

# Google for Education

## Safeguards for international data transfers with Google Workspace and G Suite for Education

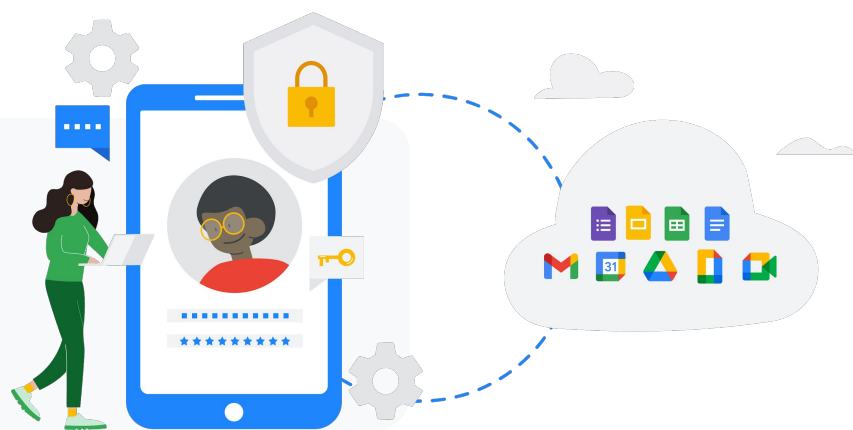


# Introduction

This whitepaper explains some of the safeguards and supplementary commitments to GDPR requirements that Google Cloud offers to protect and enhance your<sup>1</sup> control of customer data in [Google Workspace](#) and G Suite for Education.<sup>2</sup>

This information should assist you in assessing the impact of the Court of Justice of the European Union (CJEU) case [C-311/18](#), known as the Schrems II decision, as it relates to data transfers on Google Cloud. We have also included information about United States laws and their applicability to Google Cloud to aid your risk assessment in light of that decision.

On July 16, 2020, the CJEU invalidated the European Commission's decision underlying the EU-US Privacy Shield Framework but did not invalidate EU Model Contract Clauses (MCCs, also known as Standard Contractual Clauses) as a mechanism by means of which personal data can be transferred outside of the EU, Switzerland or the UK (as applicable) in compliance with the strict requirements imposed by EU data protection law regarding international data transfers.



<sup>1</sup> In this whitepaper, "You/your" refers to G Suite for Education / Google Workspace customers as well as G Suite for Education / Google Workspace partners. Unless indicated otherwise, references to "customers" will include G Suite for Education / Google Workspace partners and references.

<sup>2</sup> We are bringing Google Workspace to our education and nonprofit customers in the coming months. Education customers can continue to access our tools via G Suite for Education, which includes Classroom, Assignments, Gmail, Calendar, Drive, Docs, Sheets, Slides, and Meet. G Suite for Nonprofits will continue to be available to eligible organisations through the Google for Nonprofits program.



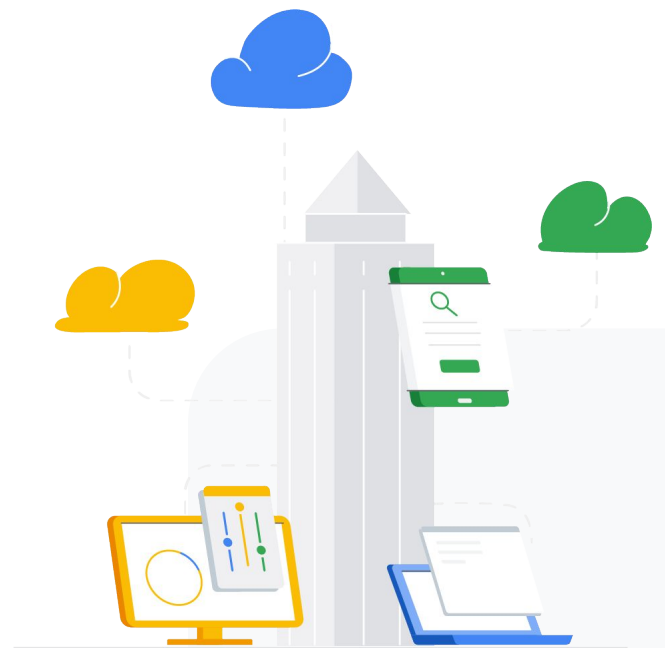
## Google has offered customers MCCs as a data transfer mechanism for G Suite for Education/ Google Workspace since 2012.

The European Union's Data Protection Authorities [confirmed](#) in 2017 that Google's MCCs for G Suite for Education / Google Workspace were in alignment with the European Commission's [SCCs](#). To date, millions of G Suite for Education / Google Workspace customers have chosen to rely on Google's MCCs for compliant transfers of their data. Following the CJEU ruling, Google updated its [data processing terms](#) (G Suite for Education / Google Workspace customers) to deem those MCCs to apply automatically to all G Suite for Education / Google Workspace customers who are subject to EU data transfer requirements, in the absence of any alternative transfer mechanism.

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 MCCs should assess whether that third country provides protection essentially equivalent to that guaranteed by EU law in order to determine whether the MCCs can ensure an adequate level of protection in practice. In other words, in order to transfer personal data based on MCCs, the data exporter and importer should assess whether the laws in the relevant third country undermine the adequate level of protection otherwise provided by the MCCs.

If it is uncertain whether in specific circumstances MCCs alone will ensure the protection required by EU law, the CJEU indicated that "supplementary measures", when used with MCCs, could establish an adequate level of protection.

Guidance from the European Data Protection Board and national data protection authorities on "supplementary measures" is pending, and this whitepaper will be updated when that guidance is issued. In the meantime, this whitepaper provides information on the additional safeguards and supplementary commitments offered by Google Cloud to enhance the protection for transfers of EU personal data. However, please note that as a provider of cloud services, we are not in a position to provide you with legal advice – this is something only your legal counsel can provide.




# 1. Technical safeguards

## Encrypting data in transit and at rest

Encryption is an important piece of the G Suite 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 below 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 an 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 controls for Google Workspace and G Suite for Education

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

- 1 Direct customer access:** All authentication sessions to Google Workspace are encrypted and users can only access the services enabled by their Domain Administrator.
- 2 Internal Google access by authorised individuals:** Google implements strict access controls to ensure the person accessing the data is authorised 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](#).<sup>3</sup>
- 3 Service Access:** Google uses technologies like [Binary Authorization](#) to ensure the provenance and integrity of software allowed to access customer data.

<sup>3</sup> For those services integrated with Access Transparency. Access Transparency is available to Google Workplace Enterprise and G Suite Enterprise for Education customers only.

In addition to the above controls, G Suite Enterprise for Education / Google Workspace customers can use [Context-Aware Access](#)<sup>4</sup> 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.

### State of the Art Security

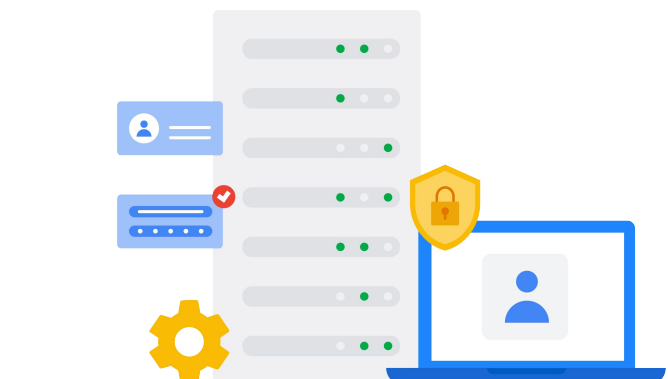
Understanding our [Security Infrastructure Design](#) may facilitate your compliance assessment of G Suite for Education / Google Workspace services. Google has a global scale technical infrastructure designed to provide security through Google's entire information processing life cycle. Specifically, 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.

Our infrastructure is not designed to, and does not, give the United States government or any other government "backdoor" access to your data or to our servers storing your data.

### Data Residency

Our customers who wish to have more control over the geolocation of their data can use Data Regions. [Data Regions](#) for G Suite Enterprise for Education and Google Workspace Enterprise provide control over the geolocation for storage of email messages, documents, and other G Suite for Education/ Google Workspace content. Customers can choose to store their covered data in the United States or Europe or globally, and can customize this for groups within their organisation. For G Suite for Education / Google Workspace data location commitments, please see our [Service Specific Terms](#).








<sup>4</sup> Using context-aware access capabilities to protect access to Google Workspace apps requires a Cloud Identity Premium, Enterprise Standard, or Enterprise Plus license.

<sup>5</sup> 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:

-  **MCCs apply automatically**  
As mentioned above, as long as there is no alternative transfer solution available, MCCs now apply automatically to all G Suite for Education / Google Workspace customers who are subject to EU data transfer requirements.
-  **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 organisational 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. Organisational safeguards

## Government requests for data

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:

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

When we receive a government request for customer data, our team reviews it to make sure it satisfies applicable legal requirements and Google's policies. Generally speaking, for us to produce any data, the request must be made in writing, signed by an authorised 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.

### 2 Customer notification

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 customer 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.

### 3 Consideration of customer objections

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 MCCs entered with Google Cloud customers. 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 US 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 authorised under Section 702 of the FAA are referred to as “Upstream” and “Downstream”.**

### Section 702 Upstream

authorises US authorities to collect data travelling over internet “backbone” infrastructure controlled by electronic communication service providers in the United States (e.g. US 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

authorises US 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.

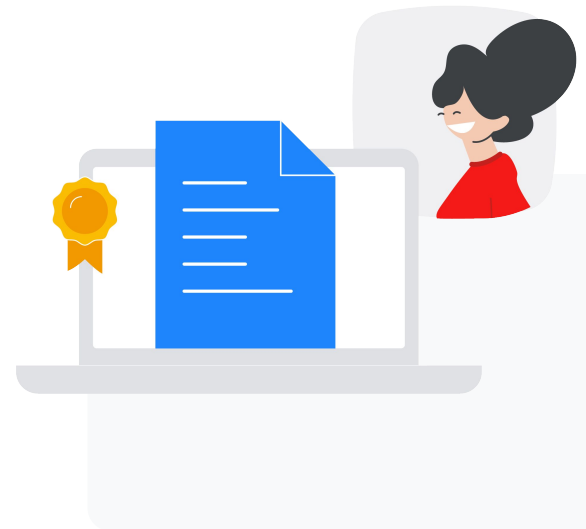


To learn more about how we handle government requests for data, please see our whitepaper ([Government requests for customer data: controlling access to your data in Google Cloud](#)), our [policy page](#), and our regularly-updated [Transparency Report](#), which was the first report of its kind to be published by a cloud provider.

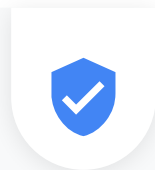


## 4. Third-party certifications, compliance offerings, and customer commitments

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 facilitate a detailed [SOC 2 report](#) 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 organisational safeguards that will support Google Cloud customers in assessing the risk of international data transfers. We firmly believe that Google Cloud's MCCs, along with the safeguards and commitments discussed above, provide our customers with adequate protection for transfers of their data. We will promptly notify customers, as our MCCs would require us to do, if there is any change that substantially and adversely affects our ability to process their customer data as instructed.



We hope this whitepaper is helpful for 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.