December 2018

G Suite Data Protection Implementation Guide

This guide is intended to help G Suite customers better understand how to use and customize G Suite services and settings to help meet data protection compliance needs. We recommend that you consult with a legal expert to obtain guidance on the specific requirements applicable to your organization, as this guide does not constitute legal advice.

Google Cloud

Google Cloud

Table of contents

Google Cloud

Processing personal data within our services

Under the G Suite Data Processing Agreement (DPA), Google acts as a processor of the personal data that is submitted, stored, sent or received by your organization via G Suite services. As a customer, you typically act as the controller of such personal data, which means that you determine the purposes and means of processing. Google acts as a processor, which means that we process such data on your behalf and under your instructions.

We recommend that you conduct a meaningful assessment of the G Suite Terms of Service for US customers or EMEA customers (here for customers in EMEA outside the European Economic Area (EEA) and here for EEA customers in EMEA) and the G Suite DPA, as well as the terms applicable to any other Google services that you use in connection with your G Suite account. You will find below information on the terms applicable to the G Suite services and those other Google services:

G Suite Services

G Suite Core Services

G Suite Core Services are governed by the G Suite Terms of Service described above and are in the scope of the G Suite Data Processing Amendment (DPA).

The list of G Suite Core Services is available here.

Organizations established outside the EEA that are subject to data protection regulations and wish to use G Suite to process personal data should consider opting in to the G Suite DPA, and are required to do so if they are subject to the EU's General Data Protection Regulation. In order to review and accept the DPA in the Google Admin Console, an administrator from your organization can follow the instructions provided here, or watch this video. For organizations established in the EEA , the DPA is automatically incorporated into their contracts.

Other services for G Suite

In addition to G Suite Core Services, you may also use "Other Services" for G Suite, such as those listed here. These services are governed by the G Suite Terms of Service and are also in the scope of the G Suite DPA.

Complementary Services

A customer may also use “Complementary Services” in connection with G Suite services. Complementary Services (such as Hire by Google) are governed by separate Terms of Service. These services must be activated by a G Suite customer and require acceptance of the applicable separate Terms of Service.

Additional Products

“Additional Products” are any additional Google services that may be used with a Google account. A non exhaustive list of Additional Products is given here. These products are not part of the G Suite offering and are not covered by the G Suite DPA. Your organization’s Legal Counsel, Data Protection Officer (DPO), or equivalent, when applicable, should conduct an impact assessment of the processing of personal data with these products to determine whether, and how, your organization can fulfill its obligations as a data controller or a data processor, as applicable, for each of these products.

The Terms of Service applicable to the use of Additional Products can be found by following this link and clicking on “View available services.” Please also refer to Google’s Privacy Policy to conduct a privacy and security assessment on the processing of personal data in relation to any Additional Products that are subject to the Privacy Policy.

Google Cloud

Implementation considerations for G Suite Core Services

G Suite Core Services have configurable settings to help ensure that your organization's data is secured, used, and accessed according to your organization's unique requirements.

The configurations below reflect the strictest controls that a G Suite customer can implement. We suggest that you seek advice from your Legal, Compliance, and Security teams to determine what configurations may be most appropriate for your organization.

Monitoring account activity

The reports and logs available in the Google Admin Console make it easy for a super administrator in your organization to examine potential security risks, measure user collaboration, track access, analyze administrator activity, and much more. To monitor logs and alerts, your super administrators can configure notifications to receive activity alerts, such as suspicious login attempts; user suspended by an administrator; new user added; suspended user made active; user deleted; user's password changed by an administrator; user granted admin privileges; and user's admin privileges revoked. The administrator can also examine potential security risks by reviewing reports and logs on a regular basis, focusing on key trends in the highlights section, overall exposure to data breach in security, files created in apps usage activity, account activity, and audits.

Gmail

Gmail provides controls designed so that messages and attachments are only shared with the intended recipients. When composing emails and inserting files using Google Drive that potentially contain personal/sensitive data, end users can choose to share only with the intended recipients by changing the link settings to “Private.” If end users keep a file Private, recipients won't be able to see it if:

- their email address isn't a Google account
- they received the message through a mailing list (unless the mailing list is managed through Google Groups and the file is shared with the Group).

If the file is not already shared with all email recipients, the default will be set to be viewable by “Anyone with the link” within the G Suite Organization (Exhibit A). Administrators can also control how users in the organization share Google Drive files and folders (Exhibit B), as further described in section related to Drive below.

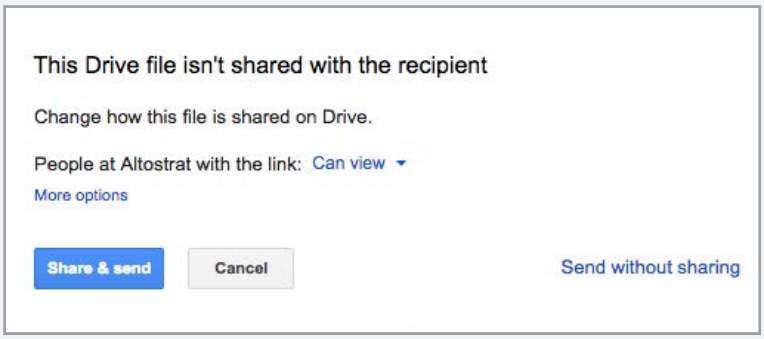


Exhibit A

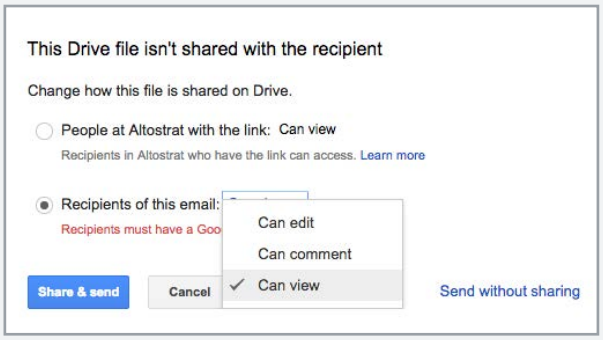


Exhibit B

Please refer to the “Use of third party applications” section below for guidance on using third party applications with Gmail.

Calendar

By default, meeting information in calendar is visible to anyone within the domain, and availability information (i.e. whether a user is free or busy) is visible to external parties. Within the domain, users can control whether and how their calendars are shared, and administrators can set sharing options for all calendars created in the domain. To limit exposure of personal/sensitive data within the domain, users may set calendar entries that contain personal or sensitive data to “Private.” Calendar also provides a feature that can add a link to a Hangout video meeting to a Calendar entry.

After conducting a risk assessment, where necessary your administrator can disable the option to automatically add Hangout video calls to calendar event entries for users who manage personal/sensitive data. (Exhibit A)

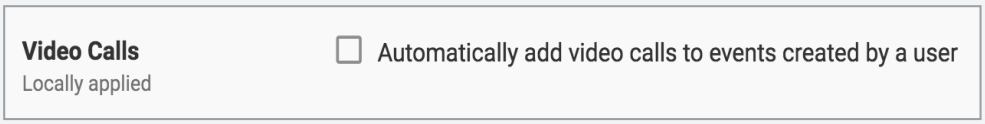


Exhibit A

Administrators may also consider setting calendar sharing options to “No sharing” or “Only free/busy information”, depending on the needs of the organization. (Exhibit B-C)

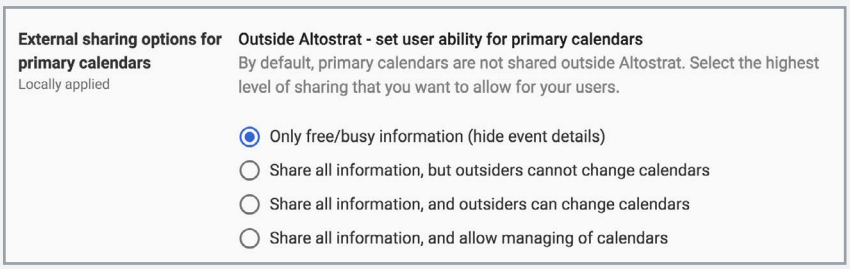


Exhibit B

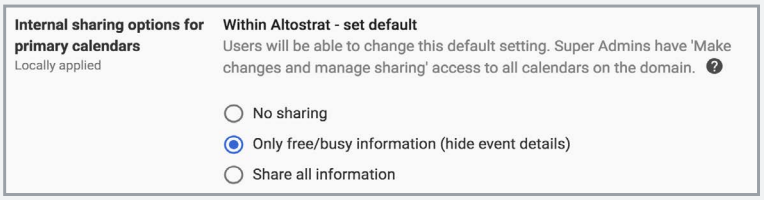


Exhibit C

Drive

**includes: Docs, Sheets, Slides, and Forms*

When sharing files in Google Drive (including Docs, Sheets, Slides, and Forms), users can choose who can view and access files and folders, as well as the editing and sharing capabilities of collaborators (Exhibit A). When creating and sharing files in Google Drive, users should avoid including personal/sensitive data in the titles of files, folders, or Team Drives.

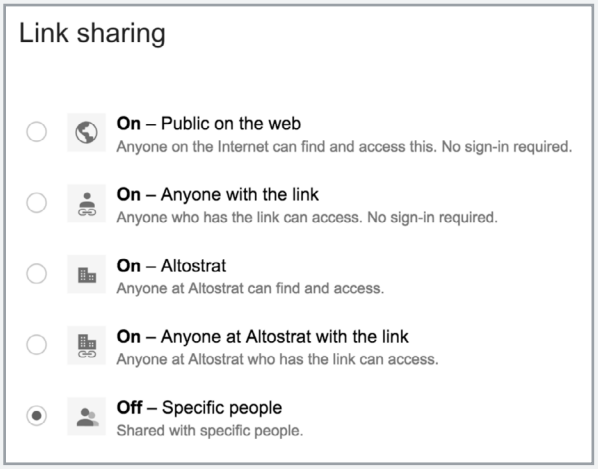


Exhibit A

Administrators can also control how users in the organization share Google Drive files and folders. For example, they can restrict sharing of files with users outside the domain, or set default file visibility to "Private" (Exhibit B). Administrators can also manage the sharing settings for Team Drives, including controlling whether external users can be members. For more on Team Drives, see this article.

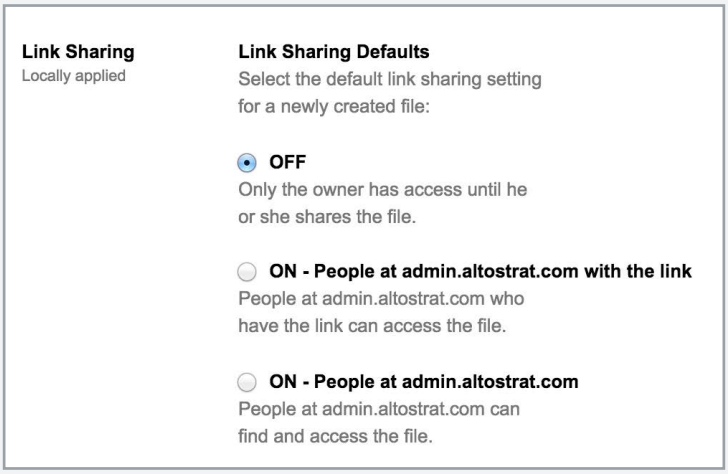


Exhibit B

Use of third party applications with Google Drive and Google Docs

Organizations should evaluate the usage of third party applications. Administrators have the option to disable users from installing third party applications, such as Google Drive apps and Google Docs add-ons.

We recommend that your organization reviews the security documentation provided by the third party developer, as well as the applicable data processing terms, before using any such third party application with Google Drive and Google Docs.

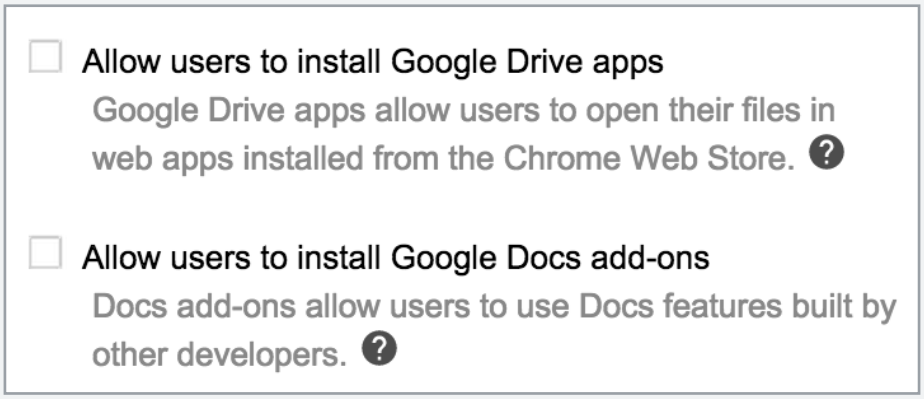


Exhibit A

Please refer to the section "Use of third party applications" below for additional guidance on using third party applications.

Keep

In Drive sharing settings for Google Keep, administrators can set file sharing permissions to the appropriate visibility level for the G Suite account. Administrators can “Restrict” or “Allow” sharing of documents outside the domain by users, and set the default file visibility to “Private.” (Exhibit A)

The sharing settings for notes created in Google Keep are a subset of Drive sharing settings, but all Keep notes created by users have a default visibility set to “Private,” regardless of the Drive setting.

Google Keep does not support the concept of “Public” notes, or notes visible to those with the URL. Instead, users can choose to add collaborators to individual Keep notes via email addresses or group aliases. All collaborators added to a note have full access to view and edit its contents (e.g. content in the title, body and list of the note, in addition to any attached images, drawings, or audio) (Exhibit B)

Users can color, label, add reminders to, and archive their notes. However, these note attributes are per user, and are not shared with other note collaborators. The original owner of a note has the option to put the note in the trash, and doing so will “Trash” it for all collaborators as well. Collaborators on a note are not able to trash the note, but can choose to unsubscribe from it.

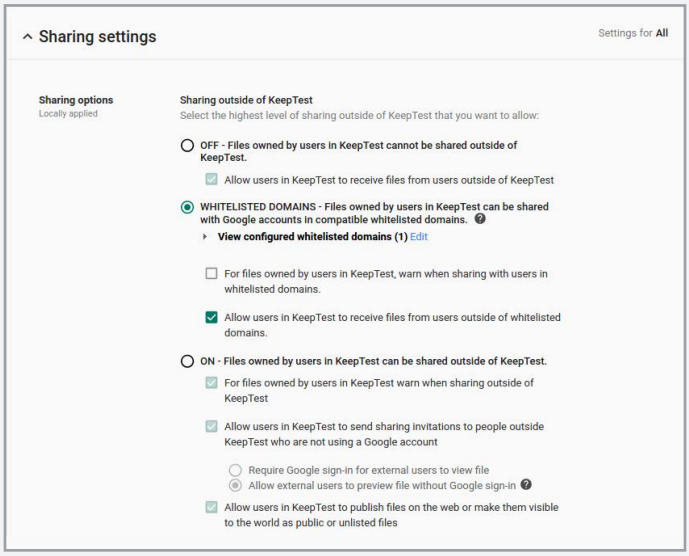


Exhibit A

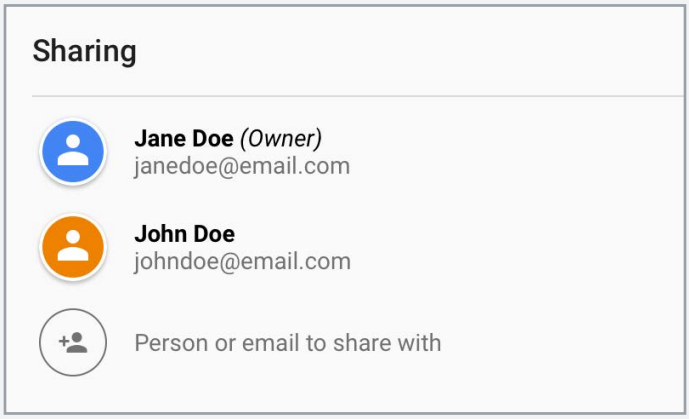


Exhibit B

Sites

Sites (both classic and new versions), like all G Suite Core Services, does not use customer data for advertising purposes or to serve ads. Sites owners may elect to enable Google Analytics on their Sites, as well as embed other content that may process the personal data of visitors to their Sites. G Suite does not access Google Analytics data.

For sites that process personal/sensitive data, users should configure Sites sharing and visibility settings appropriately. Personal/sensitive data can be included in a site in the form of text, images, or other content (such as a Google Calendar or content stored in Google Drive (including Docs, Sheets, Slides, and Forms)). Configuration instructions for these settings are outlined below for each version of Sites (classic and new):

Sites (classic version)

For sites containing personal/sensitive data, users can use the sharing settings to control who can edit or view their sites and turn on page-level permissions to control who has access to individual web pages within a site.
(Exhibit A)

Administrators may want to consider setting the default visibility for sites to “Private.” (Exhibit B)

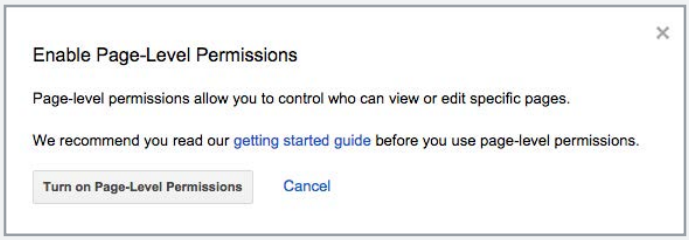


Exhibit A

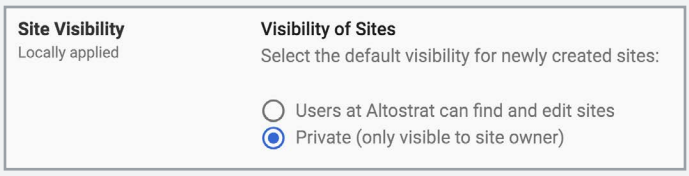


Exhibit B

Sites (new version)

The new version of Sites relies on a combination of Sites and Drive settings. Administrators can allow users to create and edit sites or restrict them from doing this by means of a control located under the Sites icon in the Admin console. Administrators can control the level of sharing and visibility allowed for these sites using the sharing settings for Drive in the Admin console.

For sites containing personal/sensitive data, users should consider giving limited editing access to specific individuals, and publishing their site only within their domain.

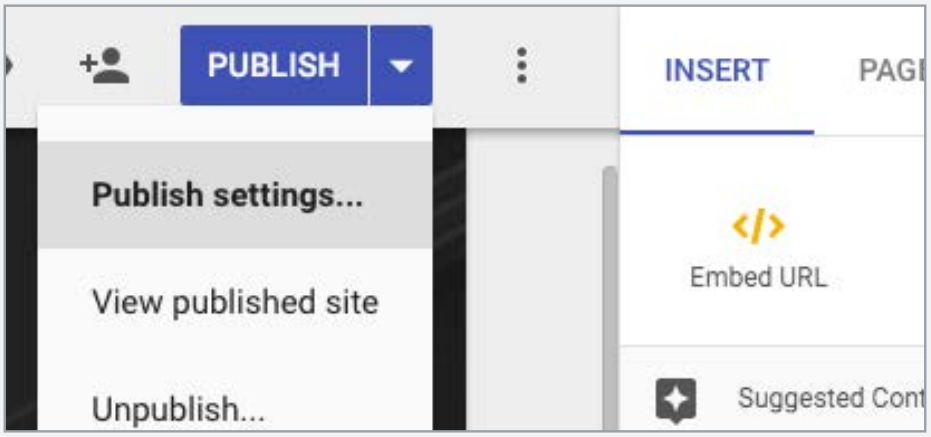


Exhibit A

Jamboard

Jamboard is a collaborative, digital whiteboard designed to make it easy to create without boundaries and share ideas in real time. Moving the whiteboard to the cloud, Jamboard also includes a Jamboard app that can be deployed on other devices, such as a phone or tablet, so users can collaborate regardless of location. Documents hosted on any of the above devices are called Jams.

Your administrator can configure settings for Jamboard within the Admin console. The Jamboard app has a service On/Off switch in the Admin console, shown below. This is where an administrator can turn off the service if they wish to.

For more information, please refer to Turn on the Jamboard service for users support article. (Exhibit A)

Only an active Jam session is stored locally on a Jamboard device. Once a new Jam is started, the previous Jam document is deleted from the device.

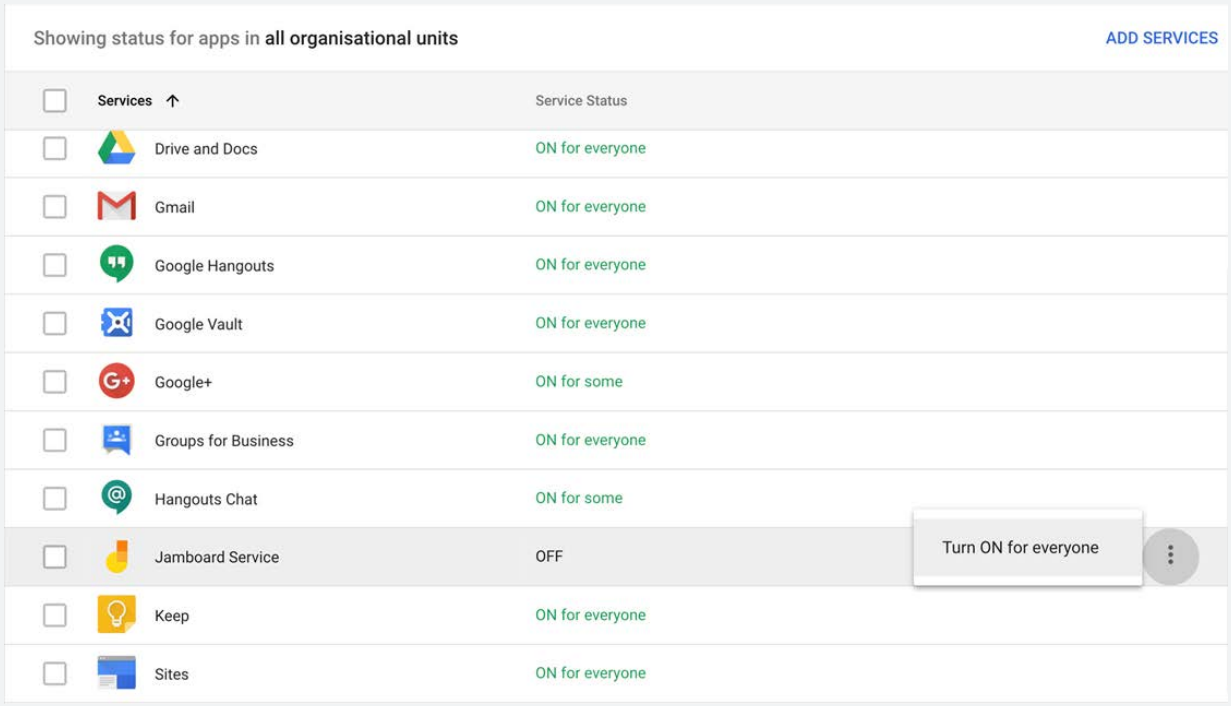


Exhibit A

Jamboard

Sharing settings for Jamboard

In Drive sharing settings, administrators will be able to set file sharing permissions to the appropriate visibility level for the G Suite account. Administrators can “Restrict” or “Allow” users to share documents outside the domain, and set the default file visibility to “Private.”

The sharing settings for Jam files are a subset of Drive sharing settings. For more information on how to use the Jamboard to create, host, and edit Jams, refer to the Working in a live Jam session support article. *(Exhibit A)*

Jam files created on a board will initially be owned by the board account. Once a user claims a file from the board, ownership is transferred to the user, and the board will appear in the “Who has access” list as a collaborator (see image above for reference). Only users within the same domain as the board can claim Jam files from the board.

The original owner of a Jam file has the option to “Trash” the Jam, which will trash it for all collaborators as well. Collaborators can also trash a Jam file, but that does not trash it for any other collaborator; it simply removes the Jam file from their Jam list.

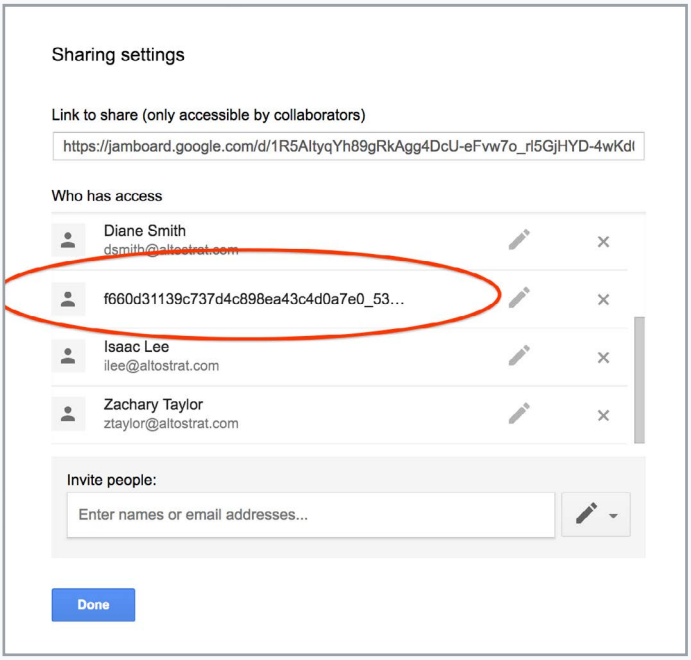


Exhibit A

Google Hangouts

**chat messaging feature only*

Users may choose to start a new conversation when adding multiple members to a chat conversation, since new members added to group chats can see the previous chat history. We recommend that users refrain from using personal/sensitive data when naming a group chat.

Administrators can control whether their users can chat with others outside of their organization or display their chat status outside of their organization, and can warn users when they are chatting with others outside of their organization. For more information, see this article.

Additionally, Google Hangouts settings allow users to directly control whether others inside or outside of their organization can see when they were last seen online, which device they are on, and when they are in a video or phone call on their devices.

Administrators are able to configure these settings to be consistent with the organization's policies.

Hangouts Chat

Hangouts Chat provides several options for administrators to use to control sharing of personal and sensitive data. Hangouts Chat can be enabled or disabled for everyone in the domain or selectively enabled for specific organizations.

To enable the service for specific organizations, administrators can select the “ON for some organizations” option which displays “Organizational Units” to search and select.

Note that cross domain and external communication is not supported in Hangouts Chat. (Exhibit A)

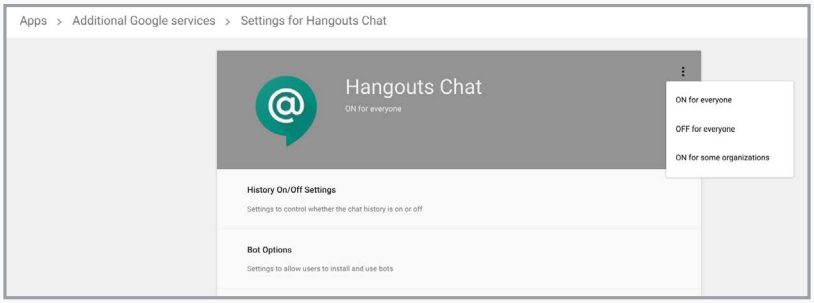


Exhibit A

Users may prefer to create a new room when adding multiple members to a chat conversation. Additionally, users should avoid using personal or sensitive data in room naming. New members that are added to rooms will be able to see previous chat history. Invitees can preview the room and read messages. (Exhibit B)

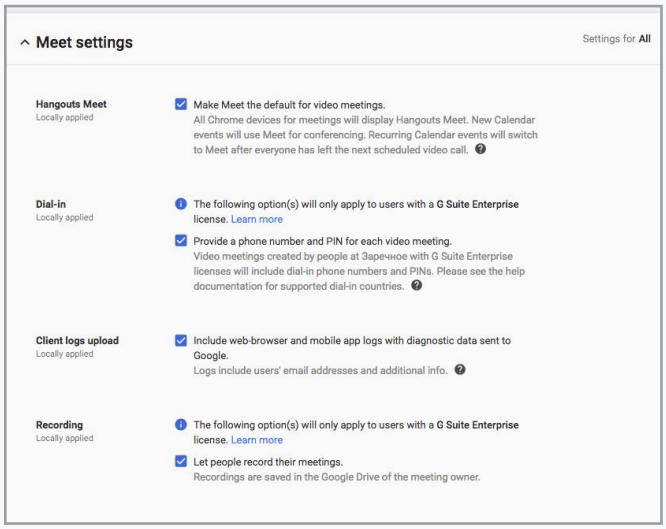


Exhibit B

Hangouts Meet

**Hangouts new video meeting experience*

When configuring and using Meet, please ensure the checkbox below is selected in the Hangouts administrator settings. Enabling Meet, the new video meeting experience, will cause Google Calendar to offer this type of video meeting instead of classic Hangouts video calls.

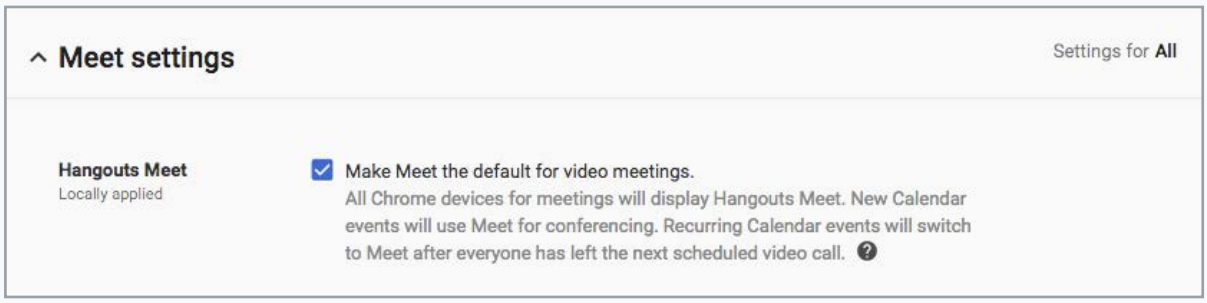


Exhibit A

To prevent users from starting video calls from classic Hangouts, uncheck the box below to disable this functionality.

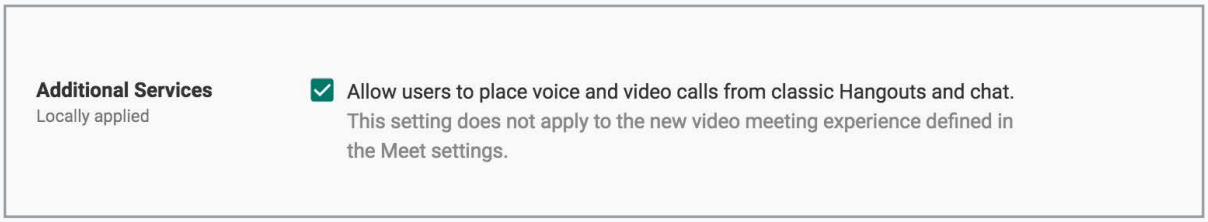


Exhibit B

Meet allows users to control whether external guests may participate in each video meeting. Users in the same domain can control who gets invited to the meeting, determine whether to permit anonymous guests to join a running video call, and remove unwanted participants from the call. Please see the Hangouts support pages for more information on inviting guests.

Meet uses randomized meeting identifiers and dial-in details. It is not possible to customize external access identifiers to video meetings, so there is no need to randomize any addressing information.

Meet allows users to record meetings, which are then saved to the Drive of the meeting owner in MP4 format, as a regular file in Drive with all Drive controls available, including Vault policies. The recording is automatically shared with guests invited to the Calendar event.

Meet meetings allow users to share text-based chat messages with other participants during the call, which are preserved as a .txt file alongside the call recording.

Administrators are able to control whether users can record their meetings in the Admin console.

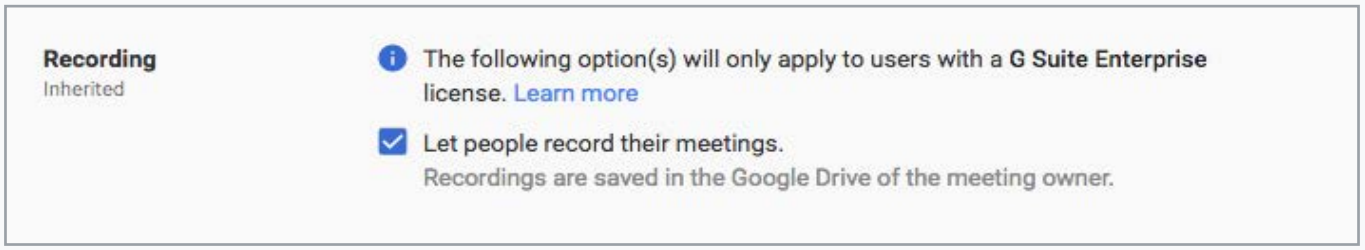
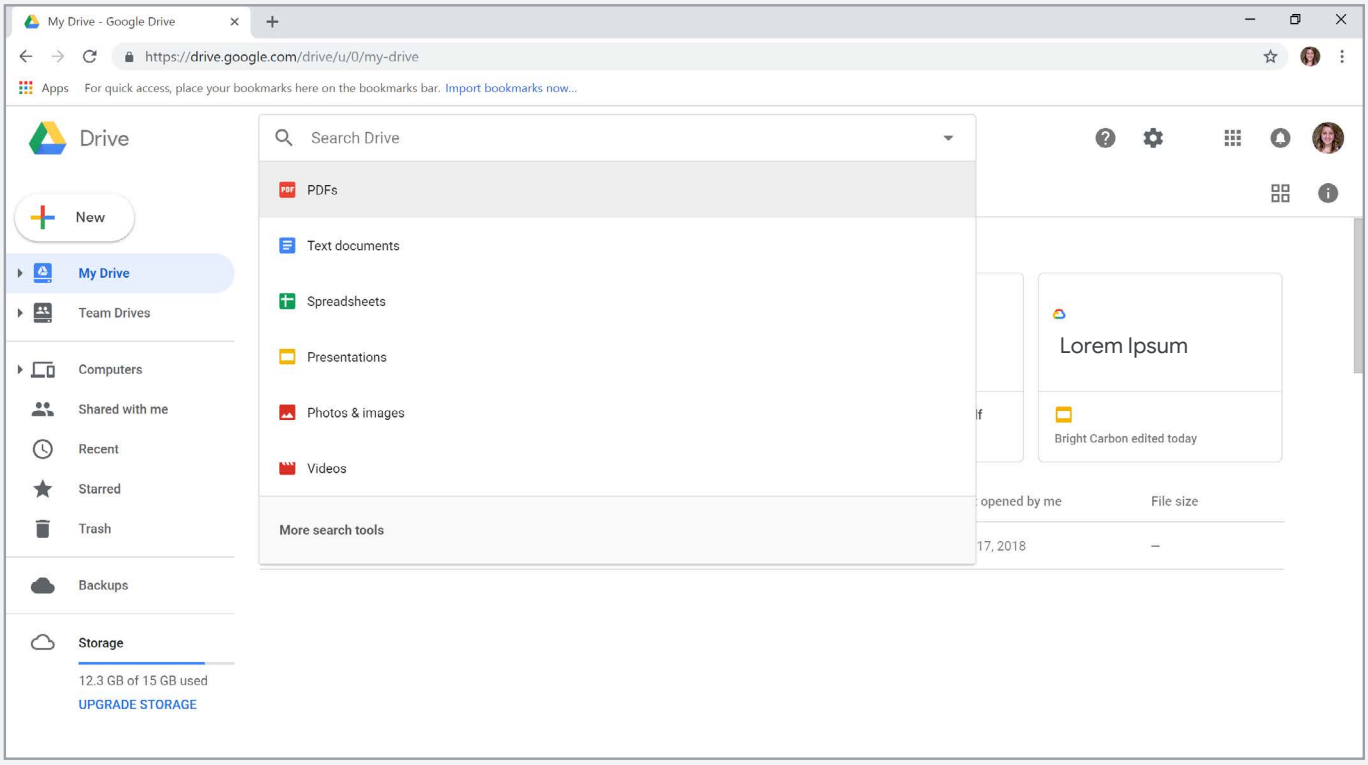


Exhibit C

Google Cloud Search

Administrators can control the use of search history with Google Cloud Search via the Web History service in the Admin console. Administrators can turn the web history service On or Off for everyone, or for specific organizational units. Users with Web History turned on will have their personal search history stored, and will benefit from better search results and suggestions. Search history is stored until deleted by a user at history.google.com.



For more information about Cloud Search, please see https://support.google.com/cloudsearch.

Google Groups for business

To help prevent data from being accidentally shared, by default Google Groups' sharing settings are set to best protect privacy:

- Viewing groups: By default, no one outside the domain can view or search groups in the domain.
- Posting to groups: By default, no one outside the domain can post to the groups.
- Joining groups: By default, no one outside the domain can become a group member.
- Creating groups: By default, only those within the domain can create groups.

Your administrator can adjust each of these default settings individually. They can review and update the sharing permissions for their domains from the Admin console, while end users can review and update Google Groups permissions in group settings.

Administrators should consider taking the following actions to help protect the privacy of data processed within Google Groups:

- Disable the ability for their users to create public Google Groups in the admin console. This will apply to all new groups.
- Change the privacy settings for Google Groups retroactively, via APIs or Groups UI.
- View and update Groups settings in bulk using the Directory API and Groups Settings API.

More information on this is available in the blog post here and also in our Help Center.

Google Cloud

Additional considerations

Turning Google Services on and off

Administrators can control which Google services are accessible by users by turning each service “On” or “Off” for those users in the Google Admin console as described here. When users sign in to their account, they’ll see only those services that are turned On for them.

In addition to G Suite and other Google products that your administrator can manage individually with an On or Off control in the Google Admin console, your administrator can manage access to unlisted Google services that don't have an individual control (such as Allo, Chromecast, and Google Surveys). Administrators might need to restrict users from accessing services with their managed Google Account for reasons such as adherence to company policies or compliance with data protection regulations. For details on how to turn these services On or Off, see manage services that aren't controlled individually.

G Suite services can be configured by your administrator to help ensure that your data is protected in accordance with your organization’s desired configuration.

Separating user access within the domain

To manage end user access to different sets of G Suite Services and Additional Products, your administrator can create organizational units to separate into different groups end users who manage personal/sensitive data and end users who do not. Once these units are set up, administrators can turn specific services/products On or Off for groups of users.

For example, the Human Resources department may manage personal/sensitive data, but only a subset of HR users may actually need access to this data. In that case, administrators are able to configure an HR organizational unit for users using G Suite Core Services with personal/sensitive data, with certain services disabled and settings configured appropriately.

To learn more, administrators can refer to our Support resources on how to set up organizational units and how to turn services on and off.

Use of third party applications

Some G Suite Core Services may make it possible for an end user to share personal/sensitive data with a third party (or a third party application). However, it is your organization's responsibility to ensure that appropriate, compliant measures are in place with any third party (or third party application) before sharing or transmitting personal/sensitive data. Your organization is responsible for determining whether any other data protection terms need to be in place before sharing personal/sensitive data with the third party using G Suite services, or applications that integrate with them. Your administrator can selectively whitelist third-party applications that can access API scopes across G Suite services.

To learn more, administrators can refer to our Support resources on how to control user installation of Marketplace apps.

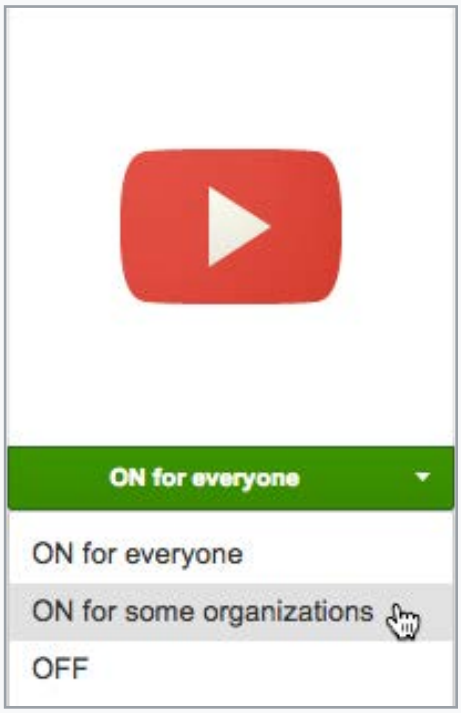


Exhibit B

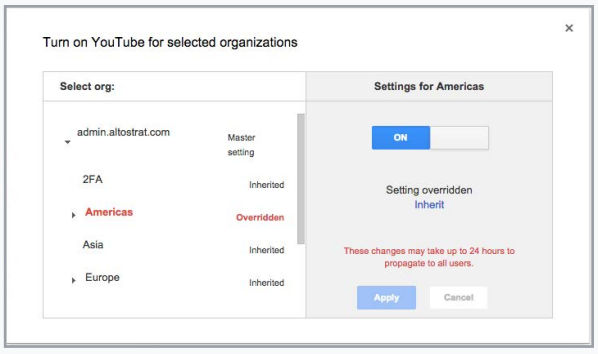
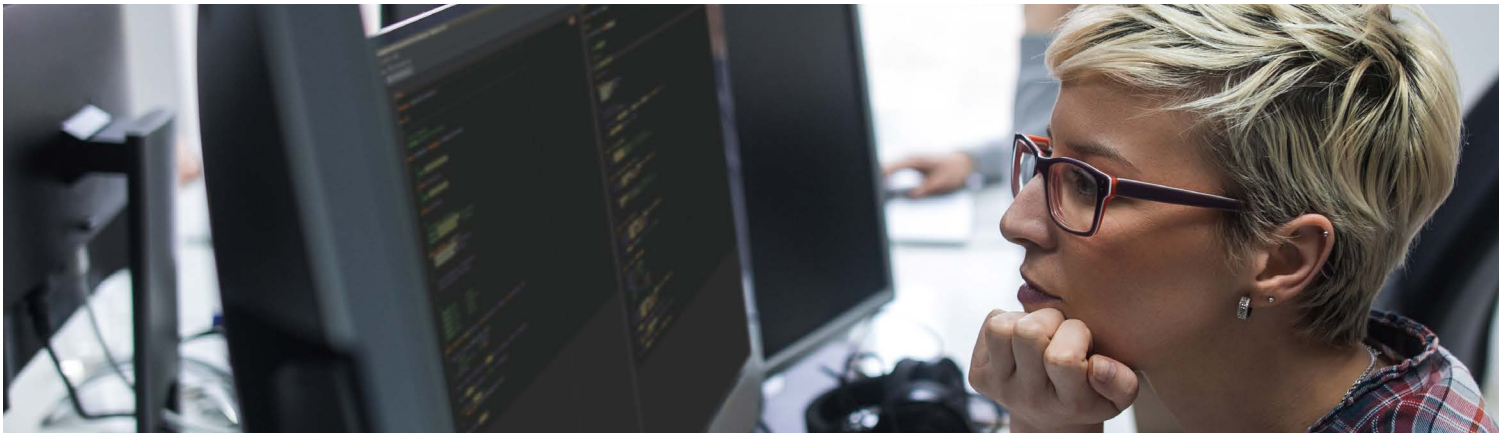


Exhibit C

Security Best Practices

To increase the safety and security of your organization's data, consider reviewing the recommendations provided by the security health tool. All organizations can see these security recommendations in the Help Center articles here.



Security Audits and Certifications

To help your organization with compliance and reporting, we share information and best practices and provide easy access to documentation. Our products regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards to earn your trust. A list of G Suite standards, regulations, and certifications can be found on our website here.

Additional resources

For more information on how G Suite services are designed with privacy, confidentiality, integrity, and availability of data in mind, see:

- Google Cloud Standards, Regulations & Certifications
- G Suite Security eBook
- G Suite Security page
- G Suite Help Center
- Google Cloud & the GDPR
- GDPR Resource Center
- G Suite Security & Compliance Whitepaper

Appendix: URLs

Page 3:

Data processing agreement: https://gsuite.google.com/terms/dpa_terms.html

G Suite Terms of service: https://gsuite.google.com/intl/en_uk/terms/2013/1/premier_terms.html

EMEA G Suite Terms of service: https://gsuite.google.com/terms/premier_terms_emea.html

EEA G Suite Terms of service: https://gsuite.google.com/terms/premier_terms_eea.html

Page 4:

Data Processing Amendment: https://gsuite.google.com/terms/user_features.html

G Suite Core Services: https://gsuite.google.com/terms/user_features.html

Accept the DPA: https://support.google.com/a/answer/2888485?hl=en

Watch the video: https://www.youtube.com/watch?v=EiepWDabaR4&feature=youtu.be&autoplay=1

“Other Services" for G Suite: https://gsuite.google.com/terms/user_features.html

Page 5:

Additional Products:https://support.google.com/a/answer/181865

The Terms of Service: https://support.google.com/a/answer/181865

Privacy Policy: https://policies.google.com/privacy

Page 7:

Configure notifications: https://support.google.com/a/answer/3230421?hl=en

Page 8:

Inserting files using Google Drive:

https://support.google.com/mail/answer/2487407?visit_id=636824802325449492-336116528&rd=1

Share only: https://support.google.com/mail/answer/2487407

Anyone with the link: https://support.google.com/drive/answer/2494822?visit_id=636824802325449492-336116528&rd=1

Share Google Drive files and folders: https://support.google.com/a/answer/60781

Page 9:

Shared calendars: https://support.google.com/calendar/answer/37082?visit_id=636824802325449492-336116528&rd=1

Set sharing options: https://support.google.com/a/answer/60765

Page 10:

Sharing files in Google Drive: https://support.google.com/drive/answer/2494822

Share Google Drive files and folders: https://support.google.com/a/answer/60781

Team Drives: https://support.google.com/a/answer/7212025

Page 11:

Google Drive apps: https://support.google.com/a/answer/7281227#scopes

Google Docs add-ons: https://support.google.com/a/answer/7281227#scopes

Page 12:

Sharing permissions: https://support.google.com/a/answer/60781

Page 14:

Giving limited editing access:

https://support.google.com/sites answer/97934?hl=en&ref_topic=6372882&visit_id=636685732143833599-1194629127&rd=1

Publishing: https://support.google.com/sites/answer/6372880?hl=en&ref_topic=6372882

Page 15:

Turn on the Jamboard service: https://support.google.com/jamboard/answer/7393321?hl=en&ref_topic=7389415

Page 16:

Sharing permissions: https://support.google.com/a/answer/60781

Working in a live Jam session: https://support.google.com/jamboard/answer/7384353?hl=en&ref_topic=7383644

Page 17:

More information: https://support.google.com/a/answer/60767?hl=en

Configure: https://support.google.com/a/answer/60767?hl=en

Page 19:

Inviting guests: https://support.google.com/a/answer/6097610

Page 21:

Web history service: https://support.google.com/a/answer/6304876?hl=en

Search history: https://myactivity.google.com/

Page 22:

Review and update sharing premission: https://support.google.com/a/answer/167097

Review and update Google Groups: https://support.google.com/groups/answer/2464975

Directory API: https://developers.google.com/admin-sdk/directory/v1/guides/manage-groups

Groups Settings API: https://developers.google.com/admin-sdk/groups-settings/manage

Blog post: https://gsuiteupdates.googleblog.com/2018/06/configure-your-google-groups-settings.html

Help Center: https://support.google.com/a/answer/167093?hl=en&ref_topic=14869

Page 23:

Admin console:

https://accounts.google.com/signin/v2/identifier?service=CPanel&passive=1209600&cpbps=1&continue=

https%3A%2F%2Fadmin.google.com%2FDashboard&followup=https%3A%2F%2Fadmin.google.

com%2FDashboard&skipvpage=true&flowName=GlifWebSignIn&flowEntry=ServiceLogin

Described here: https://support.google.com/a/answer/182442?hl=en

Manage services that aren't controlled individually: https://support.google.com/a/answer/7646040?hl=en

Page 24:

Support resources: https://support.google.com/a/answer/4352075

How to turn services on and off: https://support.google.com/a/answer/182442

Page 25:

Whitelist third-party applications: https://support.google.com/a/answer/7281227?hl=en

Page 26:

A list of G Suite standards etc: https://cloud.google.com/security/compliance/#/

Google Cloud Standards, Regulations & Certifications: https://cloud.google.com/security/compliance/#/

G Suite Security eBook: http://services.google.com/fh/files/misc/gsuite_security_and_trust_ebook.pdf

G Suite Security page: https://cloud.google.com/security/

G Suite Help Center: https://support.google.com/a/#topic=7570177

Google Cloud & the GDPR: https://cloud.google.com/security/gdpr/

GDPR Resource Center: https://cloud.google.com/security/gdpr/resource-center/

G Suite Security & Compliance Whitepaper:

https://static.googleusercontent.com/media/gsuite.google.com/en//files/google-apps-security-and-compliance

-whitepaper.pdf