Google Cloud Whitepaper
September 2021

Safeguards for international data transfers with Google Cloud

Google Cloud

Table of Contents

Disclaimer

The content contained herein is correct as of September 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 to GDPR requirements Google offers to protect and enhance your[1] control of your customer data in Google Cloud. This information can assist in assessing the impact of the European Data Protection Board (EDPB) Recommendations on Supplementary Measures following the Court of Justice of the European Union's (CJEU) ruling known as Schrems II, as it relates to data transfers. We have also included information about United States laws and their applicability to Google Cloud to aid you with any risk assessment you may need to complete in light of that decision.

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 in compliance with the strict requirements imposed by EU data protection law regarding international data transfers[2].

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 undermine 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.

[1] In this whitepaper, "you/your" refers to GCP customers as well as partners and to Google Workspace and Cloud Identity customers. Unless indicated otherwise, references to "customers" will include GCP partners and references to "customer data" will include GCP "partner data".
[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.
.

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.

Technical safeguards

Customers place a high priority on protecting their data, especially sensitive information. We are happy to confirm that many of the EDPB's Recommendations are in line with Google's long-standing commitment to security and technical safeguards, such as encryption and auditable access controls. We are also continuing to invest in the development of additional customer-managed controls.

Encryption

Google will continue its well-established practice of implementing state of the art encryption into Google Cloud services to protect against unauthorized third-party access to Google Cloud customer data.

Encryption is a process that takes readable data as input (often called plaintext), and transforms it into an output (often called ciphertext) that prevents reading of the plaintext. If data is encrypted, it will be unreadable to a third party without the encryption key, and cannot be accessed in a meaningful form by a U.S. or other government agency unless they go through formal access channels to obtain the plaintext, as described in the "Organisational safeguards" section of this whitepaper below. Encryption is therefore an effective means of preventing third-party access to Google Cloud customer data except through a formal legal request to Google and, depending on the type of encryption used, may even prevent access via formal legal channels.

Encryption in transit for Google Cloud Platform and Google Workspace

Google Cloud enforces encryption in transit by default using FIPS 140-2 validated cryptographic modules to encrypt all inter-region traffic. Read more about Google Cloud's encryption in transit here.

Google's Application Layer Transport Security (ALTS) is a mutual authentication and transport encryption system developed by Google and used for securing Remote Procedure Call (RPC) communications within Google's infrastructure. ALTS is similar in concept to mutually authenticated TLS but has been designed and optimized to meet the needs of Google's data centre environments.

Google has also 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. In Workspace, 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.

.

Encryption at rest: Google Cloud Platform

Whenever data is stored at rest, Google Cloud Platform applies encryption by default at the storage level using AES256.[3] We use several layers of encryption, which adds several levels of data protection and allows us to select the optimal approach based on application requirements. Read more about Google Cloud Platform's encryption at rest here.

Cryptographic key management

In addition to Google's default encryption, Google Cloud Platform customers have additional key management options available for protecting their data at rest:

- Our **Cloud Key Management Service** (Cloud KMS) enables customers to manage specific cryptographic keys in a central cloud service for either direct use or use by other cloud resources and applications. For qualifying services,[4] customers can use the key management capabilities built into Cloud KMS to protect their data at rest, a control we also refer to as customer-managed encryption keys (CMEK).

- The **Cloud HSM Service** (Cloud HSM), which is similar to Cloud KMS, allows customers to protect supported data at rest, but with keys that are protected and cryptographic operations that all occur within a FIPS 140-2 Level 3 certified hardware security module. Customers can use Cloud HSM keys for encryption, decryption, and signing operations, as well as for CMEK scenarios. Cloud HSM is a fully managed service, meaning that Google will own, control, and administer the hardware in which the keys are protected. However, all keys within the service will be created as non-extractable which means that the hardware device will prevent any entity, including Google, from extracting the key material.

Please see the Google Cloud Platform Encryption whitepaper for more information on encryption at rest.

Encryption in use: Google Cloud Platform

In Google Cloud, we offer customer-configurable controls to encrypt and protect data in-use in virtual machine (VM) and kubernetes nodes (GKE) memory. Encryption keys are ephemeral, generated on chip and are non-exportable based on the CPU-based encryption engine that transparently encrypts and decrypts the data in memory. Encryption keys are kept hidden from untrusted parts of the platform and most importantly non-extractable by software.

[3] A small number of Persistent Disks created before 2015 use AES128. See the Google Cloud Platform Encryption whitepaper for more information.

[4] See Using Cloud KMS with other products for more information on the products integrated with the Cloud KMS platform that support CMEK.

.

Encryption at rest: Google Workspace

Google Workspace applies encryption by default when data is stored at rest - stored on a disk (including solid-state drives) or backup media. We use an Advanced Encryption Standard (AES) cipher with a unique 128-bit or stronger key for each chunk of Google Workspace data stored on a local disk. Each chunk key is then encrypted by another 128-bit or stronger key that is managed by a Google-wide key management service (KMS). Google Workspace data is also encrypted when stored on backup media, each of which is protected with a 256-bit secret that itself is encrypted via KMS. Read more about encryption of Google Workspace data at rest here.

Please see the Google Workspace Encryption whitepaper for more information on encryption.

Enhanced customer controls

Google also offers enhanced customer controls to help GCP and Google Workspace customers meet their security and compliance needs. For customers who wish to access the bundle of enhanced customer controls that includes data residency, External Key Manager, Key Access Justifications and European support, these controls are available as the EU Regions and Support with Sovereign Controls package inside Assured Workloads. More information on these controls can be found below.

Cloud External Key Manager - GCP

Cloud External Key Manager (Cloud EKM) may help GCP customers meet security and compliance requirements by allowing them to maintain possession of their encryption keys and providing them with the ability to mandate key separation from data. Cloud EKM allows customers to encrypt data at rest with keys that are stored and managed in third-party key management systems deployed outside of Google's infrastructure.

Cloud EKM provides several benefits:

- **Key provenance:** You control the location and distribution of your externally-managed keys. Externally-managed keys are never cached or stored within Google Cloud Platform. Whenever Google Cloud Platform needs to decrypt data, it communicates directly with the external key manager.

- **Access control:** You manage access to your externally-managed keys. Before you can use an externally-managed key to encrypt or decrypt data in Google Cloud, you must grant the Google Cloud project access to use the key. You can revoke this access at any time.

- **Centralized key management:** You can manage your keys and access policies from a single location and user interface, whether the data they protect resides in the cloud or on your premises.

If you use Cloud EKM, Google cannot access clear text without your permission for in-scope products. So unless you give Google access to the external key, we would only be able to produce ciphertext in response to a request for stored data encrypted with that external key.

.

In addition to Cloud EKM, customers may leverage Key Access Justifications to control each time their externally hosted keys are used to decrypt data. Using Key Access Justifications with Cloud EKM, customers will receive:

- Visibility into every request for an encryption key that permits data to change state from at rest to in use, with a justification for that request.
- A mechanism to explicitly approve or deny decryption using the key in the context of that request, using an automated policy that you set (via third-party functionality).

This means there is no way for Google to decrypt customer data at rest without customer approval, which you can withhold for any reason. This is because:

- Data is always encrypted at rest
- Encryption keys needed to decrypt the data are stored and managed outside of Google's technical infrastructure
- Decrypting customer data requires a call outside of Google to the customer's externally-managed key
- Customers can expect every request to come with a justification, and block requests automatically for any reason they don't like
- Reasons for key requests are detailed so that customers can understand what is happening to their data

Additionally, the overall solution comes with an integrity commitment that gives customers confidence in the controls working as described.

Client-side Encryption Solutions: Google Workspace

Workspace is taking encryption a step further by giving customers the ability to manage access through 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 web-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, and allows customers to keep keys in their preferred geo-location and better manage access to covered content.

Our customers can also choose third party encryption solutions (including with EU-based companies) for some of our products, such as Gmail. To achieve complete segregation of keys and data, third-party partners like Virtru or FlowCrypt offer client-side encryption for Gmail. The keys can be geo-located either on prem or in the cloud. We will continue to invest in both customer-controlled encryption technology and can provide further information about our product roadmap upon request.

.

Confidential Computing: GCP

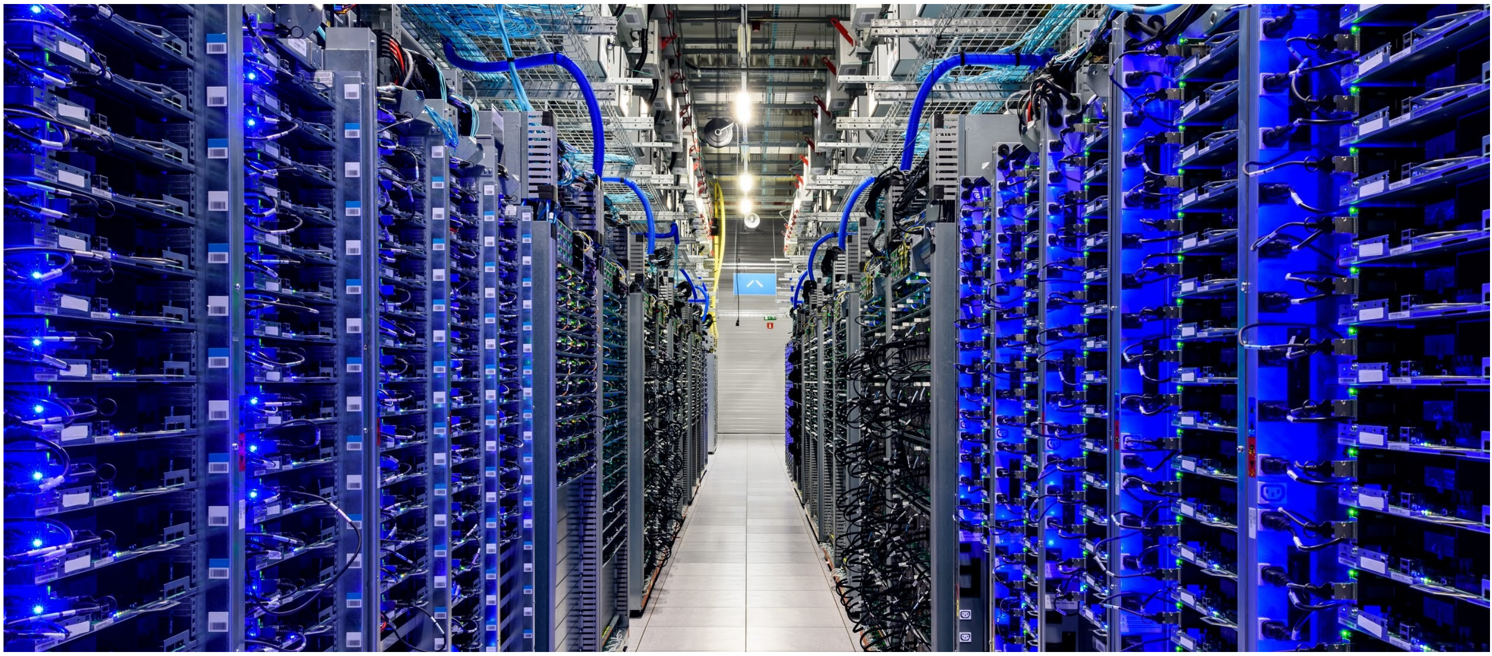
Google Cloud Platform now offers Confidential Computing, which is technology that allows you to encrypt data in the cloud while it’s being processed. With the confidential execution environments provided by Confidential VM and AMD SEV, Google Cloud keeps customers' sensitive code and other data encrypted in memory during processing. Google does not have access to the encryption keys.

Confidential computing has the potential to provide a flexible, isolated, hardware-based trusted execution environment to users, allowing them to protect their data and sensitive code against malicious access and memory snooping while data is in use in addition to protecting data in-transit and at-rest.

We will continue to invest in customer-controlled encryption technology and can provide further information about our product roadmap upon request.

Access control

At Google Cloud, the privacy and security of customer data underpins the design of all of the services that we offer. We believe that customers should have a strong level of control over data stored in the cloud. To support that mission, we’ve developed industry-leading product capabilities that enhance your control over your data and provide expanded visibility into when and how your data is accessed.



Access control for Google Cloud Platform

Google Cloud Platform has implemented several controls designed to ensure that each of the data access pathways functions as intended:

.

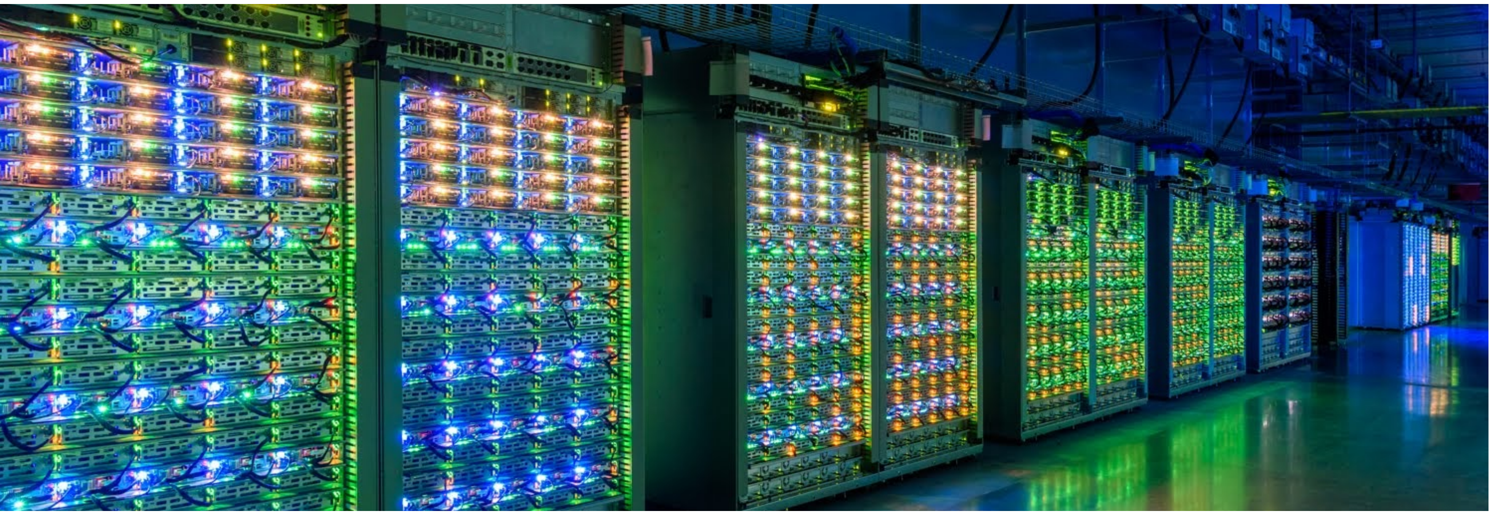
- **Customer authorization**: When services access data on behalf of a customer, they perform authorization checks to ensure the customer has appropriate permissions before proceeding.
    - **Zero trust access model**: BeyondCorp provides user and device based authentication and authorization for Google's core infrastructure. 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.

- **Access Transparency:** As part of Google's long-term commitment to security and transparency, you can use Access Transparency to review logs of actions taken by Google staff when accessing certain customer data as permitted by law. Access Transparency logs include data about Google staff activity, including:
    - Actions by the Support team that you may have requested by phone
    - Basic engineering investigations into your support requests
    - Other investigations made for valid business purposes, such as recovering from an outage.

- **Access Approval:** GCP also offers Access Approval, which allows customers to explicitly approve access to data or configurations on Google Cloud. Additional information can be found in our Access Approval documentation.

- **Service authorization**: GCP offers Google Binary Authorization services to validate and continue monitoring the provenance and integrity of the containers processing customers data. Binary Authorization is an integrated part of customers' deployment software supply chain and their CI/CD flow.

- **European Support**: GCP is expanding its existing Assured Support offering to the EU. Coming soon, customers using Assured Workloads for EU will have the ability to obtain support from EU Personnel only, ensuring that their issues are supported by local staff to help minimise the risk of customer data leaving the EU while customers are receiving support. The capability extends to administrative and operational support, and this control will ensure that system



administration actions involving customer data will only be performed by EU personnel from an EU location.

Access control for Google Workspace

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

- **Direct customer access:** All authentication sessions to Google Workspace are encrypted and users can only access the services enabled by their Domain Administrator.
    - **Zero trust access model:** In addition to the above controls, Google Workspace customers can use Context-Aware Access[5] 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.

- **Access Transparency:** As part of Google's long-term commitment to security and transparency, you can use Access Transparency to review logs of actions for covered service data taken by Google staff when accessing certain customer data as permitted by law. 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[6].

- **Service Access:** Google uses technologies like Binary Authorization to ensure the provenance and integrity of software allowed to access customer data.

State of the art security

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

[5] Using context-aware access capabilities to protect access to Google Workspace apps requires a Cloud Identity Premium, Enterprise Standard, or Enterprise Plus license.

[6] For those services integrated with Access Transparency. Access Transparency is available to Google Workplace for Education Standard, or Education Plus license
.

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 centres, 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.

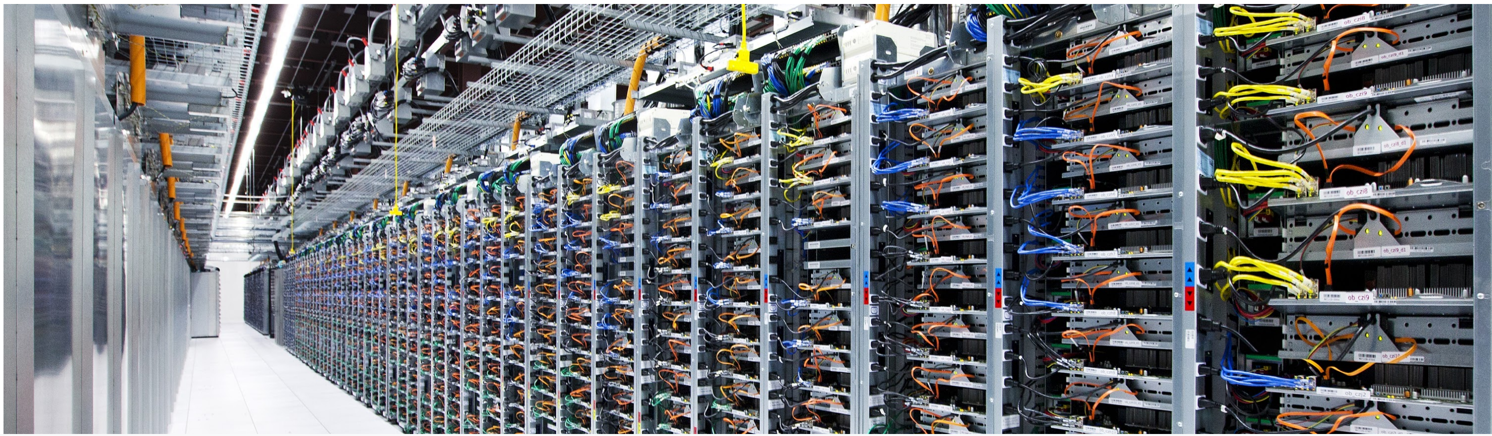
At Google, all employees are required to think "security first". Google employs many full-time security and privacy professionals, including some of the world's leading experts in information, application, and network security. To ensure Google stays protected, we incorporate security into our entire 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.



Contractual measures

Legal protections

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 GCP customers and partners and 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 and Security Terms (DPST) for Google Cloud Platform and 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 strictly as instructed by the customer.

- **Availability of Additional Security Controls.** We commit to making additional security controls (including encryption) available to our customers to use in order to further protect their data

- **Security measures.** Google gives robust commitments around the technical and organisational measures it takes to secure customers' data.

Subprocessor commitments

Google engages subprocessors to perform limited activities in connection with the GCP and Google Workspace. Our GCP and Google Workspace subprocessor pages show what activity each subprocessor performs.

.

Before onboarding a subprocessor, Google conducts an audit of the security and privacy practices of the subprocessor to ensure the subprocessor provides a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide.

Once Google has assessed the risks presented by the subprocessor, the subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms. In particular, Google will ensure via the contract that the subprocessor accesses customer data only to the extent required to perform their limited activity and that all access is in accordance with Google Cloud's data protection terms, including the SCCs where applicable.

Google remains fully liable for all the activities of its subprocessors and continuously monitors their performance and contractual compliance, including via regular assessments and audits.

Organisational safeguards

Transparency

At Google Cloud, we believe that trust is created through transparency, and we want to be transparent about our commitments and what you can expect when it comes to our shared responsibility for protecting and managing your data in the cloud. We understand that a big part of being transparent is providing information on when requests are made for access to your data.

In our Transparency Reports, we share our data about how the policies and actions of governments and corporations affect privacy, security, and access to information.

We also offer Access Transparency for GCP and Google Workspace that log and surface to the customer administrative access to customer data by Google Cloud as permitted by law. We also undergo third party audits to verify our privacy and security compliance obligations publicly.

Government requests for data

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. For example, our report shows that no Google Cloud Platform Enterprise customer data was produced in response to such requests in the last reporting period.

We also work hard to help give our customers a clear and detailed understanding of our process for responding to government requests for Cloud customer data in the 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. This approach is generally aligned with US government policy.

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.** 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. If we believe a request is overly broad, we'll seek to narrow it.

- **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 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.** 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 U.S. 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.

Government engagement on a bilateral and multilateral level is critical for modernising laws and establishing rules on the production of electronic evidence across borders in a manner that respects international norms and sovereignty, and that resolves any potential conflicts of law. Google has supported these efforts and will continue to do so while protecting the privacy and security of our customers.

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 U.S. 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 U.S. law as well as specific questions around U.S. Executive Order 12333 (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.

.

EO 12333 largely governs U.S. intelligence activities outside the United States. It does not impose obligations on Google LLC. Although, in principle, the U.S. government may use EO 12333 to collect data directly from infrastructure outside the United States, such as undersea cables, Google Cloud customer data is always encrypted in transit between regions and, as stated above, Google's infrastructure does not give the U.S. government "backdoor" access to customer data. EO 12333 requires the U.S. government to use the least intrusive means feasible of obtaining intelligence.

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 Government requests for customer data: controlling access to your data in Google Cloud whitepaper, and our policy page. Customers and end users can also review the number of requests Google LLC has received under U.S. National Security authorities for all Google services (including Google Cloud) in our Transparency Report.

Adoption of standards and best practices

We are always looking at ways to increase accountability, compliance support, and additional data transfer mechanisms to our customers. We are glad to announce our adherence to the Scope EU GDPR Code of Conduct. We believe that codes of conduct are effective collaboration instruments among industry players and data protection authorities where state-of-the-art industry practices can be tailored to meet robust data protection requirements.

For details of some of the supplementary commitments we offer beyond the requirements of the GDPR, please see our ISO/IEC certifications (ISO/IEC 27001, 27017, 27018 and 27701) as well our SOC 3 Audit Report, available here. 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.

Data residency

Our customers may also want to consider our data residency capabilities, which differ slightly depending on the Google Cloud products they are using. For example, in European Union, even if data localisation is not strictly required by law, our compute and storage key services allow customers to store customer data at rest exclusively in regions in Belgium, Germany, Finland, the Netherlands, Poland, and other EU regions becoming available in the future. These offerings may help satisfy company-specific policies around locating data at rest.

Physical storage of data

- For GCP, our compute and storage key services allow customers to store customer data at rest exclusively in regions in Belgium, Germany, Finland, the Netherlands, Poland, and other EU regions becoming available in the future. These offerings may satisfy company specific policies around locating data at rest. Our customers with data residency requirements can set up a Resource Locations policy that constrains the location of new resources for their whole organisation or individual projects. With these capabilities, customers can prevent their employees from accidentally storing customer data in an unintended Google Cloud region. For GCP's data location commitments, please see our GCP Service Specific Terms.

- Data regions for Google Workspace provide control over the geographical location for storage of email messages, documents, and other Google Workspace content.[7] Our customers can

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

choose to store their covered data in the United States or Europe or globally, and can customize this for groups within their organisation. For Google Workspace's data location commitments, please see our Google Workspace Service Specific Terms.

Location based access

- GCP customers can use VPC Service Controls to restrict the network locations from which their users can access data, defining a service perimeter outside of which customer data cannot be accessed. This functionality allows customers to limit user access by IP address filtering, even if the user is authorized.
- Cloud Armor also allows customers to restrict locations from which traffic is allowed to their external load balancer.

Conclusion

We are committed to providing and continuing to advance technical, legal, and organisational safeguards that will support Google Cloud customers in assessing and mitigating (as necessary) any risk associated with international data transfers.

With the capabilities we offer, Google Cloud Platform customers can store data in the European region, ensure certain customer data is not moved outside of Europe, and prevent users and administrators outside of Europe from accessing their data. They can exercise additional control over who accesses their data by managing their own encryption keys, ensure the keys are stored in a European region, and store their encryption keys outside Google Cloud's infrastructure. Customers can require detailed justification and approval each time a key is requested to decrypt data, and deny Google the ability to decrypt their data for any reason. You can learn more by reading our blog on advancing control and visibility in the cloud. For insight into what this commitment to customers means from a technical perspective, please see our post on options for data residency, operational transparency and control.

Our Google Workspace (formerly G Suite) Enterprise[8] customers can select to store their covered data in Europe. Our customers can also choose client-side encryption or third party encryption solutions (including with EU-based companies) for some of our products, such as Gmail. With these solutions, customers can keep keys in their preferred geo-location and manage access to content. We also offer Access Transparency which provides customers visibility into actions taken by Google staff when they access their covered services data.

[8] Including Google Workspace for Education Standard and Education Plus editions, and Google Workspace Enterprise editions.

.

We firmly believe that Google Cloud's SCCs, along with the safeguards and commitments discussed in this whitepaper, provide our customers with adequate protection for international 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.

.