Google Whitepaper
September 2023

Google Cloud & Federal Act on Data Protection (Revision)

Google Cloud

Table of contents

Disclaimer

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

Introduction

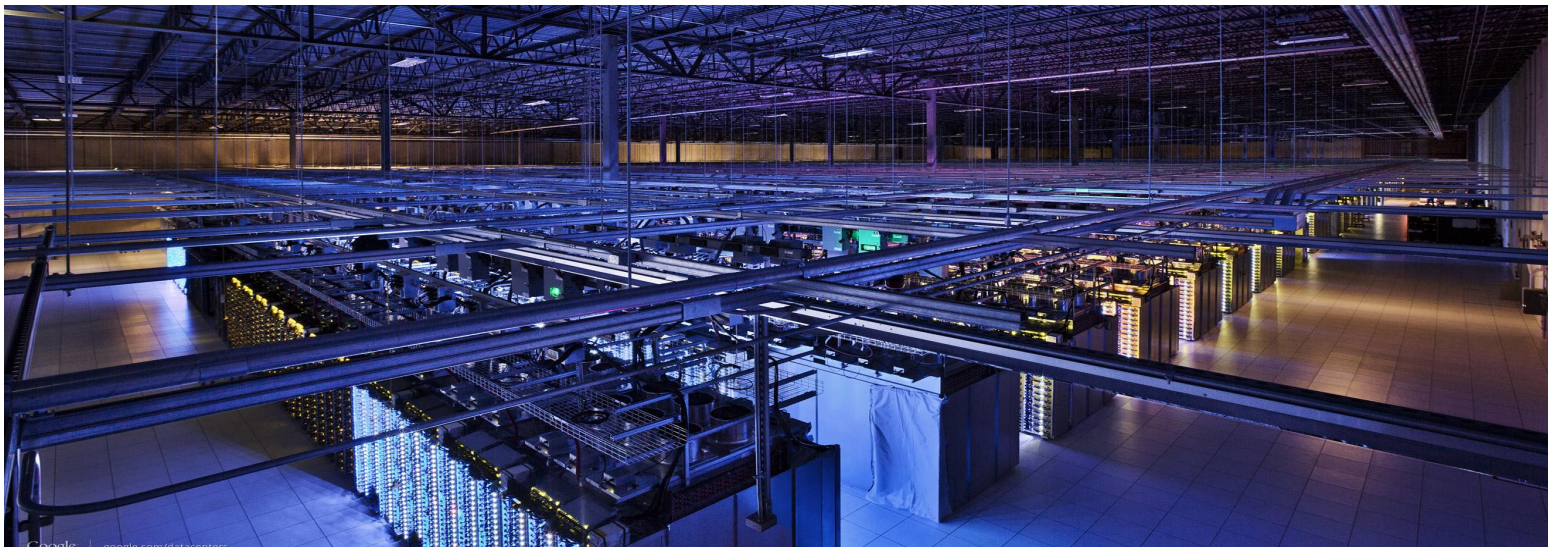
Switzerland is implementing the **Revised Federal Act on Data Protection** (revFADP) to better protect its citizens' data. Swiss based companies will have to comply with this legislation from September 1, 2023.

The revFADP aims to protect the personal rights and the fundamental rights of natural persons whose personal data is processed. Since Switzerland is not a member state of the European Union or the European Economic Area, and thus did not already implement the principles of the General Data Protection Regulation (GDPR), it seeks to align the current Swiss Federal Act on Data ProtectionData Protection Act with the Council of Europe's Convention 108, and with the General Data Protection Regulation (GDPR). An adequate level of privacy is also important in view of the pending adequacy finding by the EU Commission.

The revFADP applies to the processing of personal data pertaining to natural persons by private persons and federal bodies. In contrast to the current law, personal data of legal persons is no longer protected under the revFADP.

The revFADP sets out an updated set of data protection principles. These principles for the processing of personal data laid out in Art. 6 revFADP form its main body. These include the principles of lawfulness, good faith, transparency and correctness, as well as the processing in a proportional manner for a defined purpose and the storage limitation.

Google is committed to revFADP compliance for our Google Cloud services where applicable. We are also committed to helping our customers with their revFADP compliance journeys by providing robust privacy and security protections built into our services and contracts.



What you can do

What are the specific roles of the parties?

Google Workspace[1] and Google Cloud customers will act mainly as the data controller for any personal data they provide to Google in connection with their use of Google's services.
Like in the GDPR[2], the data controller determines the purposes and means of processing personal data, while the data processor processes data on behalf of the data controller.

Data controllers and processors are responsible for implementing appropriate technical and organizational measures to ensure and demonstrate that any data processing is performed in compliance with the revFADP. Controllers' obligations relate to principles such as lawfulness, good faith and transparency, purpose limitation, storage limitation, and correctness, as well as fulfilling data subjects' rights with respect to their data.

Where processing is to be carried out on behalf of a controller, both parties shall enter into a data processing agreement. The controller shall ensure in particular that the processor is able to guarantee data security, data protection compliance and shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures as well as implement the security of the personal data that appropriately addresses the risk in such a manner that processing will meet the requirements of the revFADP. Google is committed to providing you with sufficient guarantees to protect your personal data. The Federal Council will issue provisions on the minimum requirements for data security.

The processor's obligation is to receive prior authorisation in case the processor assigns the processing to a third party. Google may only assign the processing to a third party with the prior authorisation to the controller.

If you are a data controller, you may find guidance related to your responsibilities under revFADP by regularly checking the website of the Federal Data Protection and Information Commissioner (FDPIC)[3], as well as consulting a lawyer should you need legal advice.

Where are you in your revFADP compliance journey?

As a current or future customer of Google Cloud, you may want to regularly assess compliance with the revFADP. Consider these tips:

---

[1] For the purposes of this whitepaper, Google Workspace includes Google Workspace for Education.
[2] GDPR and Google Cloud.
[3] We recommend you seek independent legal advice to determine your appropriate national or lead data protection authority.

- Conduct a gap analysis by reviewing your current controls, policies, and processes to assess whether they meet the requirements of the revFADP, and create a roadmap to address any gaps
- In case you have already implemented the GDPR successfully, please assess your revFADP compliance by evaluating the differences between the GDPR and the revFADP
- Continue updating your inventory and classifying data
- 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 Google Workspace or Google Cloud 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're doing

Google Workspace & Google Cloud commitments to the revFADP

Data controllers are required to only use data processors that provide sufficient guarantees to implement appropriate technical and organizational measures to meet the requirements of the revFADP. Here are some resources you may want to consider when conducting your assessment of Google Workspace and Google Cloud services.

Enterprise Privacy Commitments	**Our Privacy Commitments** Google makes the Google Cloud Enterprise Privacy Commitments for Google Workspace and Google Cloud products to describe our overarching responsibility to protect your business when you use our enterprise solutions. • **You control your data** - Customer data is only processed according to your agreement(s). • **We never use your data for ads targeting** - We do not process your customer data or service data to create ads profiles or to improve Google Ads products. • **We are transparent about data collection and use** - We are committed to transparency, compliance with regulations like the GDPR, and privacy best practices. • **We never sell customer data or service data** - We never sell customer data or service data to third parties. • **Security and privacy are primary design criteria for all of our products** - We build the strongest security technologies into our products. We prioritize the privacy of our customers by protecting the data you trust us with.

	These privacy commitments are backed by the strong contractual privacy commitments we make available to you for Google Workspace, Google Workspace for Education, and for Google Cloud Platform. Plus please refer to the Google Cloud Privacy Notice. See the following documents to dig deeper into Google's enterprise privacy, trust, and commitments. • our Google Cloud Trust whitepaper • our Google Workspace Trust whitepaper • our Google Workspace Data Subject Requests guide • our Google Cloud European Commitments whitepaper
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. These individuals are 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 Google Workspace and Google Cloud services in a manner that helps customers meet their compliance needs.
Data Protection Commitments	**Data Processing Agreements** Our Cloud Data Processing Addendum for Google Workspace and Google Cloud services clearly articulates our privacy and security commitment to customers. We have evolved these terms over the years based on feedback from our customers and regulators. We specifically updated these terms to reflect the revFADP and have made these updates available: • for Google Cloud and Google Workspace Cloud Data Processing Addendum including the EU Standard Contractual Clauses (with the relevant Swiss Annex IV) Our customers automatically enter into these terms.

	Processing According to Instructions Any Customer Data that a customer and its users put into our systems will only be processed in accordance with the customer's instructions. **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 Google Workspace and Google Cloud services. However, we do engage subprocessors 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 Google Workspace 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. Customers can find a list of our Google group and third party subprocessors documented for Google Cloud Platform and for Google Workspace.
Security of the Services	According to the revFADP, the controller shall implement **appropriate technical and organizational measures** to ensure a level of security appropriate to the risk and ensure in particular that the processor is able to guarantee data security. 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. Google Workspace and Google Cloud 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. Cloud 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. To learn more about our infrastructure, refer to the Google Workspace security whitepaper and Google security whitepaper.

Storage Media Security
Google utilizes barcodes and asset tags to track the status and location of data center equipment from acquisition to installation, retirement, and destruction. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google hard drives leverage technologies, such as Full Disk Encryption (FDE) and drive locking, to protect data at rest. Personable Identifiable Information (PII) on removable media leaving Google facilities is approved and encrypted. To learn more about our storage media security, refer to the Google Workspace security whitepaper and Google security whitepaper

Disaster Recovery 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 Google Workspace is protected using HTTPS, which is activated by default for all users. Google Workspace and Google Cloud 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 whitepapers for data-at-rest and data-in-transit. In addition to encrypting data-at-rest and data-in-transit, customers can now take advantage of Google's industry-leading Confidential Computing (Preview) suite of encryption-in-use capabilities on Compute Engine Confidential VMs and Confidential GKE Nodes.

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 defined 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. Data centers that house Google Cloud systems and infrastructure components are subject to physical access restrictions and equipped with 24 x 7 on-site security personnel, security guards, access badges, biometric identification mechanisms, physical locks and video cameras to monitor the interior and exterior of the facility. More information on our access control processes can be found in our Google security whitepaper.

Incident Management
Google has established a dedicated security team responsible for security and privacy of customer data and managing security 24 hours a day and 7 days a week worldwide. Individuals from this team receive incident-related notifications and are responsible for helping resolve emergencies 24 x 7. Incident response policies are in place and procedures for resolving critical incidents are documented. Information from these events are used to prevent future incidents and can be used as examples for information security training.
Google incident management processes and response workflows are documented. Google's incident management processes are tested on a regular basis as part of our ISO-27017, ISO-27018, ISO-27001, PCI-DSS, SOC 2 and

FedRAMP programs to provide our customers and regulators with independent verification of our security, privacy, and compliance controls. More information can be found in our Whitepaper on Data incident response process.

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 Google Workspace, Google Cloud, 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: Google Workspace
Google Workspace customers can leverage product features and configurations to further protect personal data against unauthorized or unlawful processing:

- Google Workspace Core Services, including Gmail, Google Admin Console, Calendar, Drive, Docs, Keep, Sites, Jamboard, Hangouts, Chat, Meet, Cloud Search and Google Groups offer configurable settings to help ensure that your organization's data is secured, used, and accessed according to your unique requirements.
- 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 https://workspace.google.com/security/.

Product Security: Google Cloud
Google Cloud customers can leverage product features and configurations to further protect personal data against unauthorized 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.
- Google Cloud Identity and Access Management (Cloud IAM) allows you to create and manage fine-grained access and modification permissions for Google Cloud resources.
- Data Loss Prevention API helps to identify and monitor the processing of special categories of personal data in order to implement adequate controls.
- Cloud Logging and Cloud Monitoring integrate logging, monitoring, alerting, and anomaly detection systems into Google Cloud.
- Cloud Identity-Aware Proxy (Cloud IAP) controls access to cloud applications running on Google Cloud.
- Cloud Security Scanner scans for and detects common vulnerabilities in Google App Engine applications.
- VPC Service Controls provide perimeter protection for services that store highly sensitive data to enable service-level data segmentation.
- Cloud KMS and HSM allow for management of encryption keys and cryptographic operations from within a cluster of FIPS 140-2 Level 3 certified Hardware Security Modules (HSMs). KMS allows customers to use Google-managed or customer-managed encryption keys as required to fulfill compliance requirements.
- Cloud Security Command Center allows customers 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 from a single, centralized dashboard.

To learn more, please visit https://cloud.google.com/security/.

Data Return & Deletion	Administrators can export customer data via the functionality of Google Workspace and Google Cloud 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 to enhance the robustness of the data export capabilities. Google Workspace admins can also use Google Vault for targeted user-based searches and export. You can also delete customer data, via the functionality of the Google Workspace or Google Cloud 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 Google Workspace and Google Cloud administrative consoles and services functionality to help access, rectify, restrict the processing of, or delete 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 revFADP. Data subjects (users) can also use the Google Takeout interface to directly access and export customer personal data by themselves. For instructions, see the Google Workspace Data Subject Requests Guide. **Data Protection Team** Our Google Workspace and Google Cloud customers have a dedicated team where data protection related enquiries can be directed. Where required, Google enterprise products have designated teams to address customer inquiries in relation to data protection. The way to contact these teams is described in the relevant agreement. For Google Workspace the Cloud Data Protection Team can be contacted by Customer's administrators at this contact page (while administrators are signed in to their admin account) and/ or directly by providing a notice to Google as described in the applicable agreement. For Google Cloud, the Cloud Data Protection Team can be contacted at this contact page.

	Incident Notifications Google Workspace and Google Cloud 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. Please review our data incident response process for more information.
International Data Transfers	The revFADP provides for several mechanisms to facilitate transfers of personal data outside of Switzerland. 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 for data transfers to a third country with Google can be provided by standard contractual clauses plus supplementary measures. More information on how Google supports you with appropriate safeguards can be found in the Safeguards for international data transfers with Google whitepaper.
Standards & Certifications	Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google Workspace and Google Cloud undergo several independent third-party audits on a regular basis to provide this assurance. **ISO/IEC 27701 (Privacy Information Management)** ISO 27701 is an international data privacy standard that is an extension of the ISO 27001 standard, with an emphasis on the creation of a Privacy Information Management System (PIMS). Google Cloud and Google Workspace have received an accredited ISO/IEC 27701 certification as a PII processor after undergoing an audit by an independent third party. Google Cloud and Google Workspace ISO 27701 certificates may be requested via the Compliance Reports Manager. **ISO/IEC 27001 (Information Security Management)** ISO 27001 is one of the most widely recognized, internationally accepted independent security standards. Google Cloud, our Common Infrastructure, and Google Workspace are certified as ISO/IEC 27001 compliant. Google Cloud and Google Workspace ISO/IEC 27001 certificates may be requested via the Compliance Reports Manager.

ISO/IEC 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 Cloud and Google Workspace are certified as ISO/IEC 27017 compliant. Google Cloud and Google Workspace ISO 27017 certificates may be requested via the Compliance Reports Manager.

ISO/IEC 27018 (Cloud Privacy)
ISO 27018 is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Google Cloud and Google Workspace are certified as ISO/IEC 27018 compliant. Google Cloud and Google Workspace ISO 27018 certificates may be requested via the Compliance Reports Manager.

SSAE 16/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 and Google Workspace. These reports can be requested via the Compliance Reports Manager.

FAQs

What is the Federal Act on Data Protection (Revision)?

The Revision of the Federal Act on Data Protection is a Swiss privacy legislation that will replace the Federal Act on Data Protection of 19 June 1992 on 1st September 2023.

In what contexts does the regulation apply?

The revFADP is applicable to circumstances that have an effect in Switzerland and abroad. The revFADP also applies to the processing of personal data by an establishment who is a controller or processor in Switzerland. In addition, the revFADP applies to the processing of personal data of data subjects who are in Switzerland by a controller or processor not established in Switzerland, where the processing activities are related to:

- A subject with their ordinary residence in Switzerland; or
- Through a Swiss establishment.

What are the main changes?

- Only data of natural persons are now covered.
- The revised Federal Act on Data Protection expands the list of data that fall under the category of sensitive personal data. Genetic and biometric data fall under the definition of sensitive data.
- The principles of "Privacy by Design" and "Privacy by Default" are introduced in the revised Federal Act on Data Protection.
- It is mandatory to keep and maintain a register of processing activities. However, the ordinance allows exemptions for SMEs whose data processing activities present limited risk to the data subjects.
- A Notification to the Federal Data Protection and Information Commissioner (FDPIC) is required in the event of a data breach.
- The concept of profiling is now a part of the revFADP.

Does the revFADP require storage of personal data in Switzerland?

No. Like the Federal Act on Data Protection of 19 June 1992, the revFADP sets forth certain conditions for the cross-border disclosure of personal data outside of Switzerland. Where personal data is disclosed to a country with adequate protection, no further safeguards are needed. Where personal data is disclosed to a country without adequate protection, safeguards must be implemented by data protection provisions in a contract between the controller or processor or processor-processor relationship, by an international treaty or by standard data protection clauses previously approved, established or recognized by the FDPIC.

If personal data is disclosed abroad, the controller must also inform the data subject of the identity of the state or international body to whom the disclosure was made and the implemented safeguards.

What are the key differences between the revFADP and the GDPR

Profiling is partially stricter than the requirements in the GDPR. Besides the profiling, the “high-risk” profiling has been introduced in the revFADP. “High-risk” profiling means a combination of different data sets to assess essential aspects of the data subject's personality.

In case the controller conducts a high risk profiling, he must carry out a Data Protection Impact Assessment, appoint a Swiss representative, inform the data subject about the profiling and where required must receive explicit consent from the data subject.

The revFADP does not go as far as the GDPR concerning the requirements for lawful consent. Consent is for example less strictly regulated than the GDPR does. In general, consent is not required, but the controller/processor needs to abide by the data processing principles. However, there are exceptions.

Explicit consent is required when it comes to the transfer of personal data to a country without an adequate level of protection and without an alternative legal basis which justifies the transfer.

Also, the duty of information in the case of an automated individual decision shall not apply in case the data subject explicitly consented to the decision being taken in an automated manner. Personal data on the data subject's health may be communicated to the data subject, provided consent is given, by a healthcare professional dedicated to the data subject.

Important: The Opt-out approach is valid under the revFADP.

What tools and features does Google offer me to help find my sensitive personal data?

Google Cloud and Google Workspace provide our customers with a suite of tools that help customers identify sensitive information on an ongoing basis. These tools include:

- Sensitive Data Protection helps you discover, classify, and de-identify sensitive data inside and outside Google Cloud. This Sensitive Data Protection overview describes the services that make up Sensitive Data Protection.
- **Cloud DLP API** offers off the shelf as well as custom Data Loss Prevention rules, and classification, masking, tokenization, and transformation capabilities designed to help your organizations discover, classify, and protect your most sensitive data on Google Cloud.
- **DLP rules for Drive** helps you protect sensitive information within Gmail and Drive from unauthorized sharing. Learn more in our DLP Whitepaper.
- **Cloud Security Command Center** allows customers 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 from a single, centralized dashboard.
- **Cloud Logging** and **Cloud Monitoring** integrate logging, monitoring, alerting, and anomaly detection systems into Google Cloud.

What role do third-party CSA STAR, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701 and SOC 2/3 reports play in compliance with the revFADP?

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. Our ISO/IEC 27701 certification provides greater clarity on privacy-related roles and responsibilities, which can facilitate efforts to comply with privacy regulations, including the revFADP. Please find more helpful information in the Compliance reports manager.

Google's CSA self assessment can help your assessment of our services, particularly as it relates to Article 9 para 2 of the revFADP. Article 9 para 2 of the revFADP obliges the controller that he must ensure in particular that the processor is able to guarantee data security. Cloud service providers can't

provide formal certification of our customers' compliance with revFADP. However, we try to ease the compliance process for your organization as much as possible via our products, technical capabilities, guidance documents and legal commitments.

On May 19th 2021, the European Data Protection Board (EDPB) approved the EU Cloud Code of Conduct (CoC), a mechanism for cloud providers to demonstrate how they offer sufficient guarantees to implement appropriate technical and organizational measures as data processors under the GDPR.

Google Cloud and Google Workspace have received provisional adherence (Level 2 of Compliance) to the EU Cloud Code of Conduct.

What other information has Google provided on European Data Protection Law?

Refer to the Compliance page in Google's Business Data Responsibility website and our GDPR resource center.

Please also refer to our Data Protection Impact Assessment (DPIA) resource center for more helpful information on the DPIA requirements.