
11. Collect all values of Correlation that match that WacSessionId
12. Repeat steps 10-11 for all values of WacSessionId in your list for the user in question
13. Filter for all Correlation equals the first Correlation in your list
14. Collect all logs matching that Correlation
15. Repeat steps 13-14 for all values of Correlation in your list for the user in question

## Types of Data

Office logs contain a variety of different types of data. The following are examples of the data that ULS logs may contain:

- Error codes for issues encountered during use of the product
- Button clicks and other pieces of data about app usage
- Performance data about the app and/or particular features within the app
- General location information about where the user's computer is (e.g. country / region, state, and city, derived from the IP address), but not precise geo location.
- Basic metadata about the browser, e.g. browser name and version, and the computer, e.g. OS type and version
- Error messages from the document host (e.g. OneDrive, SharePoint, Exchange)
- Information about processes internal to the app, unrelated to any action the user has taken



# GDPR for on-premises Windows Server file shares

2/5/2021 • 2 minutes to read • [Edit Online](#)

The basic recommended approach for file shares is:

- Use Azure Information Protection to label sensitive data.
- Use Azure Information Protection scanner to find data.

The recommended approach for files shares includes these steps:

## 1. Install and configure Azure Information Protection scanner.

- Decide which sensitive data types to use.
- Specify local folders and network shares to use.

## 2. Complete a discovery cycle.

- Run the scanner in discovery mode and validate the findings.
- If needed, optimize the conditions and sensitive information types.
- Assess the expected impact of automatically applying labels.

## 3. Run the Azure Information Protection scanner to apply labels to qualifying documents.

## 4. For protection:

- Configure Exchange data loss prevention rules to protect documents with the desired label.
- Be sure to use permissions to limit who can access files.

## 5. For monitoring, integrate Windows Server logs with a SIEM tool.

- To find personal data for data subject requests, use Azure Information Protection scanner. You can also configure SharePoint Server search to crawl file shares.

For more information on using Azure Information Protection scanner to find and label personal data, see [Deploy AIP Scanner](#).

For information on configuring the scanner for conditions and using the Office 365 data loss prevention (DLP) sensitive information types, see [How to configure conditions for automatic and recommended classification for Azure Information Protection](#). Note that new Office 365 sensitive information types will not be immediately available to use with the scanner and custom sensitive information types cannot be used with the scanner.

# Additional steps to export system-generated log data

2/5/2021 • 2 minutes to read • [Edit Online](#)

**Kaizala:** The Kaizala management portal lets you export an organization's product and service usage data and then use Excel functionality to filter that data for a specific user. For detailed instructions, see [Export or delete a user's organizational data in Kaizala](#).

**Office Roaming Service:** Office Roaming is a service that stores Office-related settings, such as Office theme, custom dictionary, language settings, developer mode, and auto correct. For instructions on how to export this data, see [Manage GDPR data subject requests with the DSR case tool in the Security & Compliance Center](#).

**Workplace Analytics:** The data log export tool provides usage data for those users in your organization who have permission to run Workplace Analytics reports. Workplace Analytics also computes and stores pseudonymized data derived from Office 365 data to improve performance. If you would like to make this pseudonymized data available to a user and need assistance, contact [Microsoft Support](#).

**Yammer:** The Yammer admin center lets you export a user's account activity data. When you export the user's data, you receive an email message containing the user's account activity data. You can provide this information to the user if you choose. For detailed instructions, see [Manage GDPR data subject requests in Yammer Enterprise](#).

## Learn more

[Office 365 Data Subject Requests for the GDPR and CCPA](#)

# GDPR discovery, protection, and reporting in the dev/test environment

2/5/2021 • 8 minutes to read • [Edit Online](#)

**Summary:** Demonstrate GDPR capabilities in Microsoft 365.

This article describes how you configure and demonstrate personally identifiable information (PII) discovery, protection, and reporting for the General Data Protection Regulation (GDPR) in a Microsoft 365 dev/test environment.

## Phase 1: Create and configure your trial Microsoft 365 subscription

First, follow the steps in [Phase 2 of the Microsoft 365 dev/test environment](#) article.

Next, use these steps to configure the eDiscovery manager:

1. Sign in to your Microsoft 365 trial tenant with your global administrator account.
2. From the Microsoft 365 home page, click **Security & Compliance**.
3. From the new Security & Compliance tab, click **Permissions > eDiscovery Manager**.
4. Click **Edit** for eDiscovery Manager, and then click **Choose eDiscovery Manager**.
5. Click + **Add**, search for your global administrator account name and add your global administrator account as an eDiscovery Manager.
6. Click **Done > Save > Close**.

## Phase 2: Add personally identifiable information to your tenant

In this phase, you create a document with PII for a set of example International Banking Account Numbers (IBANs) and store it on a SharePoint Online site in your Microsoft 365 dev/test environment.

1. On your local computer, open Microsoft Word.
2. Paste the following table in the Word file and save it as 'IBANs.docx' on your local computer.

NUMBER	COUNTRY	CODE	IBAN
1	Austria SEPA	AT	AT611904300234573201
2	Bulgaria SEPA	BG	BG80BNBG96611020345678
3	Denmark SEPA	DK	DK5000400440116243
4	Finland SEPA	FI	FI2112345600000785
5	France SEPA	FR	FR1420041010050500013M02606
6	Germany SEPA	DE	DE89370400440532013000

NUMBER	COUNTRY	CODE	IBAN
7	Greece SEPA	GR	GR1601101250000000 12300695
8	Italy SEPA	IT	GR1601101250000000 12300695
9	Netherlands SEPA	NL	NL91ABNA0417164300
10	Poland SEPA	PL	PL271140200400003002 01355387

Note:- This sample data set is derived from publicly available information and is intended to be used for test purposes only.

3. In a new tab of your browser, type: **https://<YourTenantName>.sharepoint.com**
4. Click **Documents** to open the document library for this site. If you're prompted for a new list experience tour, click **Next** until it's finished.
5. Click **Upload > Files** and select the IBANs.docx you created in step 2.

## Phase 3: Demonstrate data discovery

In this phase, you demonstrate search to find the document created and stored in Phase 2, based on its content containing IBANs.

1. From the Security & Compliance tab, click **Home**, and then click **Search & investigation > Content search**.
2. Create a new search item by clicking on **+**.
3. In a new window, provide the following information: a. Name: IBAN Search b. Where do you want us to look?: **Choose specific sites to search** (click **+**), and then enter the site's URL: **https://<YourTenantName>.sharepoint.com/** c. Click **Add**, and then click **OK**. If you see a Warning, click **OK**. d. Click **Next** on a **New search** window. e. For **What do you want us to look for?**: **SensitiveType:"International Banking Account Number (IBAN)"**, and then click **Search**.
4. Make sure you see at least one item listed in the **IBAN Search** results.

## Phase 4: Create a custom sensitive information type via PowerShell

In this phase, you create a custom sensitive information type for the fictional Contoso Corporation using Microsoft PowerShell. Contoso uses a Contoso Customer Number (CCN) to identify each customer in their customer database. A CCN consists of the following structure:

- Two digits to represent the year that the record was created.
  - Contoso was founded in 2002; therefore, the earliest possible value would be 02.
- Three digits to represent the partner agency that created the record.
  - Possible agency values range from 000 to 999.
- An alphabetic character to represent the line of business.
  - Possible values are a-z and should be case insensitive.
- A four-digit serial number.
  - Possible serial number values range from 0000 to 9999.

Contoso always refers to customers by using a CCN in internal correspondence, external correspondence, documents, and other forms. Contoso needs a custom sensitive item type to detect the use of CCNs in Microsoft 365 content so that they may apply protection to the use of this form of personal identifiable information.

1. Use the multi-factor authentication (MFA) connection instructions in [Connect to Security & Compliance Center PowerShell](#) and connect to the Security & Compliance Center with UPN of your global administrator account.
2. Run the following PowerShell commands.

```
#Create & start search for sample data
$searchName = "Sample Customer Information Search"
$searchQuery = "15080P9562 OR 1404001119 OR 15020J8317 OR 14050E2330 OR 16050E2166 OR 1704001118"
New-ComplianceSearch -Name $searchName -SharePointLocation All -ExchangeLocation All -
ContentMatchQuery $searchQuery
Start-ComplianceSearch -Identity $searchName#Create & start search for sample data
$searchName = "Sample Customer Information Search"
$searchQuery = "15080P9562 OR 1404001119 OR 15020J8317 OR 14050E2330 OR 16050E2166 OR 1704001118"
New-ComplianceSearch -Name $searchName -SharePointLocation All -ExchangeLocation All -
ContentMatchQuery $searchQuery
Start-ComplianceSearch -Identity $searchName
```

3. Run the following PowerShell commands and copy the generated GUIDs to an open instance of Notepad on your computer in the order in which they are listed.

```
#Generate three unique GUIDs
Write-Host "GUID1 = "([guid]::NewGuid()).Guid)
Write-Host "GUID2 = "([guid]::NewGuid()).Guid)
Write-Host "GUID3 = "([guid]::NewGuid()).Guid)
```

4. On your local computer, open another instance of Notepad and paste in the following content:

```

<?xml version="1.0" encoding="utf-8"?>
<RulePackage xmlns="https://schemas.microsoft.com/office/2011/mce">
<RulePack id="GUID1">
<Version major="1" minor="0" build="0" revision="0" />
<Publisher id="GUID2" />
<Details defaultLangCode="en">
<LocalizedDetails langcode="en">
<PublisherName>Contoso Ltd.</PublisherName>
<Name>Contoso Rule Package</Name>
<Description>Defines Contoso's custom set of classification rules</Description>
</LocalizedDetails>
</Details>
</RulePack>
<Rules>
<!-- Contoso Customer Number (CCN) -->
<Entity id="GUID3" patternsProximity="300" recommendedConfidence="85">
<Pattern confidenceLevel="85">
<IdMatch idRef="Regex_contoso_ccn" />
<Match idRef="Keyword_contoso_ccn" />
<Match idRef="Regex_eu_date" />
</Pattern>
</Entity>
<Regex id="Regex_contoso_ccn">[0-1][0-9][0-9]{3}[A-Za-z][0-9]{4}</Regex>
<Keyword id="Keyword_contoso_ccn">
<Group matchStyle="word">
<Term caseSensitive="false">customer number</Term>
<Term caseSensitive="false">customer no</Term>
<Term caseSensitive="false">customer #</Term>
<Term caseSensitive="false">customer#</Term>
<Term caseSensitive="false">Contoso customer</Term>
</Group>
</Keyword>
<Regex id="Regex_eu_date">(0?[1-9]|[[12][0-9]|3[0-1]][\/-](0?[1-9]|1[0-2]|j\x00e4n(uar)?
|jan(uary|uari|uar|eiro|vier|v)?|ene(ro)?|genn(aio)?|feb(ruary|ruari|rero|braio|ruar|br)?
|f\x00e9vr(ier)?|fev(ereiro)?|mar(zo|o|ch|s)?|m\x00e4rz|maart|apr(ile|il)?|abr(il)?|avr(il)|may(o)?
|magg(io)?|mai|mei|mai(o)?|jun(io|i|e|ho)?|giugno|juin|jul(y|io|i|ho)?|lu(glio)?|juil(let)?
|ag(o|osto)?|aug(ustus|ust)?|ao\x00fbt|sep|sept(ember|iembre|embre)?|sett(embre)?|set(embro)?
|oct(ober|ubre|obre)?|ott(obre)?|okt(ober)?|out(ubro)?|nov(ember|iembre|embre|embro)?|dec(ember)?
|dic(iembre|embre)?|dez(ember|embro)?|d\x00e9c(embre)?)[\/-](19|20)?[0-9]{2}</Regex>
<LocalizedStrings>
<Resource idRef="GUID3">
<Name default="true" langcode="en-us">Contoso Customer Number (CCN)</Name>
<Description default="true" langcode="en-us">Contoso Customer Number (CCN) that looks for additional
keywords and EU formatted date</Description>
</Resource>
</LocalizedStrings>
</Rules>
</RulePackage>

```

- Replace the values of GUID1, GUID2, and GUID3 in the XML text of step 4 with their values from step 3, and then save the contents on your local computer with the name ContosoCCN.xml.
- Fill in the path to your ContosoCCN.xml file and run the following commands.

```

#Create new Sensitive Information Type
$path="<path to the ContosoCCN.xml file, such as C:\Scripts\ContosoCCN.xml">
New-DlpSensitiveInformationTypeRulePackage -FileData (Get-Content -Path $path -Encoding Byte -
ReadCount 0)

```

- From the Security & Compliance tab, click **Classifications > Sensitive information types**. You should see the Contoso Customer Number (CCN) in the list.

## Phase 5: Demonstrate data protection

Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.

There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.

In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.

1. From the Security & Compliance tab of your browser, click **Home**.
2. Click **Data loss prevention > Policy**.
3. Click **+ Create a policy**.
4. In **Start with a template or create a custom policy**, click **Custom > Custom policy > Next**.
5. In **Name your policy**, provide the following details and then click **Next**:
  - a. Name: **EU Citizen PII Policy**
  - b. Description: **Protect the personally identifiable information of European citizens**
6. In **Choose locations**, select **All locations in Microsoft 365**. This will include content in Exchange email and OneDrive and SharePoint documents. And then click **Next**.
7. In **Customize the type of content you want to protect**, click **Find content that contains:** and then click **Edit**.
8. In **Choose the types of content to protect**, click **Add > Sensitive info types**.
9. In **Sensitive info types**, click **+ Add**.
10. In **Sensitive info types**, search for **IBAN**, select the check box for **International Banking Account Number (IBAN)**, and then click **Add**.
11. Confirm that the **International Banking Account Number (IBAN)** sensitive information type was added, and then click **Done**.
12. In **Content contains**, confirm that the sensitive information types were added and then click **Save**.
13. In **Customize the type of content you want to protect**, confirm **Find content that contains:** contains the **International Banking Account Number (IBAN)**, and then click **Next**.
14. In **Detect when content that's being shared contains:**, change the value from **10** to **1**, and then click **Next**.
15. In **Do you want to turn on the policy or test things out first?**, choose the following settings, and then click **Next**:
  - a. Select the option for **I'd like to test it out first**
  - b. Select the check box for **Show policy tips while in test mode**
16. In **Review your settings**, click **Create** after reviewing the settings. NOTE: After you create a new DLP policy, it will take a while for it to take effect.
17. On your local computer, open a private instance of your browser.
18. In the address bar, type **https://<YourTenantName>.sharepoint.com** and sign in using your global administrator account.
19. Click **Documents**.
20. Click the file named 'IBANs.docx'. You should see 'Policy tip for IBANs.docx'. The IBANs.docx file was shared with external recipients, which violates the DLP policy.

21. In the address bar, type: `https://outlook.office365.com`

22. Click **New - Email message** and provide the following:

- **To:** <a personal email address>
- **Subject:** GDPR Test
- **Body:** Copy in the table of values shown below.

NUMBER	COUNTRY	CODE	IBAN
1	Austria SEPA	AT	AT611904300234573201
2	Bulgaria SEPA	BG	BG80BNBG96611020345678
3	Denmark SEPA	DK	DK5000400440116243
4	Finland SEPA	FI	FI2112345600000785
5	France SEPA	FR	FR1420041010050500013M02606
6	Germany SEPA	DE	DE89370400440532013000
7	Greece SEPA	GR	GR1601101250000000012300695
8	Italy SEPA	IT	GR1601101250000000012300695
9	Netherlands SEPA	NL	NL91ABNA0417164300
10	Poland SEPA	PL	PL27114020040000300201355387

Note:- This sample data set is derived from publicly available information and is intended to be used for test purposes only.

23. You will see that the DLP policy recognized that body of the email contains IBANs and provides you with the policy tip at the top of the message window.

24. Close the private instance of your browser.

## Phase 6: Demonstrate reporting

In this phase, you demonstrate Microsoft 365 reporting based on the DLP policy configured in Phase 5.

1. From the Security & Compliance tab of your browser, click **Home**.
2. Click **Reports > Dashboard > DLP policy matches**.
3. Your DLP policy helps identify and protect organization's sensitive information. For example, in the report you will see that the policy identified the document that contains IBANs stored in SharePoint Online.



# California Consumer Privacy Act (CCPA) Frequently Asked Questions

11/30/2020 • 8 minutes to read • [Edit Online](#)

## NOTE

This topic is provided "as-is." Information and views expressed in this topic, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. This topic has been created as a guide and should not be construed as legal advice. You should consult with your own legal professionals. This topic does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this topic for your internal, reference purposes.

## Fast FAQs

### What is the CCPA?

The California Consumer Privacy Act (CCPA) is the first comprehensive privacy law in United States. It was signed into law at the end of June 2018 and provides a variety of privacy rights to California consumers. Businesses regulated by the CCPA will have a number of obligations to those consumers, including disclosures, General Data Protection Regulation (GDPR)-like rights for consumers, an "opt-out" for certain data transfers and an "opt-in" requirement for minors.

### Who needs to know about the CCPA?

The CCPA only applies to companies doing business in California, which annually satisfy one or more of the following: (1) have a gross revenue of more than \$25 million, (2) derive 50% or more of its annual revenue from the sale of consumer personal information, or (3) buys, sells, or shares the personal information of more than 50,000 consumers.

### When will the CCPA come into effect?

The CCPA goes into effect on January 1, 2020. However, enforcement by the Attorney General (AG) will not begin until July 1, 2020.

### How will the CCPA affect my company?

Many of the CCPA's rights afforded to Californians are similar to the rights the GDPR provides, including the disclosure and consumer requests similar to data subject right (DSR) requests, such as access, deletion, and portability. As such, customer can look to our existing GDPR solutions to help them with their CCPA compliance.

To begin your CCPA journey, you should focus on five key steps:

- **Discover:** Identify what Personal Information you have and where it resides.
- **Map:** Determine how you are sharing Personal Information with third parties and identify if the third party is subject to an exception from the CCPA opt-out requirements.
- **Manage:** Govern how the data is used and accessed.
- **Protect:** Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches.
- **Document:** Document a data breach response program and ensure your contracts with applicable third parties are able to take advantage of the opt-out exceptions.

You need to understand what your organization's specific obligations are under the CCPA and how you meet

them, though Microsoft is here to help you on your journey.

## Comprehensive FAQs

### What rights must companies enable under the CCPA?

The CCPA requires regulated businesses that collect, use, transfer, and sell personal information to, among other things:

- Provide disclosures to consumers, prior to collection, regarding the categories and purposes of collection.
- Provide detailed disclosures in a privacy policy regarding the sources, business purposes, and categories of personal information that is collected, including how those categories are sold or transferred to other entities.
- Enable Consumer rights relating to access, deletion, and portability of the specific pieces of personal information that has been collected by you.
- Enable a control that will permit consumers to opt out of the “sale” of the consumer’s data. However, certain transfers, like transfers to service providers, remain permitted.
- For minors, under 16, enable an opt-in process so that no sale of the minor’s personal information can occur without actively opting in to the sale.
- Ensure that consumers are not discriminated against for exercising any of their rights under CCPA.

### What are the CCPA required disclosures?

The CCPA requires disclosure of the following:

- Categories of personal information of the consumer that have been collected.
- Categories of sources used in collection.
- The business or commercial purposes for collecting.
- The categories of third parties with whom the personal information is “shared”.
- Categories of personal information that has been “sold” and the categories of “third parties” to whom each category of personal information was sold.
- Categories of personal information that has been “disclosed for a business purpose” (that is, transferred but not a “sale”) and the categories of “third parties” to whom each category of personal information was transferred.
- The specific pieces of personal information that has been collected about that consumer.

### How is data “sold” under the CCPA?

The definition of “sell” in the CCPA is incredibly broad, including “making personal information available to” a third party for monetary or other valuable consideration. Where a consumer has elected to “opt-out”, the business will be required to turn off the flow of personal information to any third party.

The CCPA does provide a number of carve-outs to this “sale” opt-out control. The three primary carve-outs are transfers (i) to a Service Provider, (ii) to an “exempted entity” or “contractor”, and (iii) at the direction of the consumer. Even if a consumer has elected to “opt-out”, personal information can continue to transfer to third parties who fit into those carve-outs.

To take advantage of the first two exemptions, businesses will have to ensure that the transfers are governed by written contracts containing the specific terms required by the CCPA.

### What do *Businesses* and *Service Providers* mean in the context of CCPA?

In the context of CCPA, Businesses are individuals or entities that determine the purposes and means of the processing of consumer’s personal data, and Service Providers are individuals or entities that process information on behalf of a business. These are broadly synonymous with the terms *Controllers* and *Processors* used in GDPR.

## How much can companies be fined for noncompliance?

The private right of action in the CCPA is limited to data breaches. Under the private right of action, damages can come in between \$100 and \$750 per incident per consumer. The California AG also can enforce the CCPA in its entirety with the ability to levy a civil penalty of not more than \$2,500 per violation or \$7,500 per intentional violation.

## What is Microsoft doing to achieve CCPA compliance?

As Microsoft has implemented GDPR-related DSRs globally, we are currently in an excellent position to meet the related CCPA requirements. We have also reviewed our third-party data sharing agreements and taken steps to establish that the necessary contractual terms are in place to ensure that we do not "sell" personal information.

## What are some tools that can help my organization to start preparing for CCPA?

- Start leveraging the GDPR assessment in Compliance Manager as part of your CCPA privacy program.
- Establish a process to efficiently respond to Consumer Requests.
- Set up label and policies to discover, classify & label, and protect sensitive data with Microsoft Information Protection.
- Use email encryption capabilities to further control sensitive information.
- Learn more in this [blog post](#).

## What are the differences between GDPR and CCPA?

There are many differences. It's easier to focus on the similarities, including:

- Transparency/disclosure obligations.
- Consumer rights to access, delete, and receive a copy of data.
- Definition of "service providers" that is similar to how GDPR defines "processors" with a similar contractual obligation.
- Definition of "businesses" that encompasses the GDPR definition of "controllers".

The biggest difference in CCPA is the core requirement to enable an opt-out from sales of data to third parties (with "sale" broadly defined to include sharing of data for valuable consideration). This is a narrower and more specific obligation than the broad GDPR right to object to processing, which encompasses this type of "sale," but is not specifically limited to covering this type of sharing.

## What are *Processors* and *Controllers*?

A controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. A processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

## What specifically is deemed personal information?

Personal information is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. The defined term "personal information" roughly lines up with "personal data" under GDPR. However, CCPA also includes family and household data.

Examples of personal data include:

### *Identity*

- Name
- Home address
- Work address
- Telephone number

- Mobile number
- Email address
- Passport number
- National ID card
- Social Security Number (or equivalent)
- Driver's license
- Physical, physiological, or genetic information
- Medical information
- Cultural identity

#### *Finance*

- Bank details / account numbers
- Tax file number
- Credit/Debit card numbers
- Social media posts

#### *Online Artifacts*

- Social media posts
- IP address (EU region)
- Location / GPS data
- Cookies

#### **How does the CCPA apply to children?**

- CCPA introduces parental consent obligations consistent with The Children's Online Privacy Protection Act (COPPA) for children under the age of 13.
- For children between 13 and 16 years old, CCPA imposes a new obligation to obtain opt-in consent from the child for any "sale" of their personal information.

#### **What about personal data from my employees?**

In October 2019, a number of amendments were passed to the CCPA. One amendment clarified that the CCPA obligations do not apply to the personal information of employees of the business. However, legislators put a one-year sunset on that exemption. We expect California to legislate a new data protection law for employees in 2020.

#### **As a Microsoft customer, do I need to implement the opt-out control for transfers to Microsoft?**

No. As a provider of online services, we are taking steps to ensure that we qualify as a "Service Provider" under CCPA. As noted above, transfers of personal information to service providers are permitted, even where a consumer has opted out.