Google Cloud Whitepaper
February 2022

Government Requests for Cloud Customer Data

Table of Contents

Disclaimer

The content contained herein is correct as of February 2022 and represents the status quo as of the time it was written. Google Cloud's policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

At Google, we know that transparency plays a critical role in earning and maintaining customer trust. That is why Google Cloud has taken steps to develop industry-leading product capabilities that enhance the control that our customers have over their data, and that give customers visibility into when and how their data is accessed. We think it is important to be clear at the outset about where we stand: our customers own their data and have the right to control access to it.

Like other technology and communication companies, Google receives requests from governments and courts around the world for customer information, including requests for Google Cloud customer information. Google Cloud has developed a transparent, fair, and thorough process that meets international best practices when it comes to data access requests from law enforcement agencies and governments. Google provides a response on a case-by-case basis, taking into account different circumstances and informed by legal requirements, customer agreements, and privacy policies. We are committed to protecting privacy while also complying with applicable laws.

Google was the first cloud provider to publish regular transparency reports on government requests for customer information, as well as requests for Google to remove content from publication. While greater transparency can increase customer trust, it also helps in public policy discussions about the appropriate scope and authority of government requests.

The purpose of this whitepaper is to describe Google's practices around government requests for customer information. This whitepaper should not be considered as legal advice. If you are seeking legal advice, please consult your attorney.

Government requests for Cloud customer information

What is a government request for customer information?

Like many technology companies, Google receives requests from governments and courts to disclose customer information. Most requests are issued in the context of criminal investigations, but government agencies may also request information in the context of civil or administrative cases.

Most governments have created legal means to request data from communications services providers. These requests can be for information about the use of our services, such as when an end user signed into their account, or for information about the content that is stored with Google, such as a request for an end user's email messages. In the U.S., the Electronic Communications Privacy Act (ECPA) regulates how a U.S. government agency can compel companies like Google to disclose customer information. ECPA sets forth the type of legal process the U.S. government must use to compel the production of different types of information, ranging from a subpoena for basic subscriber information, to a search warrant for the content of communications. ECPA places more restrictions on the U.S. government's ability to obtain data from service providers than the laws of most other countries. More information about ECPA can be found in the legal process section of our transparency report.[1]

Governments outside of the U.S. also submit requests for disclosure of customer information, and many countries have laws that govern the parameters of such disclosures. The European Commission has put forth an e-Evidence proposal that, analogous to the ECPA, imposes procedural requirements and safeguards around requests for electronic information by law enforcement and judicial authorities.

We believe that our customers should have confidence that government requests of any nature will be subject to a transparent legal framework that requires government agencies to first seek data directly from customers and guarantees due process for customers and service providers.

[1] Information about the collection of data for national security investigations by the U.S. is also provided in our United States National Security Requests FAQs.

The CLOUD Act

Overview of the CLOUD Act

The Clarifying Lawful Overseas Use of Data Act, also known as the CLOUD Act, is a 2018 amendment to the Stored Communications Act (SCA). The CLOUD Act:

- ***Does*** create a mechanism by which a qualifying foreign government may enter into an executive agreement with the U.S., provided that the qualifying foreign government meets baseline privacy, due process, and human rights standards in the CLOUD Act;
- ***Does not*** extend the U.S. government's authority to obtain user data in criminal investigations with lawful legal process when it has jurisdiction;
- ***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;
- ***Does not*** modify the DOJ's policy that prosecutors should request data from cloud customers directly, not from the customer's provider; and
- ***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, Google not only maintains strict standards for government disclosure requests but also has developed products and services 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.

In addition, cloud providers can challenge a U.S. government data request on the basis of conflict of law related to a qualifying foreign government, provided the foreign government's law allows for a reciprocal right to challenge in the event of a request that conflicts with U.S. law. CLOUD Act requests are reviewed by Google according to the same guidelines outlined in our How Google responds to government requests for Cloud customer information section.

As a final point, the CLOUD Act clarifies that the U.S. government can compel production of data where the data is under the "possession, custody, or control" of a provider subject to US jurisdiction, regardless of where that data is physically stored. In other words, data localization requirements do not impact whether a cloud provider may have to disclose data in response to a government request. Regardless, for customers that seek to store their data at rest in certain locations due to company-specific policies, Google Cloud does offer data residency solutions. In addition, we provide state-of-the art encryption products that allow customer data to remain unusable and unreadable as text even if Google is compelled to turn over the data. Both of these are described in the Security section below.

Executive Agreements under the CLOUD Act

Before the CLOUD Act, in most cases foreign governments could only obtain communications content from U.S. providers through diplomatic procedures with the United States. The CLOUD Act allows Google, in certain circumstances, to disclose customer data directly to qualifying foreign governments

pursuant to a CLOUD Act data request.[2]

We use the term *CLOUD Act request* in this whitepaper to refer to a request for customer information issued by a qualifying foreign government pursuant to an executive agreement under the CLOUD Act. Qualifying foreign governments are those that meet baseline privacy, due process, and human rights standards in the CLOUD Act. For example, the United Kingdom and Australia have both entered into CLOUD Act agreements with the U.S., although neither agreement has entered into force at the time of this writing. The term *CLOUD Act request* in this whitepaper does not include requests issued by the U.S. government based on pre-existing authorities to issue a demand to a U.S. based service provider for records in its possession, custody, or control, which will generally be referred to as a U.S. request.

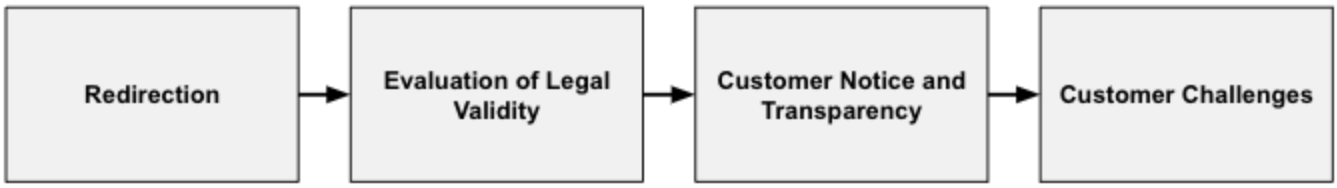
Other customer requirements

We recognize that our customers may seek information on the applicability and relevance of other US and global requirements to their Cloud customer data. For resources on Schrems II, EO 12333, and FISA 702, please consult our whitepaper. For resources on Google Cloud Standard Contractual Clauses (SCCs), please see our whitepaper. For any other requirements, please review our Privacy Resource Center and Compliance Resource Center.

[2] Such a request will be subject to review by Google according to the review guidelines outlined below.

How Google responds to government requests for Cloud customer information

Google has robust operational policies and procedures and other organizational measures in place to protect against unlawful or excessive requests for user data by public authorities. Our approach to government requests for information, regardless of the type of request, follows the same steps unless prohibited by or unreasonable under the applicable laws.



1. **Redirection**: If Google receives a request from a government agency for Cloud customer data, Google informs the government that it should issue the request directly to the organization in question. This approach is aligned with U.S. government policy and our contractual commitments.

2. **Evaluation of Legal Validity**: 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, proportionate, and satisfies Google's policies. Google maintains a dedicated, specialist, and cross-functional team to evaluate and process requests for user data while upholding the law and protecting users' privacy and security. All requests for user data must be processed and approved by team members before any data is made available. Training and support from legal counsel equips the relevant employees with the necessary skills to evaluate the validity of the legal process and ensure that all requests are handled in accordance with both the law and Google's policies and procedures. Furthermore, we object to, or limit or modify, any legal process that we reasonably determine to be overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful.

3. **Customer Notice and Transparency**: We will notify the customer before their customer data is disclosed unless such notification is prohibited by law, could obstruct a government investigation, or lead to death or serious physical harm to an individual. Where prior notification by Google is prohibited under applicable law, it is Google's policy to notify the customer when any prohibition is eventually 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.

4. **Customer Challenges**: 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 for customer data and the customer subsequently files an objection to disclosure with an appropriate tribunal and provides a copy of the objection to Google, Google will not provide the data in response to the request and hold it in escrow if legally permissible through the pendency of a customer challenge.

Google's commitment to transparency, advocacy, and security

Transparency

Google is committed to building trust through transparency about government requests for customer information. As stated in the How Google responds to government requests for information section, Google has robust policies and procedures and organizational measures in place to ensure transparent handling and protection of customer data. We also publish a Transparency Report, where we share our data about how the policies and actions of governments and corporations affect privacy, security, and access to information.

In our reports on requests for user information, we disclose, where permitted by applicable laws, the number of requests made globally by law enforcement agencies and government bodies for Cloud customer information. For all requests, we apply the procedures described above.

- For global requests, we report the number of requests made by governments for user information, and the number of accounts subject to those requests. These requests do not include U.S. national security requests.
- For enterprise requests, we provide additional details on a subset of those requests that involve Enterprise Cloud customers. As a subset of our global requests, these enterprise requests do not include U.S. national security requests.
- For U.S. national security requests, we separately report requests from U.S. authorities using national security laws because these laws restrict how much information companies like us are allowed to share, and when we are allowed to share it. More information can be found in our United States National Security Requests FAQs.

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 data being affected by these types of requests is low.

Google has designed and built custom tools to manage requests for user data in a consistent, secure and auditable manner. Strict access control measures apply to ensure that only authorized members of Google's legal team can access these tools, and all use is logged and susceptible to audit. As part of this tooling, Google maintains a Law Enforcement Request System (LERS) to allow public authorities to request user data, track request status and - where appropriate - securely receive responsive user data.

Google also challenges user data requests in court where appropriate. Google is an active advocate for legislative reform to improve the safeguards that apply to government requests for user data in the U.S. and around the world.

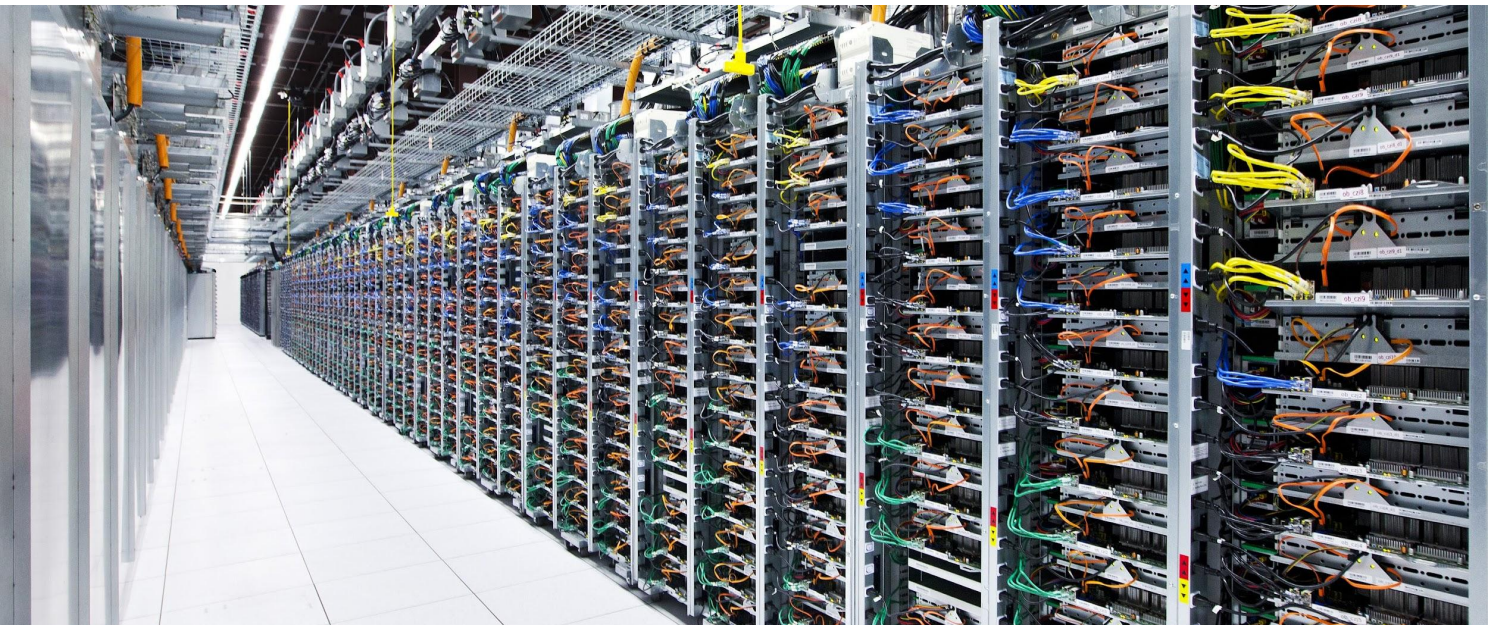
Advocacy

Google is continuing its efforts to support regulatory and legal reforms that promote customers' ability to safeguard their data. Government engagement on a bilateral basis and in multilateral forums is critical for modernizing laws and establishing rules governing compelling the production of electronic evidence across borders in a manner that respects international norms and sovereignty. Customers should have a right to know when governments seek disclosure of their information and the public should understand how often governments are making these requests. Governments should support transparency efforts by providers and put forward their own transparency initiatives to ensure that administrative powers are being used responsibly. Google has supported these efforts and will continue to do so, including resolving potential conflicts of law and protecting the privacy and security of our customers.

Google is a member of the Trusted Cloud Initiative, which commits to working with governments to ensure the free flow of data, to promote public safety, and to protect privacy and data security in the cloud. We support laws that allow governments to request data through a transparent process and support improved rules and regulations at the national and international levels that protect the safety, privacy, and security of cloud customers and their ownership of data. As the Trusted Cloud Principles state, governments should engage customers first and cloud providers should have a right to protect customers' interests.

Google is also a member of the Global Network Initiative (GNI), a non-governmental organization that advocates for expanded transparency, oversight, and accountability of laws, regulations, and actions related to communications surveillance. As a member, we commit to implementing a framework of principles and guidelines (the GNI Principles) on addressing government demands for access to data in a manner consistent with internationally recognised laws and standards. As a GNI member, Google is independently assessed every two years on its practices and progress in implementing the GNI Principles.

Google has also demonstrated a commitment to protect customer data. In early 2019 we filed a legal challenge to protect a customer's right to know when its data is accessed, in a case that was partially unsealed by the United States Court of Appeals for the Second Circuit. Our lawsuit challenged two gag orders that restricted our right to speak about the U.S. Government's request to access enterprise customers' data for a criminal investigation. It builds on our support for litigation to oppose indefinite non-disclosure orders. While there are valid reasons for governments to request access to data, it is also important to be transparent with customers about these requests.



Security

Google is dedicated to continuing innovation efforts 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. We believe that customers should have the strongest levels 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 Controls and Transparency

- **Customer Authorization:** BeyondCorp Enterprise for GCP provides user and device-based authentication and authorization for Google Cloud resources.
- **Access Transparency:** Access Transparency for GCP and Workspace is available for customers to review logs of actions taken by Google staff when accessing certain customer data as permitted by law.
- **Access Approval:** GCP customers can use Access Approval to explicitly approve access to their data or configurations on Google Cloud.
- **Context Aware:** Google Workspace customers can use Context-Aware Access[3] to create granular access control policies to apps based on attributes such as user, location, device security status, and IP address.

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

Encryption

- **Encryption in Transit:** Google Cloud enforces encryption in transit by default using FIPS 140-2 validated cryptographic modules to encrypt all inter-region traffic.
- **Encryption at Rest:** GCP and Google Workspace offer encryption at rest by default.
- **Encryption in Use:** In GCP, we offer customer-configurable controls to encrypt and protect data in-use in virtual machine (VM) and kubernetes nodes (GKE) memory.
- **Application Layer Transport Security:** 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. We believe increased adoption of TLS is so important for the industry that we report TLS progress in our Email Encryption Transparency Report.

Cryptographic key management

GCP 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.
- 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.

Enhanced customer controls

- **Cloud External Key Manager** (Cloud EKM): Cloud EKM allows customers to store and manage encryption keys outside of Google Cloud infrastructure, supporting mandates requiring key separation from data.
- **Key Access Justifications:** Key Access Justifications works with Cloud EKM and provides customers visibility into requests for encryption keys, a justification for that request, and a mechanism to explicitly approve or deny decryption using the key in the context of that request. This means there is no way for Google to decrypt customer data at rest without customer approval, which you can withhold for any reason.
- **Confidential Computing:** Confidential Computing is technology that allows you to encrypt data in the cloud while it's being processed.
- **Client-Side Encryption:** Google Workspace client-side encryption is currently available for Google Drive, Docs, Sheets, and Slides.
- **Data residency:** For GCP, our compute and storage key services allow customers to store customer data at rest exclusively in specific regions. For GCP's data location commitments, please see our GCP Service Specific Terms. Data regions for Google Workspace provides customer control over the geographical location for storage of email messages, documents, and other Google Workspace content.[4] For Google Workspace's data location commitments, please see our Google Workspace Service Specific Terms. These offerings may satisfy company-specific policies around locating data at rest.

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

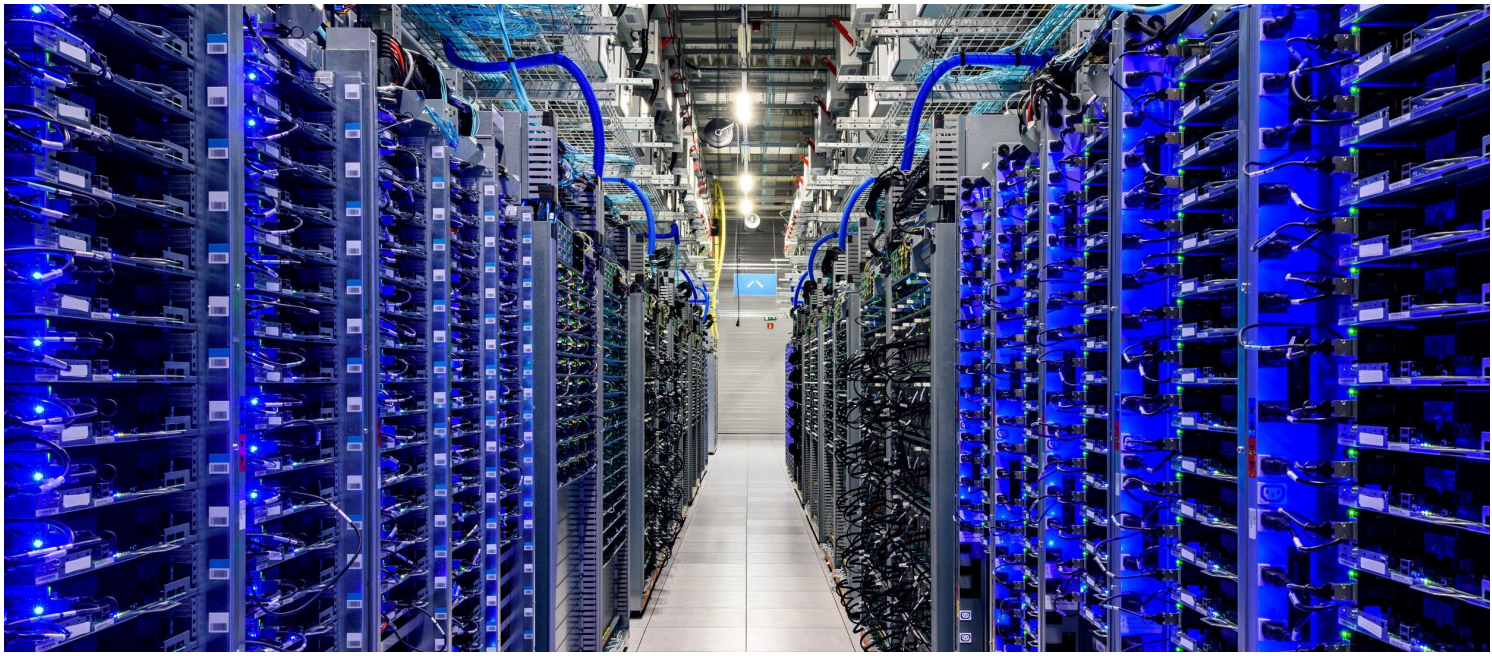
- **Assured Workloads**: For GCP, Assured Workloads provides Google Cloud customers with the ability to apply and enforce security controls to an environment in support of compliance requirements such as data residency and encryption.

More detailed information on the above mentioned products and tools can be found in our Safeguards for international data transfers with Google Cloud whitepaper, as well as our GCP product pages and Google Workspace product and security and trust pages. For the latest Google Cloud product announcements, please see our Blog.

Conclusion

Google takes the security and privacy of its customers very seriously. To this end, we will continue to innovate to provide customers with even better controls[5] to protect the security and privacy of their information, and improve transparency to help address broader uncertainty about how governments request access to enterprise customer data. Furthermore, we will continue to advocate with governments to help drive forward policies that protect our customers' data. Google has supported these efforts and will continue to do so—including resolving potential conflicts of law and promoting transparency to ensure that administrative powers are being used responsibly.

For more information on how we protect your business's data, please visit https://privacy.google.com/businesses/. For more information on the security and privacy of data in Google Cloud, please visit https://cloud.google.com/security/transparency/govt-requests/.



[5] See recent announcements here and here.