ManageEngine
Log360

A Security Admin's Survival Guide to the GDPR

www.manageengine.com/log-management

Table of Contents

Scope of this guide

Every enterprise that handles the personal data of EU citizens needs to comply with the General Data Protection Regulation (GDPR) before May 25, 2018. Non-compliance with this regulation attracts a huge penalty—up to four percent of a company's global annual turnover or €20 million, whichever is higher.

This hefty fine is not the only highlight of the GDPR. As one of the most stringent compliance mandates of recent times, the GDPR aims to standardize how organizations deal with personal data. The GDPR lays out requirements that ensure the safety of personal data at all stages of data handling, including collection, storage, processing, transfer, and deletion.

Translating the GDPR's security requirements into actionable items is the toughest job for any security professional. This guide aims to provide the exact actions that security administrators and to-be data protection officers can take to ensure their organization's GDPR compliance.

The GDPR requirements that need your attention

With 11 chapters and 99 articles, the GDPR lays out rules for safeguarding personal data in all stages—including data that is at rest and in motion. But more than 75 percent of this regulatory mandate dictates the way organizations have to collect personal data and addresses the rights of data subjects. The remaining 25 percent of the GDPR's requirements, which outline the security of processing rules, need the attention of security professionals.

Overview of the requirements that need the attention of security professionals

- Principles relating to the processing of personal data: Article 5
  - Using appropriate technical or organizational measures to prove that data is processed in a secured manner and is protected against unauthorized or unlawful processing, accidental loss, and destruction or damage.

- Responsibilities of a controller: Article 24
  - Deploying technical and organizational measures and implementing data protection policies to ensure and demonstrate that data processing is being carried out in accordance with the requirements.

- Security of processing: Article 32
  - Deploying technical measures:
    - To ensure that personal data is encrypted.
    - To ensure that the confidentiality, integrity, availability, and resilience of the system and service that store personal data is maintained.
    - To restore the availability and access to personal data in the event of a mishap.
  - Implementing security measures to ensure that personal data is protected from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and transmission.

- Notification of personal data breach to the supervisory authority: Article 33
  - Deploying technical measures to detect and report a personal data breach in no more than 72 hours after its occurrence.
  - Generating incident reports that provide information on the nature of the personal data breach, including the categories and approximate number of personal data records and data subjects affected.
  - Documenting the breach, its effects, and the remedial action taken.

Prep steps for GDPR compliance

Before you start translating the GDPR's requirements into security policies, you must:

- **Understand who you are:** The GDPR categorizes each organization as either a controller or a processor. While controllers are responsible for collecting personal data from data subjects, processors perform data operations—storing, transmitting, structuring, altering, deleting, and more—on behalf of the controller. Sometimes, an organization can act as both a controller and processor. In this case, ensure that you meet the responsibilities stated for both controllers and processors.

  The responsibilities for controllers and processors are different. The major function of a controller is just to collect personal data in accordance with the GDPR's requirements and constantly check whether the processor is performing their operations as per GDPR rules. The processor, on the other hand, needs to set up proper security policies within its organization and prove to the controller that data operations are being performed in accordance with GDPR regulations. If an incident occurs, like a breach or any other threat to personal data, processors need to report it to the controller and the supervisory authorities immediately.

- **Know what kind of personal data your organization processes:** Depending on your business context, get to know the kind of personal data your organization processes. Beyond that, understand the data flow in your organization—where data collection starts, where data is stored, what kind of applications process personal data, and when data is supposed to be deleted.

1. Data discovery, isolation, and backup

The first step in ensuring personal data security is to discover where personal data resides in your organization. It could be stored in databases, file servers, or even in Excel sheets and Word documents.

Once you discover where the data resides, isolate that personal data from the rest of the non-confidential information in your organization.

Why is it so important to separate this data from non-confidential information?

- Isolation helps in setting up exclusive security configurations for personal data. These configurations can act as an additional layer of security.
- Personal data isolation makes auditing efficient. Enabling granular auditing for only those systems that hold personal data will help you easily track potential threats and reduce the risk of missing out on a critical security incident that could possibly lead to a data breach.
- It's easier to restrict access to personal data once you've isolated that data. After isolating data, set up different levels of access policies to ensure that only authorized individuals can access personal data.
- Isolating personal data whenever possible not only helps in adding an extra security layer; it also helps in understanding the data flow—where personal data is being collected or fed, how long it's stored, and what processes are being performed on it.

Once you've isolated personal data, back it up so you can quickly restore the availability and access to that personal data (Article 32 (1)(c)) in the event of a mishap.

2. Setting up security configurations

Article 32 of the GDPR (Security of processing) instructs enterprises to deploy appropriate technical measures to ensure data security.

To meet the requirements stated in this article, you should practice security hardening for the platforms wherein personal data is stored.

Each of the platforms that store personal data—say, operating systems, applications, and devices—have different security configurations and you must take proper care to configure each platform separately.

Below is a list of security hardening best practices for common platforms and devices. If you need granular information on securing your network, feel free to contact our IT security experts.

Table 1: Security configurations for common platforms.

Platform/device	Security configuration
Firewall 	1. Not all employees in your company need to access the personal data you store. Add an extra layer of security by adding rules that limit access to servers that store personal data to specific hosts in your network. This makes it harder for malicious employees or rogue users who have stolen privileged users' credentials to access or steal personal data. 2. Configure rules that allow traffic to specific destination ports/services. 3. Set up firewall rules to deny traffic from illegitimate sources. This helps to detect and, to a certain extent, prevent external security attacks.

Windows server or file server 	1. Configure security groups. Include only privileged users who are supposed to access personal data. 2. Set up group policies that exclusively grant privileges to the security groups associated with personal data access. 3. Set up access control lists (ACLs) to granularly allow/deny operations to be performed on personal data stored as files and folders.
MS SQL database 	1. Configure firewall rules so that your SQL server isn't exposed to the internet. 2. Rename the default privileged account credentials. Especially the default **sysadmin** account. 3. Set up complex and strict password policies for the **sa** and **SQL server** login accounts. 4. Change the default ports associated with your SQL server installation. 5. Enable Windows Authentication instead of SQL Authentication. Windows Authentication validates users' credentials based on the Windows principal token in the operating system.
Oracle database 	1. Provide **CREATE EXTERNAL JOB** privileges to database administrators only. 2. Enforce strict, complex password policies. For instance, stringent rules for updating and making new passwords. 3. Enable Data **Dictionary Protection** by setting the **07_DICTIONARY_ACCESSIBILITY** initialization parameter to FALSE. This prevents users with **ANY** privilege from accessing the data dictionary. A data dictionary is a set of database tables that stores critical information such as names of database users, privileges and roles of the users, auditing information, and so on. Therefore it becomes essential to secure the data dictionary.

Amazon Web Services (AWS) instance 	1. Tag personal data as confidential and limit access to data with that tag by setting up bucket-level or object-level permissions in addition to identity access and management (IAM) policies. 2. Encrypt personal data residing in AWS RDS and EBS using file, partition, volume, or application-level encryption options. 3. In Amazon S3, enable Versioning so you can restore personal data in case of accidental or intentional unauthorized data modifications. 4. To protect personal data while in transit, especially when it's traversing a public network, encrypt the data using IPSec ESP and/or SSL/TLS.

3. Configuring alerts in a security solution to detect incidents

Once you've configured your basic and advanced security configurations, you need to enable auditing. Auditing helps to track all the activities that are happening in your network. After enabling auditing policies, set up alert profiles in security solutions to immediately detect any deviation from normal behavior. These solutions should include security information and event management (SIEM), data loss prevention (DLP), or unified threat management (UTM).

This helps to preemptively block any breach attempts and thereby save your data from being exposed or mishandled.

Rules for setting up security alerts:

- Enable auditing on all platforms. Make sure that you only enable necessary auditing policies; enabling all auditing policies will slow down your systems and throw a large number of false positives.
- Baseline your normal network activity. Automatically tune your security solution to pick up anything abnormal.
- Detect critical incidents such as:
    a. Unauthorized firewall rule changes
    b. Group membership modifications
    c. Group Policy changes
    d. User behavior anomalies—too many logon failures, a logon from an unusual place, privilege escalations, etc.
    e. File or folder permission changes and changes to ACLs
    f. User permission changes
    g. Changes to database server accounts and roles
- Link your security solution with a proper incident management system so you can establish accountability for incident investigations.

4. Setting up notifications to instantly detect breach attempts

While the previous section was about detecting incidents that are potential threats, here we'll talk about setting up notifications to detect an ongoing breach or a breach that has already happened.

According to Article 33 of the GDPR (notification of a personal data breach to supervisory authorities), organizations must take no more than 72 hours to detect and report a data breach.

What you need to do

Set up alert profiles to detect common data breach attempts such as SQL injection, ransomware attacks, logon attacks, malware installation, denial of service (DoS) and distributed denial of service (DDoS) attacks, and more.

Choose a security solution that lets you create customized rules to detect attack patterns.

Analyze the pattern of an attack that happened in your environment and identify its various indicators of compromises (IoCs). Set up custom alerts that correlate these IoCs and initiate an automatic workflow to contain attacks of a similar kind in the future, right at the initial stage of an attack.

5. Generating a post-breach incident report for assessments

Generating an incident report through forensic analysis is just as important as detecting breaches for two reasons:

1. An incident report helps you determine the total impact of the breach.
2. The report usually contains intricate details about the attack, including the vulnerable entry point and attack pattern. It's essential to retain this information to preemptively block similar breaches in the future.

What should be in an incident report?

Article 33 of the GDPR outlines the details that should be included in an incident report. Make sure that you:

- Elaborate on the personal data breach incident—how it happened, how many records were affected, and the number of data subjects who might be affected by the breach.
- Provide the name and contact information of either the data protection officer or the security professional who can provide further details about the data breach.
- Describe the consequence of the personal data breach, e.g. what data was lost or modified.
- Point out the security measures taken to address the data breach. This includes the measures taken to contain (in the case of an ongoing breach) and mitigate the adverse effect of the attack, as well as the appropriate steps taken to strengthen the security so as to preemptively block similar breaches in the future.

Does ManageEngine help meet GDPR requirements?

Absolutely. ManageEngine, the real-time IT management company, has a wide range of IT security solutions that can help you meet the GDPR's security requirements. Remember, each organization's network is unique and there's no point product that helps meet all compliance mandates. However, ManageEngine integrates its security products into a single solution that helps resolve various compliance challenges efficiently.

For instance, Log360, ManageEngine's comprehensive SIEM solution, includes:

- **ADAudit Plus,** a real-time Active Directory auditing tool, which helps detect and mitigate internal threats.
- **EventLog Analyzer,** a log management tool, which aids in mitigating external security attacks and performing efficient forensic analysis.
- **Cloud Security Plus,** a public cloud log management tool, which helps analyze user behavior on public cloud platforms, such as Amazon Web Services and Azure.
- **O365 Manager Plus,** a complete Office 365 reporting and auditing tool, which aids in detecting anomalous behavior in Office 365.

With its wide range of capabilities, Log360 will be your best bet to resolve your GDPR challenges.

Explore Log360 Learn more

Explore Log360

ManageEngine
Log360

Log360 is a comprehensive SIEM solution that helps security professionals meet their heavy auditing, security, and compliance needs. With over 1,200 predefined reports, 900 alert profiles, and over 70 correlation actions and rules, this solution can detect and mitigate both internal and external threats. Log360's in-depth Active Directory auditing capability helps administrators closely monitor privileged user activity and other user behaviors to instantly detect anomalies. Log360 also supports more than 700 log sources, including routers, switches, firewalls, IDS/IPS, servers, databases, and web servers. It collects, analyzes, correlates, and archives log data from these sources and ensures data security 24/7.

Try Log360 for free

About the author

Subhalakshmi Ganapathy currently works as a Senior Product Marketing Analyst for IT Security Solutions at ManageEngine. She has in-depth knowledge in information security and compliance management. She provides strategic guidance for enterprises on Security Information and Event Management (SIEM), network security, and data privacy.

Reach out to Subha at **subhalakshmi.g@manageengine.com.**