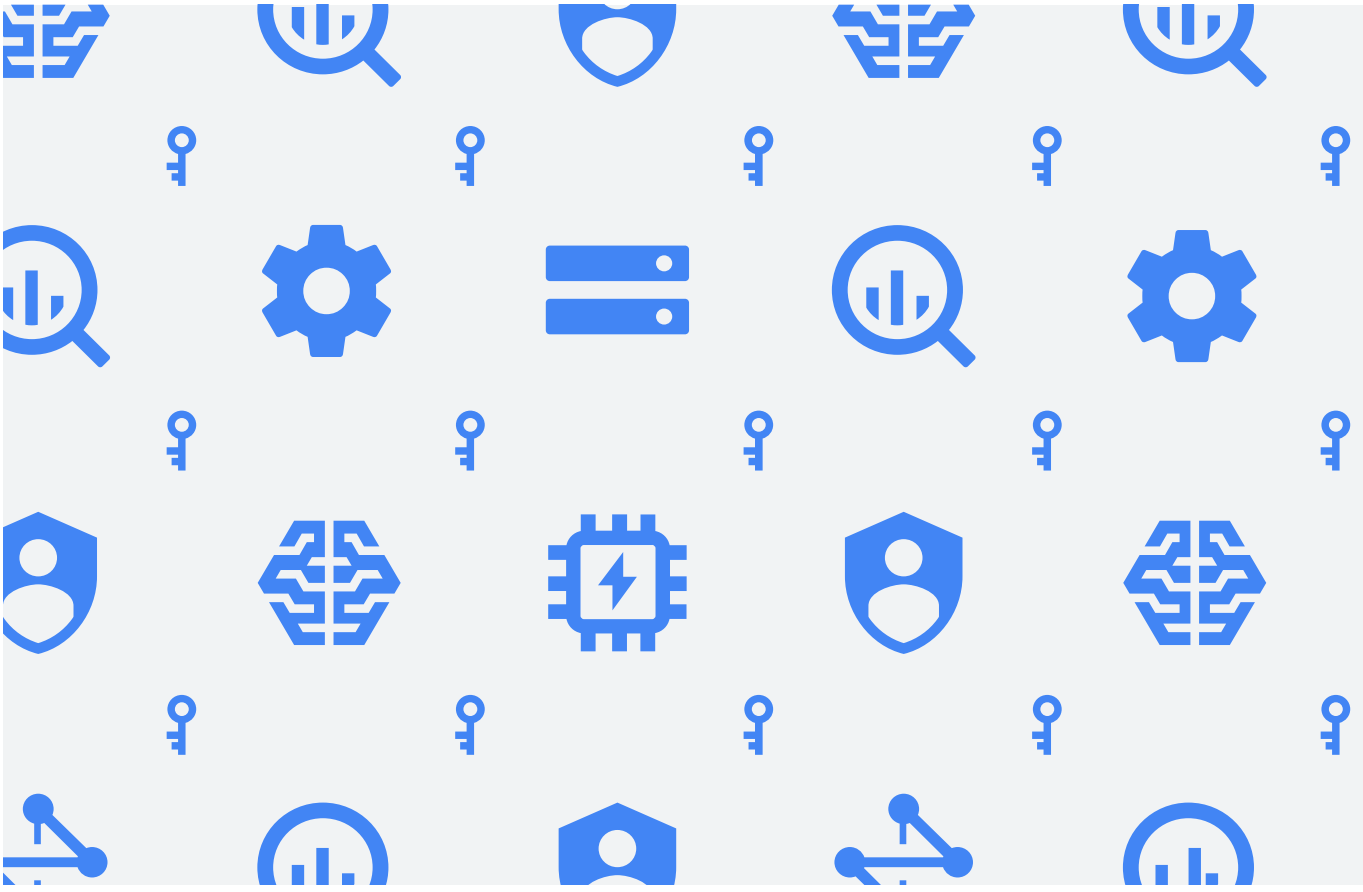
Google Cloud Whitepaper
May 2018

General Data Protection Regulation (GDPR)



Google Cloud

Introduction to the GDPR

On 25 May 2018, the most significant piece of European data protection legislation to be introduced in 20 years will come into force. The EU General Data Protection Regulation (GDPR) replaces the 1995 EU Data Protection Directive. The GDPR strengthens the rights that individuals have regarding personal data relating to them and seeks to unify data protection laws across Europe, regardless of where that data is processed.

You can count on the fact that Google is committed to GDPR compliance across Google Cloud services. We are also committed to helping our customers with their GDPR compliance journey by providing robust privacy and security protections built into our services and contracts over the years.

What can you do?

What are your responsibilities as a customer?

G Suite[1] and Google Cloud Platform customers will typically act as the data controller for any personal data they provide to Google in connection with their use of Google's services. The data controller determines the purposes and means of processing personal data, while the data processor processes data on behalf of the data controller. Google is a data processor and processes personal data on behalf of the data controller when the controller is using G Suite or Google Cloud Platform.

Data controllers are responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that any data processing is performed in compliance with the GDPR. Controllers' obligations relate to principles such as lawfulness, fairness and transparency, purpose limitation, data minimisation, and accuracy, as well as fulfilling data subjects' rights with respect to their data.

If you are a data controller, you may find guidance related to your responsibilities under GDPR by regularly checking the website of your national or lead data protection authority under the GDPR (as applicable)[2], as well as by reviewing publications by data privacy associations such as the International Association of Privacy Professionals (IAPP).

You should also seek independent legal advice relating to your status and obligations under the GDPR, as only a lawyer can provide you with legal advice specifcally tailored to your situation. Please bear in mind that nothing on this website is intended to provide you with, or should be used as a substitute for legal advice.

[1] G Suite includes G Suite for Business and G Suite for Education.

[2] We recommend you seek independent legal advice to determine your appropriate national or lead data protection authority.

Where should you start?

As a current or future customer of Google Cloud, now is a great time for you to begin preparing for the GDPR. Consider these tips:

- Familiarize yourself with the provisions of the GDPR, particularly how they may differ from your current data protection obligations.
- Consider creating an updated inventory of personal data that you handle. You can use some of our tools to help identify and classify data.
- Review your current controls, policies, and processes to assess whether they meet the requirements of the GDPR, and build a plan to address any gaps.
- Consider how you can leverage the existing data protection features on Google Cloud as part of your own regulatory compliance framework.
- Conduct a review of G Suite or Google Cloud Platform third-party audit and certification materials to see how they may help with this exercise.
- Monitor updated regulatory guidance as it becomes available, and consult a lawyer to obtain legal advice specifically applicable to your business circumstances.

What we do

G Suite & Google Cloud Platform commitments to the GDPR

Among other things, data controllers are required to only use data processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR. Here are some aspects you may want to consider when conducting your assessment of G Suite and Google Cloud Platform services.

Expert knowledge, reliability, and resources

Data protection expertise

Google employs security and privacy professionals that include some of the world's foremost experts in information, application, and network security. This team is tasked with maintaining the company's defense systems, developing security review processes, building security infrastructure, and implementing Google's security policies. Google also employs an extensive team of lawyers, regulatory compliance experts, and public policy specialists who look after privacy and security compliance for Google. These teams engage with customers, industry stakeholders, and supervisory authorities to shape our G Suite and Google Cloud Platform services in a manner that helps customers meet their compliance needs.

Data protection commitments

Data processing agreements

Our data processing agreements for G Suite and Google Cloud Platform clearly articulate our privacy commitments to customers. We have evolved these terms over the years based on feedback from our customers and regulators.

More recently, we have specifically updated these terms to reflect the GDPR, and have made these updated available well in advance of the entry into force of the GDPR to facilitate our customers' compliance assessment and GDPR readiness when using Google Cloud services. Our customers can enter into these updated data processing terms now via the opt in process described here for the G Suite Data Processing Amendment and here for the GCP Data Processing and Security Terms, and the updated terms will take effect from 25 May 2018, when the GDPR comes into force.

Processing according to instructions

Any data that a customer and its users put into our systems will only be processed in accordance with the customer's instructions, as described in our current as well as our GDPR-updated data processing agreements.

Personnel confidentiality commitments

All Google employees are required to sign a confidentiality agreement and complete mandatory confidentiality and privacy trainings, as well as our Code of Conduct training. Google's Code of Conduct specifically addresses responsibilities and expected behavior with respect to the protection of information.

Use of subprocessors

Google Group companies directly conduct the majority of data processing activities required to provide the G Suite and Google Cloud Platform services. However, we do engage some third-party vendors to assist in supporting these services. Each vendor goes through a rigorous selection process to ensure it has the required technical expertise and can deliver the appropriate level of security and privacy. We make information available about Google group subprocessors supporting G Suite and Google Cloud Platform services, as well as third-party subprocessors involved in those services, and we include commitments relating to subprocessors in our current and updated data processing agreements.

Security of the services

According to the GDPR, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Google operates global infrastructure designed to provide state-of-the-art security through the entire information processing lifecycle. This infrastructure is built to provide secure deployment of services, secure storage of data with end-user privacy safeguards, secure communications between services, secure and private communication with customers over the Internet, and safe operation by administrators. G Suite and Google Cloud Platform run on this infrastructure.

We designed the security of our infrastructure in layers that build upon one another, from the physical security of data centers, to the security protections of our hardware and software, to the processes we use to support operational security. This layered protection creates a strong security foundation for everything we do. A detailed discussion of our Infrastructure Security can be found in our Google Infrastructure Security Design Overview Whitepaper.

Availability, integrity, and resilience

Google designs the components of our platform to be highly redundant.Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products such as natural disasters and local outages. In the event of hardware, software, or network failure, services are automatically and instantly shifted from one facility to another so that operations can continue without interruption. Our highly redundant infrastructure helps customers protect themselves from data loss.

Testing

Google conducts disaster recovery testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses. All teams that participate in the disaster recovery exercise develop testing plans and post mortems which document the results and lessons learned from the tests.

Encryption

Google uses encryption to protect data in transit and at rest. Data in transit to G Suite is protected using HTTPS, which is activated by default for all users. G Suite and Google Cloud Platform services encrypt customer content stored at rest, without any action required from customers, using one or more encryption mechanisms. A detailed discussion of how we encrypt data can be found in our Encryption Whitepaper.

Access controls

For Google employees, access rights and levels are based on job function and role, using the concepts of least-privilege and need-to-know to match access privileges to denied responsibilities. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies.

Vulnerability management

We scan for software vulnerabilities using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration testing, quality assurance processes, software security reviews, and external audits. We also rely on the broader security research community and greatly value their help identifying vulnerabilities in G Suite, Google Cloud Platform, and other Google products. Our Vulnerability Reward Program encourages researchers to report design and implementation issues that may put customer data at risk.

Product security: G Suite

G Suite customers can leverage product features and configurations to further protect personal data against unauthorised or unlawful processing:

- 2-step verification greatly reduces the risk of unauthorized access by asking users for additional proof of identity when signing in. Security key enforcement offers another layer of security for user accounts by requiring a physical key.
- Suspicious Login Monitoring helps detect suspicious logins using robust machine learning capabilities.
- Enhanced email security requires email messages to be signed and encrypted using Secure/Multipurpose Internet Mail Extensions (S/MIME).
- Data loss prevention protects sensitive information within Gmail and Drive from unauthorized sharing. Learn more in our DLP Whitepaper.
- Information rights management in Drive allows you to disable downloading, printing, and copying of files from the advanced sharing menu, and to set expiration dates on file access.
- Mobile device management offers continuous system monitoring and alerts in case of suspicious device activity.

To learn more, please visit this website

Product security: GCP

GCP customers can leverage product features and configurations to further protect personal data against unauthorised or unlawful processing:

- 2 step verification greatly reduces the risk of unauthorised access by asking users for additional proof of identity when signing in. Security key enforcement offers another layer of security for user accounts by requiring a physical key.
- Google Cloud Identity and Access Management (Cloud IAM) allows you to create and manage fine- grained access and modification permissions for Google Cloud Platform resources.
- Data Loss Prevention API helps to identify and monitor the processing of special categories of personal data in order to implement adequate controls.
- Stackdriver Logging and Stackdriver Monitoring integrate logging, monitoring, alerting, and anomaly detection systems into Google Cloud Platform.
- Cloud Identity-Aware Proxy (Cloud IAP) controls access to cloud applications running on Google Cloud Platform.
- Cloud Security Scanner scans for and detects common vulnerabilities in Google App Engine applications.

To learn more, please visit this website

Data return & deletion

Administrators can export customer data, via the functionality of the G Suite or Google Cloud Platform services, at any time during the term of the agreement. We have included data export commitments in our data processing terms for several years, and we will continue offering those after the GDPR comes into force, and working to enhance the robustness of the data export capabilities of the G Suite services and each of the Google Cloud Platform services (consult the Google Cloud Platform documentation for further information).

You can also delete customer data, via the functionality of the G Suite or Google Cloud Platform services, at any time. When Google receives a complete deletion instruction from you (such as when an email you have deleted can no longer be recovered from your “trash”), Google will delete the relevant customer data from all of its systems within a maximum period of 180 days unless retention obligations apply.

Assistance to the controller

Data subject's rights

Data controllers can use the G Suite and Google Cloud Platform administrative consoles and services functionality to help access, rectify, restrict the processing of, or delete any data that they and their users put into our systems. This functionality will help them fulfill their obligations to respond to requests from data subjects to exercise their rights under the GDPR.

Data protection team

Our G Suite and Google Cloud Platform customers have a dedicated team where data protection related enquiries can be directed.

Notifications

G Suite and Google Cloud Platform have provided contractual commitments around incident notification for many years. We will continue to promptly inform you of incidents involving your customer data in line with the data incident terms in our current agreements and the updated terms that will apply from 25 May 2018, when the GDPR comes into force.

International data transfers

The GDPR provides for several mechanisms to facilitate transfers of personal data outside of the EU. These mechanisms are aimed at confirming an adequate level of protection or ensuring the implementation of appropriate safeguards when personal data is transferred to a third country.

Appropriate safeguards can be provided for by model contract clauses. An adequate level of protection can be confirmed by adequacy decisions such as the ones that supports the EU-U.S. Privacy Shields.

We contractually commit under our current data processing agreements to maintain a mechanism that facilitates transfers of personal data outside of the EU as required by the Data Protection Directive, and will offer a corresponding commitment from 25 May 2018, when the GDPR comes into force.

Google's certification under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks includes G Suite and Google Cloud Platform. We have also gained confirmation of compliance from European Data Protection Authorities for our model contract clauses, affirming that our current contractual commitments for G Suite and Google Cloud Platform fully meet the requirements under the Data Protection Directive to legally frame transfers of personal data from the EU to the rest of the world.

Standards and certifications

ISO 27001 (Information Security Management)

ISO 27001 is one of the most widely recognized, internationally accepted independent security standards. Google has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centers that make up our shared Common Infrastructure as well as for G Suite and Google Cloud Platform.

ISO 27017 (Cloud Security)

ISO 27017 is an international standard of practice for information security controls based on ISO/IEC 27002, specifically for Cloud Services. Google has been certified compliant with ISO 27017 for G Suite and Google Cloud Platform.

ISO 27018 (Cloud Privacy)

ISO 27018 is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Google has been certified compliant with ISO 27018 for G Suite and Google Cloud Platform.

SSAE16 / ISAE 3402 (SOC 2/3)

The American Institute of Certified Public Accountants (AICPA) SOC 2 (Service Organization Controls) and SOC 3 audit framework defines Trust Principles and criteria for security, availability, processing integrity, and confidentiality. Google has both SOC 2 and SOC 3 reports for Google Cloud Platform and G Suite.

Frequently asked questions

1 What is the GDPR?

The General Data Protection Regulation is a new EU privacy legislation that will replace the 95/46/EC Directive on Data Protection of 24 October 1995.

2 When will the GDPR take effect?

The GDPR will be directly applicable in all European Union Member States starting from 25 May 2018.

3 Does the GDPR require storage of personal data in the EU?

No. Like the 95/46/EC Directive on Data Protection, the GDPR sets forth certain conditions for the transfer of personal data outside the EU. Such conditions can be met via mechanisms such as model contract clauses.

4 Will the GDPR give customers the right to audit Google Cloud?

Under the GDPR, audit rights must be granted to data controllers in their contracts with data processors. The updated data processing agreements we will offer from 25 May 2018, when the GDPR comes into force, therefore include audit rights for the benefit of our customers.

5 What role do third-party ISO 27001, ISO 27017, ISO 27018, and SOC 2/3 reports play in compliance with the GDPR?

Our third-party ISO certifications and SOC 2/3 audit reports can be used by customers to help conduct their risk assessments and help them determine whether appropriate technical and organisational measures are in place.

6 What other information has Google provided on the GDPR?

Refer to Google's Businesses and Data website.