Government requests for customer data: controlling access to your data in Google Cloud
Table of contents

Introduction .................................................................................................................................. 3

Requests for data and the CLOUD act ......................................................................................... 4

Technical controls for data access and data disclosure ................................................................. 6

Access Transparency and control ................................................................................................ 6
   Access Transparency
   Access Approval

Encryption-based controls ............................................................................................................. 7
   Encryption at Google
   Key creation
   Key rotation
   Encryption implementations
     Cloud Key Management Service (KMS) and Cloud hardware security module service (HSM)
     Cloud KMS key deletion
     Google-managed encryption keys
     Customer-managed encryption keys (CMEK)
     Customer-supplied encryption keys (CSEK)
     Services supporting CSEK
     Client-side encryption
     Services supporting client-side encryption keys

Conclusion ................................................................................................................................... 16

Appendix: URLs .......................................................................................................................... 17
Introduction

This document describes the products and product features available to your enterprise to control and/or otherwise restrict access to your data. This may be especially relevant for you if you are concerned about insider access and government data disclosure requests directed to Google rather than to you, and you prefer to have more control and transparency regarding how your data is handled.
Requests for data and the CLOUD act

One particular situation that is of interest to our customers and partners relates to requests for data from U.S. law enforcement agencies and, more recently, the impact of the CLOUD Act on the privacy and security of our customers’ data.

Like other technology and communication companies, Google receives requests from governments and courts around the world to disclose customer data. Google is committed to maintaining trust with our customers by being transparent about how we respond to such requests and by vigorously defending the privacy of customer data, all while meeting our legal obligations. In 2010, Google launched its first transparency report covering government requests for user data. Google was the first cloud provider to make public the volume and type of government requests for user data that we receive in a biannual transparency report, and describe how Google responds to those requests.¹ Our reports are industry leading and have become the standard in the U.S.

Google also works to promote trust through our government access policies and practices. We have a team that reviews and evaluates each and every one of the requests we receive based on international human rights standards, our own policies, and the law. In addition, Google does not provide any government entity with direct "backdoor" access. Generally speaking, for Google to produce data in response to legal process, 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 will seek to narrow it. This process applies both to accounts held by individual users and enterprise customers alike.

¹ Page 4, Transparency Report
In addition, it is Google’s policy to encourage governments to request data from cloud customers before requesting it from Google. This is aligned with the stated policy of the U.S. Department of Justice (DOJ) to seek data from cloud customers before requesting it from cloud service providers.²

The CLOUD Act is a 2018 amendment to the Stored Communications Act (SCA), which governs the disclosure of stored electronic communications and data to governmental entities in the US.

The CLOUD Act clarifies that where data is physically stored is not itself a factor in whether a legal process issued under the SCA is valid to compel a U.S. service provider to disclose data in its possession, custody, or control. This provision is the source of ongoing interest by stakeholders like governments and cloud customers. The DOJ recently published a whitepaper³ entitled “Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act” in response to that interest.

There are four important things that the CLOUD Act does not do.

1. First, the CLOUD Act does not expand the powers of the U.S. government to issue search warrants to U.S. service providers, and it does not create new surveillance powers.

2. Second, the CLOUD Act does not modify or relax the high standards that the U.S. government must meet before it can compel the production of communications content from a U.S. service provider.

3. Third, the CLOUD Act does not modify the DOJ’s policy that prosecutors should request data from cloud customers directly, not from the customer’s provider.

4. Finally, and importantly, the CLOUD Act does not require providers like Google to weaken their strict standards for reviewing government requests for data - and Google has not done so.

In fact, as described below, Google not only maintains strict standards for government access but also has developed products and product features that further enhance the control that Google Cloud customers have over their data and that give customers transparency and visibility over how their data is accessed.

---

² Page 5, Seeking Enterprise Customer Data Held by Cloud Service Providers
³ Page 5, Promoting Public Safety, Privacy and the Rule of Law Around the World
Technical controls for data access and data disclosure

Google Cloud provides numerous products and features to help you control and understand how and why your data is accessed and prevent the unintended disclosure of and access to data.

Access transparency and control

Access Transparency

As part of Google’s long-term commitment to transparency and user trust, we developed Access Transparency so that you can review logs of actions taken by Google staff when accessing user data. Access Transparency enables you to get more visibility into actions taken by Google staff related to your data. You can view the reason for each access, including references to specific support tickets where relevant, which may help you support your audit requirements. Government requests for data will have the reason “THIRD_PARTY_DATA_REQUEST” in the Access Transparency Log. Note that there may be instances when Google is legally prohibited from notifying you of the access, so no entry will be provided.

Google does not access your data for any reason other than those necessary to fulfill our contractual and or legal obligations. Google also performs regular audits of access by administrators as a check on the effectiveness of our controls.

Learn more about Access Transparency coverage for specific products and services for Google Cloud Platform and G Suite.

Access Approval

Access Approval allows you to explicitly approve access to data or configurations on GCP before it takes place, with exceptions for legal and outage use cases. These controls can be used to further limit what Google Support and engineering are able to do when administering services. This functionality is available to Platinum or Enterprise (Role-based) support customers on GCP.

Learn more about Access Approval.

4 Page 6, Access Transparency
5 Page 6, Using Access Transparency to report Google access
6 Page 6, Access Approval documentation
Encryption based controls

Google provides many options for you to control encryption keys and, by association, control data access. It is important to understand the nuances of each of these options when selecting a data management strategy in the Cloud.

Encryption at Google

Encryption is a process that takes legible data as input (often called plaintext), and transforms it into an output (often called ciphertext) that reveals little or no information about the plaintext. At Google, encryption is used to protect data at rest and in transit when data moves outside physical boundaries not controlled by Google or on behalf of Google.

Encryption at rest

Reduces the surface of attack by effectively “cutting out” the lower layers of the hardware and software stack. Even if these lower layers are compromised (for example, through physical access to devices), the data is still encrypted.

Encryption in transit

Protects your data if communications are intercepted while data moves between your site and the cloud provider or between two services. This protection is achieved by encrypting the data before transmission; authenticating one or both of the endpoints; and decrypting and verifying the data on arrival. For example, Transport Layer Security (TLS) is often used to encrypt data in transit for transport security, and Secure/Multipurpose Internet Mail Extensions (S/MIME) is often used for email message security.

Learn more about encryption at rest\textsuperscript{7} and encryption in transit\textsuperscript{8}.

\textsuperscript{7} Page 7, Encryption at Rest in Google Cloud Platform
\textsuperscript{8} Page 7, Encryption in Transit in Google Cloud
Google Internal Key Management Service
(Google's Internal KMS)

Customer data is broken into chunks for persistent storage. Each chunk is encrypted at the storage level with an individual encryption key. The key used to encrypt the data in a chunk is called a data encryption key (DEK). Because of the high volume of keys at Google, and the need for low latency and high availability, these keys are stored near the data that they encrypt. The DEKs are protected by a key encryption key (KEK). One or more KEKs exist for each Google storage system. These KEKs are stored centrally in Google's Internal Key Management Service, a repository built specifically for storing keys. Having a smaller number of KEKs than DEKs and using a central KMS makes storing and encrypting data at Google scale manageable, and allows us to track and control data access from a central point.
Key creation

DEKs are generated by the storage system using Google's FIPS 140-2 validated cryptographic library. They are then protected by the storage system's KEK managed within Google's Internal KMS and kept with the data chunks. When a storage system needs to retrieve encrypted data, it retrieves the wrapped DEK and passes it to Google's Internal KMS. Google's Internal KMS then verifies that this service is authorized to use the KEK, and if so, unwraps and returns the plaintext DEK to the service. The service then uses the DEK to decrypt the data chunk into plaintext and verify its integrity.

Most KEKs for encrypting data chunks are generated within Google's Internal KMS, and the rest are generated inside the storage services. For consistency, all KEKs are generated using Google's FIPS 140-2 validated cryptographic library, using a random number generator (RNG) built by Google. This RNG is based on NIST 800-90A standards and generates an 256-bit random key encryption key (KEK) to be used with AES-256. This RNG is seeded from the Linux kernel's RNG, which in turn is seeded from multiple independent entropy sources. This includes entropic events from the data center environment, such as fine-grained measurements of disk seeks and inter-packet arrival times, and Intel's RDRAND instruction where it is available (on Ivy Bridge and newer CPUs).

Data stored in Google Cloud Platform is encrypted with DEKs using AES-256 or AES-128, as described above; and any new data encrypted in persistent disks in Google Compute Engine is encrypted using AES-256. DEKs are wrapped with KEKs using AES-256 or AES-128, depending on the Google Cloud Platform service.
Key rotation

Google's Internal KMS manages KEKs, and was built solely for this purpose. It was designed with security in mind. KEKs are not exportable from Google's Internal KMS by design; all encryption and decryption with these keys must be done within Google's Internal KMS. This helps prevent leaks and misuse, and enables Google's Internal KMS to record an audit trail when keys are used. Google's Internal KMS can automatically rotate KEKs at regular time intervals, using Google's common cryptographic library to generate new keys. Though we often refer to just a single key, we really mean that data is protected using a key set: one key active for encryption and a set of historical keys for decryption, the number of which is determined by the key rotation schedule. The actual rotation schedule for a KEK varies by service, but the standard rotation period is 90 days. Google Cloud Storage specifically rotates its KEKs every 90 days, and can store up to 20 versions, requiring re-encryption at least once every 5 years (though in practice, re-encryption is much more frequent). Keys held by Google's Internal KMS are backed up for disaster recovery purposes, and they are indefinitely recoverable.

Encryption implementations

Google provides many options for you to control encryption key management and, by association, control over access to decrypted data. As anyone who manages these services will acknowledge, it is important to understand the nuances of each of these options when selecting a data management strategy in the Cloud. The options you select here can also influence your posture with respect to Google's ability to access plaintext data.
Cloud Key Management Service and Cloud hardware security module service

Cloud Key Management Service (Cloud KMS) is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services. You can generate, use, rotate, and destroy cryptographic keys suitable to perform AES-256, RSA 2048, RSA 3072, RSA 4096, EC P-256, and EC P-384 operations. Cloud KMS is integrated with Cloud IAM and Cloud Audit Logging so that you can manage permissions on individual keys and monitor how these are used. Cloud KMS can be used to protect secrets and other sensitive data that you need to store in Google Cloud Platform.

Learn more about Cloud KMS\textsuperscript{10} and secrets management.\textsuperscript{11}

Cloud HSM is a cloud-hosted hardware security module (HSM) service on Google Cloud Platform. With Cloud HSM, you can manage encryption keys and perform cryptographic operations in FIPS 140-2 Level 3 validated HSMs. With this fully managed service, you can protect your most sensitive workloads without the need to worry about the operational overhead of managing an HSM cluster. With Cloud HSM, the keys that you create and use cannot be materialized outside of the HSMs specified at the time of key creation. Using Cloud HSM, you can verifiably attest that your cryptographic keys are created and used exclusively within a hardware device. Cloud HSM service is fully integrated with Cloud Key Management Service (KMS), which allows you to easily create and use customer-managed encryption keys (CMEK) that are generated and protected by a FIPS 140-2 Level 3 hardware device.

Learn more about Cloud HSM.\textsuperscript{12}

Cloud KMS key deletion

Data is also deleted through cryptographic erasure. This is an industry standard technique that renders data unreadable by deleting the encryption keys that are needed to decrypt that data.

Similar to deletion from Google’s active systems, deleted data is eliminated from backup systems using both overwriting and cryptographic techniques within 180 days.

Learn more about data\textsuperscript{13} and key deletion\textsuperscript{14} on Google Cloud Platform

\textsuperscript{10} Page 11, Cloud Key Management Service
\textsuperscript{11} Page 11, Secrets management
\textsuperscript{12} Page 11, Cloud HSM
\textsuperscript{13} Page 11, Data deletion on Google Cloud Platform
\textsuperscript{14} Page 11, Destroying and restoring key versions
Google-managed encryption keys

Google Cloud Platform always encrypts your data on the server side, before it is stored on disk, at no additional charge. This default encryption system manages server-side encryption keys on your behalf using the hardened key management systems that we use for our own encrypted data, including strict key access controls and auditing. Google Cloud Platform encrypts user data at rest using FIPS 140-2 validated AES. There is no setup or configuration required, no need to modify the way you access the service, and no visible performance impact. Data is automatically and transparently decrypted when read by an authorized user.

To protect your data as it travels over the Internet during read and write operations for HTTPS and gRPC requests, Google uses Transport Layer Security, commonly known as TLS.

Learn more about Google-managed encryption.15

Implications for government data requests

If your data is only encrypted by Google Managed Keys and not by you, Google may be forced to decrypt the data with a valid court order.

15 Page 12, Encryption at Rest in Google Cloud Platform
Customer-managed encryption keys (CMEK)

In addition to Google-managed encryption keys, you can choose to use keys generated by Cloud Key Management Service and managed by you. Such keys are known as customer-managed encryption keys. If you use a customer-managed encryption key, your encryption keys are stored within Cloud KMS, including optionally protected by the FIPS 140-2 level 3 HSMs of Cloud HSM.

When you protect your data with CMEK, you grant permission so the storage system that hosts the data can make use of the corresponding KMS decryption key. Protecting an object with a CMEK key does not disable standard read paths for any entity with sufficient permissions.

Services supporting customer-managed encryption keys
- Google Cloud Storage (GCS)
- Google Compute Engine (GCE)
- BigQuery
- Dataproc
- Container Registry

Learn more about Customer-managed encryption keys and supported services.

Implications for government data requests

If you no longer want Google to have access to your keys, you can request your keys to be deleted. Once the keys are deleted, Google will no longer be able to decrypt any data encrypted with that key version. Deleting keys in Google Cloud Platform follows the standard deletion time frames indicated in the published data deletion whitepaper.

Learn more about deleting key versions.
Customer-supplied encryption keys (CSEK)

With Customer-supplied encryption keys, you can choose to provide your own 256-bit key. This key is known as a customer-supplied encryption key. If you provide a customer-supplied encryption key, Google does not permanently store your key on Google's servers or otherwise manage your key. Instead, you provide your key for each operation, and your key is purged from Google's servers after the operation is complete. For Cloud Storage, we store only a cryptographic hash of the key so that future requests can be validated against the hash. Your key cannot be recovered from this hash, and the hash cannot be used to decrypt your data.

Services supporting customer-supplied encryption keys:

**Google Cloud Storage (GCS)**

When you use a customer-supplied encryption key and work directly with the JSON20 or XML21 API, you must provide both the AES-256 key and a SHA256 hash of the key. You should store both the key and the SHA256 hash of the key securely. Google stores the SHA256 hash of your key in the object's metadata, where you can retrieve it later. This SHA256 hash cannot be used by Google (or anyone else) to decrypt your data. It is stored as a way to uniquely identify the AES-256 key that was used to encrypt a particular object.

Learn more about customer-supplied encryption keys.22

**Google Compute Engine**

If you provide your own encryption keys, Compute Engine uses your key to protect the Google-generated keys used to encrypt and decrypt your data. Only users who can provide the correct key can use resources protected by a customer-supplied encryption key.

Learn more about customer-supplied encryption keys and how to use them.23

Implications for government data requests

Where Google does not have ongoing access to the keys we would produce ciphertext in response to a request for stored data encrypted with a customer-supplied key.

Learn more about customer-supplied encryption keys and how to use them.23

---

20 Page 14, Cloud Storage JSON API overview
21 Page 14, XML API overview
22 Page 14, Customer-supplied encryption keys
23 Page 14, Using Customer-Supplied Encryption Keys
Client-side encryption

With client-side encryption (CSE), you encrypt the data before Google has access to it. Google has no access to the keys. Third party products exist to facilitate this approach, but they limit all cloud-enabled functionality since the Google Servers don’t have access to the plaintext content.

Services supporting client-side encryption keys:

---

**Google Cloud Storage (GCS)**

You may use any encryption method to encrypt their data before sending it to GCS. Data that you encrypt on the client side arrives at Cloud Storage in an encrypted state. Cloud Storage has no access to or copies of the keys used to encrypt the data. See [best practices](#) for uploading and downloading your data for additional details.

---

**Gmail and Drive**

You can encrypt content for Gmail and Drive before it gets to the Google cloud servers by using existing third party solutions. These solutions integrate into the Gmail and Drive web clients and encrypt the content on the users device, such that unencrypted content is not accessible to Google servers. Use of these solutions disables all the cloud-enabled features like search and security assessments such as spam, malware, phishing, etc. Gmail and Drive servers have no access to or copies of the keys used to encrypt the data.

Learn more about [client-side encryption for GCP](#).

---

Implications for government data requests

The encryption keys are never sent to Google and all data is in ciphertext at all times, therefore Google would only produce ciphertext in response to a request for client-side encrypted data.

---

24 Page 15, Best practices for Cloud Storage
25 Page 15, Client-side encryption keys
Conclusion

Google Cloud is committed to earning customer trust via a number of features and products that provide you with transparency and control over your data. We have respect for the privacy and security of data you store with Google and when we receive a request, our team reviews it to make sure it satisfies legal requirements and Google's policies. If we believe a request is overly broad, we'll seek to narrow it. We will also always notify a customer of a request for data before disclosure, except in emergency situations involving a threat to life or when we are legally prohibited from doing so. Google has a trained team dedicated to these efforts.

With the rapid pace of innovation on the Internet and in cloud computing, Google recognizes that legally-sound policies and a strong understanding of international governance are a prerequisite to offering cloud computing services. This is why we advocate in favor of protecting our customers’ privacy and security in the cloud, and ensure we have the controls in place for you to feel confident in using our services.
Appendix: URLs

Page 4
Transparency report: https://transparencyreport.google.com/user-data/overview

Page 5
Seeking Enterprise Customer Data Held by Cloud Service Providers:
https://www.justice.gov/criminal-ccips/file/1017511/download
Promoting Public Safety, Privacy and the Rule of Law Around the World:

Page 6
Access Transparency: https://cloud.google.com/logging/docs/audit/access-transparency-overview
Use Access Transparency to report Google access:
https://support.google.com/a/answer/9230474?hl=en&ref_topic=9230579
Access Approval documentation: https://cloud.google.com/access-approval/docs/

Page 7
Encryption at Rest in Google Cloud Platform:
https://cloud.google.com/security/encryption-at-rest/default-encryption/
Encryption in Transit in Google Cloud:

Page 9
Intel® Digital Random Number Generator (DRNG) Software Implementation Guide:
Page 11
Cloud Key Management Service: https://cloud.google.com/kms/
Secrets management: https://cloud.google.com/solutions/secrets-management/
Cloud HSM: https://cloud.google.com/kms/docs/hsm
Data deletion on Google Cloud Platform: https://cloud.google.com/security/deletion/
Destroying and restoring key versions: https://cloud.google.com/kms/docs/destroy-restore

Page 12
Encryption at Rest in Google Cloud Platform:
https://cloud.google.com/security/encryption-at-rest/default-encryption/

Page 13
Google-managed encryption keys: https://cloud.google.com/storage/docs/encryption/default-keys
Customer-managed encryption keys:
https://cloud.google.com/storage/docs/encryption/customer-managed-keys
Data deletion on Google Cloud Platform: https://cloud.google.com/security/deletion/
Destroying and restoring key versions: https://cloud.google.com/kms/docs/destroy-restore

Page 14
Cloud Storage JSON API overview: https://cloud.google.com/storage/docs/json_api/
XML API overview: https://cloud.google.com/storage/docs/xml-api/overview
Customer-supplied encryption keys:
Using customer-supplied encryption keys:
https://cloud.google.com/storage/docs/encryption/using-customer-supplied-keys

Page 15
Best practices for Cloud Storage: https://cloud.google.com/storage/docs/best-practices#uploading
Client-side encryption keys: https://cloud.google.com/storage/docs/encryption/client-side-keys