Google Cloud

Quick Reference Guide:

Google Cloud & the General Data Protection Regulation (GDPR)

The GDPR is a top priority for Google Cloud and our customers. At its core, the GDPR intends to strengthen the rights of European Union (EU) residents over their personal data. If you are a business established in the EU, or established outside of the EU but offer goods or services to data subjects who are in the EU, it is highly likely that the GDPR will apply to you. We've made multiple updates to ensure that Google Cloud customers can confidently use our services when the GDPR takes effect.

Complying with the GDPR may require changes across your business. Here are some key actions you should consider:

- Ensure your business is educated on GDPR compliance requirements. Appoint a Data Protection Officer (where required) to manage your GDPR compliance strategy
- Know the data in your systems. Identify and classify your data
- Compare your current controls, policies, and processes for managing and protecting data with the GDPR's requirements. Find the gaps and create a plan to address them
- Make sure your privacy policy, disclosures, and security and consent mechanisms are clear and documented

When using a processor like Google Cloud, complying with the GDPR will be a collaborative effort. Partner with Google Cloud and we will support your efforts by:

- Committing in our contracts to comply with the GDPR in relation to our processing of customer data in all Google Cloud Platform and G Suite services when the GDPR comes into effect on May 25, 2018
- Offering additional security features that may help you to better protect your most sensitive personal data
- Giving you what's needed to perform a meaningful privacy assessment of our services with documentation and reporting requirements
- Continuing to evolve our capabilities as the regulatory landscape changes

Terms

Our updated GCP Data Processing and Security Terms and G Suite[1] Data Processing Agreement reflect our responsibilities as a data processor to you under the GDPR.

Our model contract clauses have been confirmed by European Data Protection Authorities to meet the requirements to legally frame transfers of data from the EU to the rest of the world.

Security & privacy certifications

Our third party audits and certifications demonstrate our commitment to implementing the technical and organizational measures designed to meet the requirements of the GDPR and industry standards.

Privacy Shield	ISO 27001 ISO 27017 ISO 27018	SOC 2 SOC 3

GDPR at a glance

- Regulates how businesses can collect, use, and store personal data
- Builds upon current documentation and reporting requirements to increase accountability
- Authorizes fines on businesses who fail to meet its requirements

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

Google Cloud

Product & feature guide

Google Cloud offers data privacy, data portability, and threat protection products and features that can support your GDPR compliance efforts. These can be leveraged to prevent abuse or unlawful access to your data, and maintain the ongoing confidentiality, integrity, and availability of your data, as may be required to meet the requirements of the GDPR.

G Suite

- 2-Step Verification 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 detects suspicious logins using robust machine learning capabilities.
- Data loss prevention protects sensitive information within Gmail and Drive from unauthorized sharing.
- Enhanced Email Security requires email messages to be signed and encrypted using Secure/Multipurpose Internet Mail Extensions (S/MIME).
- Information Rights Management in Drive allows you to disable downloading, printing, and copying of files from the advanced sharing menu.
- Security Center provides you with visibility into external file sharing, spam and malware targeting users within your organization, and metrics to demonstrate your security effectiveness in a single, comprehensive dashboard.

Google Cloud Platform

- 2-Step Verification 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.
- Google Cloud Identity and Access Management (Cloud IAM) allows you to control access rights and roles for Google Cloud Platform resources. For cloud applications running on Google Cloud Platform, Cloud Identity-Aware Proxy (Cloud IAP) does this by verifying a user's identity.
- Access Transparency gives you near real-time logs when Google Cloud Platform administrators access your content.
- Data Loss Prevention API provides sensitive data classification, discovery, monitoring, and de-identification to help meet the principles of data protection by design and by default.
- Stackdriver Logging and Stackdriver Monitoring integrate logging, monitoring, alerting, and anomaly detection systems into Google Cloud Platform.
- Cloud Security Scanner scans and detects for common vulnerabilities in Google App Engine applications to prevent potential threats.
- Cloud Security Command Center allows you to view and monitor an inventory of your cloud assets, scan storage systems for sensitive data, detect common web vulnerabilities, and review access rights to your critical resources, all from a single, centralized dashboard.

If you have additional questions regarding Google Cloud & GDPR, or want to check out our GDPR Whitepaper, visit https://cloud.google.com/security/gdpr/.