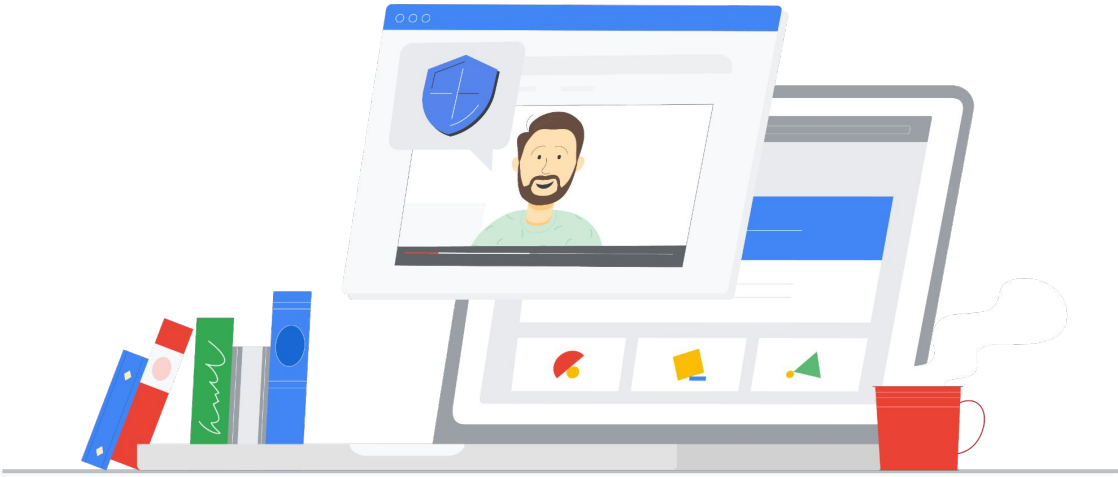
Google for Education

Safeguards for international data transfers with Google Workspace and Workspace for Education

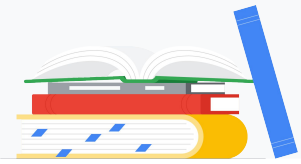


Disclaimer

The content contained herein is correct as of August 2021, and represents the status quo as of the time it was written. Google Cloud's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

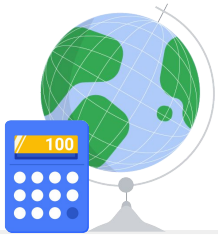
This whitepaper explains some of the safeguards and supplementary commitments that Google Cloud offers to protect and enhance your[1] control of your customer data in Google Workspace and Google Workspace for Education.



We are providing this information to assist you with any assessment of Google Cloud data transfers you may need to complete in light of the European Data Protection Board (EDPB) Recommendations on Supplementary Measures issued following the Court of Justice of the European Union's (CJEU) ruling known as Schrems II. We have also included information about United States laws to aid you with any such assessment.

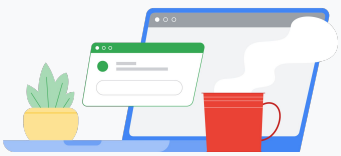
The CJEU's Schrems II ruling invalidated the European Commission's Decision underlying the EU-U.S. Privacy Shield Framework but did not invalidate EU Standard Contractual Clauses (SCCs, also known as Model Contractual Clauses), a mechanism by which personal data can be transferred to so-called "third countries"outside of the EEA[2] in compliance with the strict requirements imposed by EU data protection law regarding international data transfers.

1. In this whitepaper, "You/your" refers to Google Workspace for Education / Google Workspace customers
2. Equivalent mechanisms exist under the UK GDPR and the Swiss Federal Data Protection Act for transfers to third countries outside the UK and Switzerland respectively.



In the Schrems II case, the CJEU ruled that anyone transferring (i.e. exporting) personal data out of the EU to a third country (i.e. the country of import) in reliance on SCCs should assess whether that third country provides protection essentially equivalent to that guaranteed by EU law in order to determine whether the SCCs can ensure an adequate level of protection in practice. In other words, in order to transfer personal data based on SCCs, the data exporter and importer should assess whether the laws in the relevant third country provide the adequate level of protection otherwise provided by the SCCs. Although it is uncertain whether in specific circumstances SCCs alone will ensure the protection required by EU law, the CJEU indicated that "supplementary measures", when used with SCCs, could establish an adequate level of protection.

The EDPB's Recommendations on Supplementary Measures align with our long standing practices and we are glad to reaffirm our commitment to continue to invest in critical areas and to help Google Cloud customers protect their data and navigate their compliance journey when using our services and in light of the EDPB's Recommendations. Our customers own their data and we believe they should have the strongest levels of control over data stored in the cloud. Our public cloud empowers customers with world-class levels of visibility and control over their data through our services. This includes thorough technical safeguards and other offerings, such as the ability to store certain data in the European region and manage access to content, encryption keys, and transparency to actions taken by Google staff, to name a few.



This whitepaper provides information on the tools and resources offered by Google Cloud to help Google Cloud customers assess their compliance needs related to transfers of their EU personal data. However, please note that, as a provider of cloud services, we are not in a position to provide our customers with legal advice - this is something only legal counsel can provide.

1 Technical safeguards

Encrypting data in transit and at rest

Encryption is an important piece of the Google Workspace for Education / Google Workspace security strategy, helping to protect your emails, chats, video meetings, files, and other data. First, we encrypt certain data as described in our Google Workspace Encryption whitepaper while it is stored "at rest" — stored on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys. Second, we encrypt all customer data while it is "in transit" — traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data. We'll take a detailed look at how we encrypt data stored at rest and data in transit below.

Google has led the industry in using Transport Layer Security (TLS) for email routing, which allows Google and non-Google servers to communicate in an encrypted manner. When you send email from Google to a non-Google server that supports TLS, the traffic will be encrypted, preventing passive eavesdropping.

We believe increased adoption of TLS is so important for the industry that we report TLS progress in our Email Encryption Transparency Report. We also improved email security in transit by developing and supporting the MTA-STS standard allowing receiving domains to require transport confidentiality and integrity protection for emails.

Google Workspace customers also have the extra ability to only permit email to be transmitted to specific domains and email addresses if those domains and addresses are covered by TLS. This can be managed through the TLS compliance setting.

For further information on encryption, please see our Google Workspace Encryption whitepaper.

Access control

Google Workspace / Google Workspace for Education has implemented several types of controls designed to ensure that each of the data access pathways functions as intended:

1. Client Side Encryption

We're taking encryption a step further in Workspace by giving customers direct control of encryption keys and the identity service they choose to access those keys. With client-side encryption, customer data is indecipherable to Google, while users can continue to take advantage of Google's native cloud-based collaboration, access content on mobile devices, and share encrypted files externally. This capability is currently available in Public Beta for Google Drive, Docs, Sheets, and Slides with plans to extend it to other Workspace services. Customers can also benefit from third-party solutions that offer end-to-end client side encryption for Gmail.

2. Direct Customer Access

All authentication sessions to Google Workspace are encrypted and users can only access the services enabled by their Domain Administrator.

3. Internal Google access by authorized individuals

Google implements strict access controls to ensure the person accessing the data is authorized to do so and validates that a business justification for access is provided. The justification is made visible to the customer through Access Transparency Logs[3].

4. Service Access

Google uses technologies like Binary Authorization to ensure the provenance and integrity of software allowed to access customer data.

In addition to the above controls, Google Workspace for Education Standard and Education Plus editions / Google Workspace customers can use Context-Aware Access[4] to create granular access control policies to apps based on attributes such as user, location, device security status, and IP address. Based on the BeyondCorp security model developed by Google, users can access web applications and infrastructure resources from virtually any device, anywhere, without utilising remote-access VPN gateways while administrators can establish controls over the device. Access decisions are not based solely on static credentials or whether they originate from a corporate intranet. The complete context of a request (user identity, location, device ownership and configuration, and fine-grained access policies) is evaluated to determine its validity and guard against phishing attempts and credential-stealing malware.

3. For those services integrated with Access Transparency. Access Transparency is available to Google Workspace for Education Standard or Education Plus edition license
4. Using context-aware access capabilities to protect access to Google Workspace apps requires a Cloud Identity Premium, Enterprise Standard, or Enterprise Plus license.

State of the Art Security

Understanding our Security Infrastructure Design may facilitate any compliance assessment you need to complete of Google Workspace for Education / Google Workspace services. Google has a global scale technical infrastructure designed to provide security through Google's entire information processing life cycle. Specifically, this infrastructure is designed 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.

The security of the infrastructure is designed in progressive layers starting from the physical security of data centers, continuing on to the security of the hardware and software that underlie the infrastructure, and finally, the technical constraints and processes in place to support operational security.

At Google, all employees are required to think "security first". Google employs many full-time security and privacy professionals, including some of the world's leading experts in information, application, and network security. To ensure Google stays protected, we incorporate security into our entire software development process. This can include having security professionals analyze proposed architectures and perform code reviews to uncover security vulnerabilities and better understand the different attack models for a new product or feature.

Google commits to implementing and maintaining technical and organisational measures providing a specified level of security that is approved by the customer. We will continue to innovate to provide customers with the best technology to protect the security and privacy of their information, including technical solutions that give customers greater control of their own data, and to support legal reforms that promote rather than undermine such innovation. In line with our Trust Principles, we never give any government "backdoor" access.

Google guarantees that its technical measures will include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Google further commits to notifying customers of any data incidents without undue delay.

Google exceeds GDPR requirements by committing to offer additional security controls which customers can use as they determine. These controls include an admin console, encryption capabilities, logging and monitoring capabilities, identity and access management, security scanning, and firewalls. For details, see the "Technical safeguards" section of this whitepaper above.

Google also exceeds GDPR requirements by committing to maintain various rigorous third-party certifications as well as detailed third party audit reports. For more information, see the "Third party certifications and compliance offerings" section of this whitepaper below.

Data Residency

Our customers who wish to have more control over the geolocation of their data can use Data Regions. Data Regions for Google Workspace for Education Standard and Education Plus editions, and Google Workspace Enterprise provide control over the geolocation for storage of email messages, documents, and other Google Workspace for Education/ Google Workspace content[5]. Customers can choose to store their covered data in the United States or Europe or globally, and can customize this for groups within their organization.

For Google Workspace for Education / Google Workspace's data location commitments, please see our Service Specific Terms. Additionally, with the advent of client-side encryption (see Access Controls section, above), customers can now keep keys in their preferred geo-location for the products in scope.

5. Refer to this guidance for a list of data and services covered by Data Regions.

2 Legal safeguards

Google Cloud's data protection terms offer strong legal protections:

New SCCs.
On 4 June 2021, the European Commission issued modernized SCCs for transfers of personal data under the GDPR, and from late September 2021 Google introduced these into its compliance offering, along with separate UK SCCs, for all new and existing Google Workspace customers (ahead of the 27 December 2022 deadline set by the Commission for transitioning existing customers to the new EU SCCs). Learn more in the Google Cloud's Approach to the New EU Standard Contractual Clauses whitepaper.

Compliant data transfers.
Under Google's updated Data Processing Amendment for Google Workspace, and for as long as no alternative transfer solution is available:

- customers in the EEA, UK and Switzerland can rely on Google to legitimize transfers of their customer data by entering (and publishing) SCCs with subprocessors, meaning those customers do not enter SCCs themselves;
- other customers in Europe, the Middle East and Africa (EMEA) will automatically enter the appropriate SCCs; and
- customers outside EMEA whose use of Google Cloud services is subject to the GDPR, the UK GDPR or Swiss Federal Data Protection Act will enter the appropriate SCCs once they certify via the admin console that they are subject to these laws.

Processing in accordance with instructions.
Google commits to processing customer data as instructed by the customer and consistent with our obligations under applicable law.

Security commitments.
Google commits to implementing and maintaining technical and organizational measures providing a specified level of security that is approved by the customer. Google guarantees that those measures will include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Google further commits to notifying customers of any data incidents without undue delay.

Additional security controls.
Google exceeds GDPR requirements by committing to offer additional security controls which customers can use as they determine. These controls include an admin console, encryption capabilities, logging and monitoring capabilities, identity and access management, security scanning and firewalls. For details, see the "Technical safeguards" section of this whitepaper above.

Certifications and audit reports.
Google also exceeds GDPR requirements by committing to maintain various rigorous third-party certifications as well as onerous third-party audit reports. For details, see the "Third-party certifications and compliance offerings" section of this whitepaper below.

3 Organizational safeguards

Government Requests for Data

The EDPB's recommendations introduce a risk-based approach under which data exporters should assess the level of risk to fundamental rights that a certain transfer would entail in practice.

Our Transparency Report discloses, where permitted by the applicable laws, the number of requests made by law enforcement agencies and government bodies for Enterprise Cloud customer information. The historical numbers disclosed in our report for Enterprise Cloud requests for customer information show that the number of Enterprise Cloud-related requests is extremely low compared to our Enterprise Cloud customer base and therefore, that the likelihood of Enterprise Cloud customer information data being affected by these types of requests is low.

We also work hard to give our customers a clear and detailed understanding of our process for responding to government requests for Cloud customer data in rare cases where they do happen. This process can be summarized as follows: If a government seeks customer data during the course of an investigation, Google will typically inform the government that it should request the data directly from the customer in question. If the government nonetheless compels Google to respond to a request for customer data, a dedicated team of Google lawyers and specially trained personnel will carefully review the request to verify that it is lawful and proportionate, following these guidelines:

Respect for the privacy and security of data you store with Google 1

When we receive a government request for customer data, our team reviews it to make sure it satisfies applicable legal requirements - including under the new EU SCCs - and Google's policies. Generally speaking, for us to produce any data, the request must be made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law. If we believe a request is overly broad, we'll seek to narrow it.

Customer notification 2

We will notify the customer before any of their information is disclosed unless such notification is prohibited by law or the request involves an emergency, such as an imminent threat to life. We will provide delayed notice to the customers if a legal prohibition on prior notification is lifted, such as when a statutory or court ordered disclosure prohibition period has expired. This notification typically goes to the Google Cloud customer's point of contact.

Consideration of customer objections. 3

Google will, to the extent allowed by law and by the terms of the government request, comply with a customer's reasonable requests regarding its efforts to oppose a request, such as the customer filing an objection to the disclosure with the relevant court and providing a copy of the objection to Google. If Google notifies the customer of a legal request by the US government and the customer subsequently files an objection to disclosure with the court and provides a copy of the objection to Google, Google will not provide the data in response to the request if the objection is resolved in favor of the customer. Other jurisdictions may have different procedures and are handled on a case-by-case basis.

We also recognize that the Schrems II decision has generated uncertainty about the impact of United States law on data transfers and on the role of Google LLC, a US company, as the data importer under SCCs entered to protect Google Cloud customer data. Many customers have questions about the classification of Google Cloud and our services under US law as well as specific questions around (EO 12333) and Title 50 United States Code (U.S.C.) § 1881a (FISA 702), both of which were considered by the CJEU. To address these issues, we have set out specific information about those laws and their application to Google Cloud products below.

Specific intelligence activities conducted under EO 12333 are subject to more specific implementing procedures (which may be classified) that include safeguards and protections appropriate to that type of intelligence activity. EO 12333 primarily governs intelligence activities that occur outside the US. EO 12333 is understood to permit the US to conduct electronic surveillance outside the US consistent with US legal requirements; it does not authorise electronic surveillance within the US nor does it impose requirements on service providers inside or outside the US.

Section 702 is a provision of the FISA Amendments Act of 2008 (FAA) that permits the U.S. government to conduct targeted surveillance of foreign persons located outside the United States, with the compelled assistance of "electronic communication service providers" (as defined by 50 U.S.C. § 1881(b)(4). Two programmes authorized under Section 702 of the FAA are referred to as "Upstream" and "Downstream".

Section 702 Upstream authorizes U.S. authorities to collect data travelling over internet "backbone" infrastructure controlled by electronic communication service providers in the U.S. (e.g. U.S. telecom providers). To the extent any Google Cloud customer data traverses networks subject to Upstream 702 collection, that data is encrypted in transit as described above.

Section 702 Downstream authorizes U.S. authorities to obtain targeted data directly from electronic communication service providers. To the extent Google LLC may receive targeted requests relating to Google Cloud customer data under Downstream 702, we carefully review each request in accordance with the guidelines described above to make sure the request satisfies all applicable legal requirements and Google's policies.

To learn more about how we handle government requests for data, please see our whitepaper (Government requests for customer data: controlling access to your data in Google Cloud), our policy page (policies.google.com/terms/information-requests), and our regularly-updated Transparency Report (https://transparencyreport.google.com/user-data/us-national-security?hl=en), which was the first report of its kind to be published by a cloud provider.

4 Third-party certifications, compliance offerings, and customer commitments

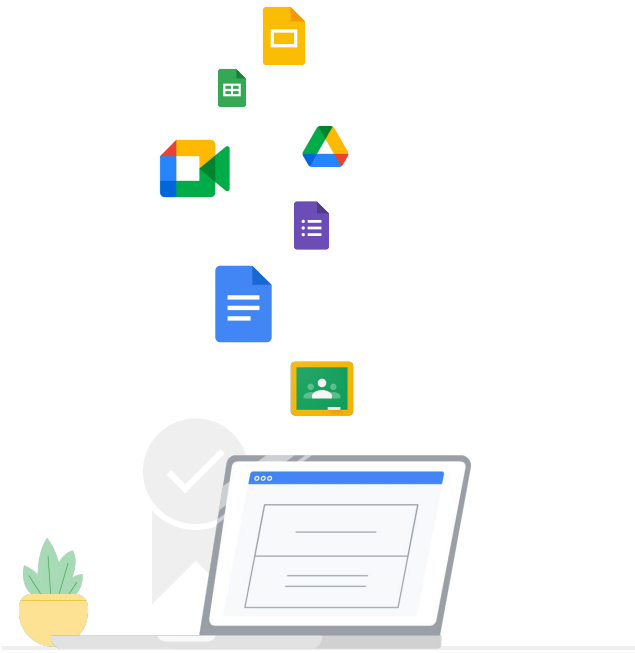
Regulations such as GDPR place significant emphasis on enterprises knowing how their data is being processed, who has access to data, and how security incidents will be managed.

Google Cloud has dedicated teams of engineers and compliance experts who support our customers in meeting their regulatory compliance and risk management obligations. Our approach includes collaborating with customers to understand and address their specific regulatory needs. Together with our reports and certifications, we assist our customers in documenting an integrated controls and governance framework.

For customers in certain regions or customers operating in certain regulated verticals, we allow customers to conduct audits to validate Google's security and compliance controls. Our products regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations of compliance, or audit reports against standards around the world.

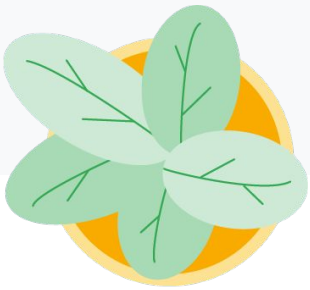
We've also created resource documents and mappings against frameworks and laws where formal certifications or attestations may not be required or applied. Certifications such as those from ISO/IEC (ISO/IEC 27001, 27017, 27018, 27701) as well our SOC 3 Audit Report, may also help customers in meeting requirements of the GDPR.

For our existing customers who want to learn more about Google's Security, we would be happy to make a detailed SOC 2 report available via the Compliance Reports Manager. You can see a full listing of all of our compliance offerings in our Compliance Resource Center. For details of some of the supplementary commitments we offer beyond the certifications please visit our Trust Principles and Enterprise Privacy Commitments.



Conclusion

We are committed to providing and continuing to advance technical, legal, and organizational safeguards that will support any Google Cloud customers assessing the risk of international data transfers.



We firmly believe that Google Cloud's SCCs, along with the safeguards and commitments discussed above, provide our customers with adequate protection for transfers of their data.

We hope this whitepaper is helpful for any customers conducting compliance risk assessments, but encourage all customers to consult with legal counsel as this whitepaper should not be used as a substitute for legal advice.