Google Cloud Whitepaper
December 2022

Trusting your data with Google Cloud

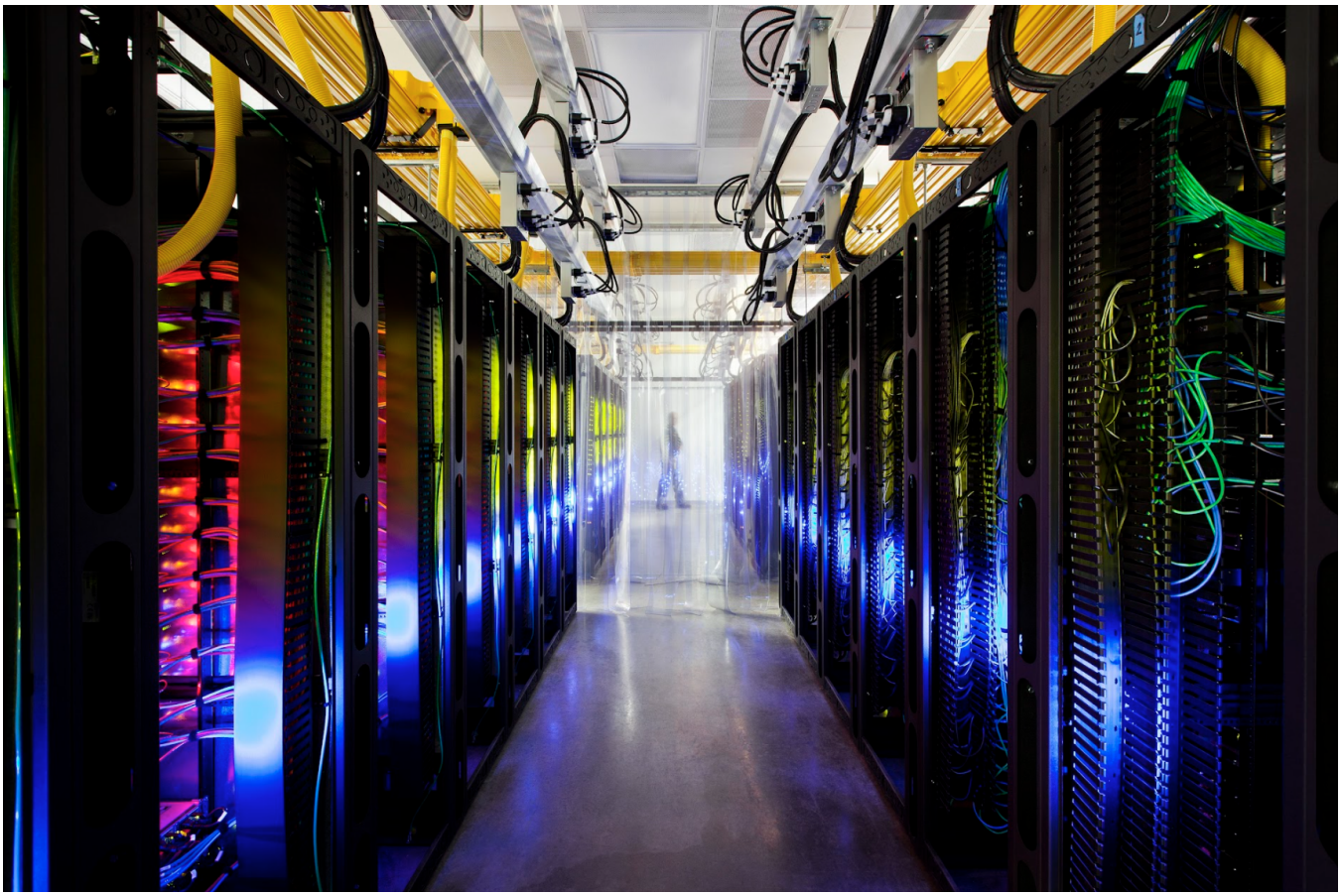


Table of Contents

1. Introduction 3
2. Managing your data on Google Cloud 5
2.1 Data Usage 5
2.2 Data Availability and Resilience 6
2.3 Data Governance 7
2.4 Data Residency 9
2.5 Security Configuration Management 9
2.6 Third Party Security Solutions 9
2.7 Incident Detection & Response 10
2.8 Business Continuity (BC) and Disaster Recovery (DR) 10
2.9 Interoperability and Portability 11
3. Safeguarding access to your data 12
3.1 Access control for Google Cloud 12
3.2 Customer controls over Google access to data 13
3.3 Google employee access authorization 14
3.4 Organizational safeguards 15
3.4.1 Transparency 15
3.4.2 Use of subprocessors 15
3.4.3 Government requests for data 16
4. Security and compliance standards 16
4.1 Independent verification of our control framework 16
4.2 Compliance support for customers 17
5. Conclusion 18

Disclaimer

This whitepaper applies to Google Cloud products described in the Google Cloud Services Summary. The content contained herein is correct as of December 2022 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

1. Introduction

At Google Cloud, we've set a high bar for what it means to host, serve, and protect our customers' data. Security and data protection are at the core values of how we design and build our products. We start from the fundamental premise that Google Cloud customers own their data and control how it is used. The customer data stored and managed on Google Cloud is processed per your instructions in accordance with the Cloud Data Processing Addendum (CDPA) and for no other purpose. Not for advertising, not for anything else. Our Google Cloud Trust Principles summarize our commitment to protecting the privacy of data stored by customers in Google Cloud.

This whitepaper provides details on how we provide customers with transparency and control over their data in Google Cloud. Google Cloud offers built-in data protection at scale, by default, designed to protect your business from intrusions, theft and attacks. In addition to continuous security monitoring for external threats, we explain the robust controls and auditing in place to protect against insider access to customer data. These include providing customers with near real-time logs of Google administrator access to customer configurations or data via Access Transparency logs. If you'd like to learn more about how we define customer data, please refer to our Cloud Terms of Service.

Google Cloud products regularly undergo independent, third-party audits and certifications to verify that our data protection practices match our controls and commitments. An overview of our key compliance reports and certifications, as well as how we support our customers with their compliance journey is also provided in this paper. Lastly, Google participates in such declarations as the EU Cloud Code of Conduct to further evidence to our customers our commitments to accountability, compliance support, and robust data protection principles.

While this whitepaper provides information on the tools and resources offered by Google Cloud, please note that, as a provider of cloud services, we are not in a position to provide our customers with legal advice - that is something only legal counsel can provide.

2. Managing your data on Google Cloud

This section describes the data lifecycle in Google Cloud through the lens of security and privacy.

2.1 Data Usage

Reading and writing data to and from Google Cloud involves transferring data outside of Google Cloud's controllable boundaries. Depending on the connection, Google Cloud enables encryption in transit by default, encrypting requests before transmission and protecting the raw data using the Transport Layer Security (TLS) protocol. Google's Application Layer Transport Security is a mutual authentication and transport encryption system developed by Google and used for securing Remote Procedure Call (RPC) communications within Google's infrastructure. More information on the subject of encryption in transit to and from Google Cloud can be found in our paper on Application Layer Transport Security in Google Cloud.

Once data is transferred to Google Cloud to be stored, Google Cloud applies encryption at rest by default at the storage level using AES256. Google Cloud customers looking to gain more control over how data is encrypted at rest may use our Cloud Key Management Service (KMS) to generate, use, rotate, and destroy encryption keys according to their own policies. We refer to this process as customer-managed encryption keys (CMEK). With CMEK, customers can use keys that they manage to protect data within Google Cloud. Customers can protect data at rest in supported CMEK integration services, or by calling the Cloud Key Management Service API directly.

To gain even more control, Google Cloud customers can implement Cloud External Key Manager (Cloud EKM) for supported services. With Cloud EKM, Google Cloud customers are able to maintain possession of their encryption keys, or use an approved external key management partner, and to mandate key separation from data. It also 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 Identity and Access Management (IAM) helps customers to define fine-grained access policies and precisely control access to Google Cloud-hosted data.

To help mitigate risks such as the misconfiguration of employee access controls or attackers taking advantage of compromised accounts, VPC Service Controls enables customers to define security perimeters around Google Cloud resources, such as Cloud Storage or BigQuery, to prevent data exfiltration. Identity-Aware Proxy (IAP) enables customers to control access to cloud applications and VMs based not only on the user's identity, but on the context of their request, such as device security status.

Enterprises storing data in the Cloud also seek **visibility into data access**. Cloud Audit Logs record the actions that members of your Google Cloud organization have taken in your Google Cloud resources. This is different from Access Transparency logs which record the actions taken by Google personnel.

Customers may also seek control over the deletion of data. Customers can use a variety of methods in the Cloud Console and via Google Cloud APIs to delete data. Google's deletion pipeline begins by confirming the deletion request and eliminating the data iteratively from application and storage layers, from both active and backup storage systems. In addition, our media sanitization program enhances the security of the deletion process by preventing forensic or laboratory attacks on the physical storage media once it has reached the end of its life cycle. For more information, please see our Data Deletion paper.

2.2 Data Availability and Resilience

Our data centers and network architecture are designed for maximum reliability and uptime. Google's computing platform assumes ongoing hardware failure, and it uses robust software failover to withstand disruption. Furthermore, Google engineers proactively identify dependencies in their systems and redesign to eliminate them. Data is replicated multiple times across Google's clustered servers so that, in the case of a machine failure, data will still be accessible through another system. Customer workloads are securely distributed across multiple regions, availability zones, points of presence, and network cables to provide strong built-in redundancy and application availability.

Google runs one of the largest private networks in existence, minimizing risk for customers. This fully software-defined network allows us to scale reliably, providing our customers consistent service 24/7/365. Some infrastructure and solutions that support consistency of service:

- 3 zone minimum per region for resiliency
- Multi-Region replication and failover
- Zero planned downtime with Live Migration
- 24/7/365 world class monitoring and detection with full transparency
- Application service deployment trust mechanisms, built for multi-tenant service from inception
- Hardened physical premises with purpose-built servers and custom security chips

- Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products such as natural disasters and local outages.

- The Google backbone network uses advanced software-defined networking, and has edge-caching services to deliver fast, consistent, and scalable performance (one of the largest backbone networks in the world).

- Google's redundant and fault tolerant infrastructure assumes a high probability of failure. Every hardware component in the critical path of a service is replicated so that a single component or system failure cannot bring down a service. This includes network switches, routers, cables, external fiber connectivity, racks, machines, storage, and many other components.

- Proprietary hardware allows us to build ahead of demand and respond to peaks (e.g., COVID-19 traffic surge).

- Automatic failover in the event of failure
  - Platform services and control planes automatically and instantly shift from one facility to another
  - Google Cloud services maintain high levels of availability (the committed services uptime in our SLAs - Google Cloud)
  - You have live visibility into service status and outages - Google Cloud

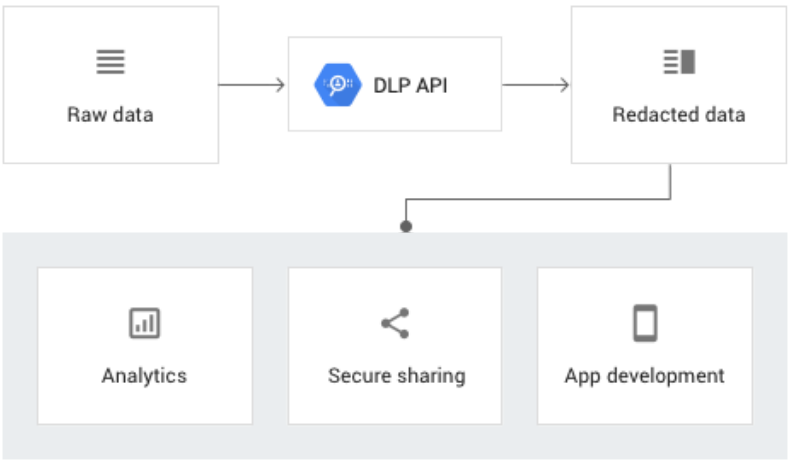
Additionally, Google runs annual, company-wide, multi-day Disaster Recovery Testing events (DiRT) to ensure that Google's services and internal business operations continue to run during a disaster. DiRT was developed to find vulnerabilities in critical systems by intentionally causing failures, and to fix those vulnerabilities before failures happen in an uncontrolled manner. DiRT tests Google's technical robustness by breaking live systems and tests our operational resilience by explicitly preventing critical personnel, area experts, and leaders from participating. All generally available services are required to have ongoing, active DiRT testing and validation of their resilience and availability.

2.3 Data Governance

Enterprises operating in certain countries and/or regulated industries, such as Healthcare and Financial Services, may be **required to meet certain compliance obligations**, including HIPAA, PCI DSS, GDPR, etc. Most organizations also have internal policies that dictate handling of sensitive data. The first step toward meeting requirements is understanding where customer data is stored.

Cloud Data Loss Prevention (DLP) helps customers to discover, classify, and de-identify data such as payment card numbers, national identification numbers, protected health information, and other types of personally-identifiable information (PII). DLP provides techniques such as pseudonymization, tokenization, bucketing, date-shifting, and more, which can help you de-risk structured and unstructured data.

For more details on these techniques, refer to our blog post: Take charge of your data: using Cloud DLP to de-identify and obfuscate sensitive information.



When customers use DLP to classify data, they can attach the data class and other business metadata (such as owner, quality, lineage) to the data via tagging. Google Cloud offers **tagging mechanisms** in multiple database and storage solutions, such as Cloud Storage, Data Catalog, BigQuery, Bigtable, Spanner, and more.

Cloud Data Catalog is a metadata management service that leverages tagging. Data Catalog simplifies data discovery, allowing search across an entire data warehouse. The search facilities from Data Catalog are enterprise access control enabled - meaning users cannot discover data they do not have permission to - as managed by Cloud IAM controls. Enterprises storing data in the cloud can benefit from Data Catalog's programmatic and scalable mechanism to associate data with meaningful tags to help meet **data retention policies** and mitigate **insider risk**.

Once data is classified, you can apply additional layers of security to protect sensitive data, including:

- Adjusting IAM permissions to finely tune the specific roles of users accessing the data, curating the right amount of access at the project, folder or dataset level.
- Applying VPC Service Controls policies to isolate services and enable context aware access which can take into account the user's identity and location before allowing access.
- Transforming it to remove or mask certain sensitive elements from the data.

To learn more, read our whitepaper, Principles and best practices for data governance in the cloud.

2.4 Data Residency

Customers who want to keep their data in a specified geographic location can take advantage of Google Cloud's data residency capabilities. Data residency services in Google Cloud allow the customer to store Customer Data at rest in their region of choice. For example, in the European Union, customers using data residency services can store customer data at rest exclusively in regions in Belgium, Germany, Finland, Poland, France, Italy, Spain, and the Netherlands, with other EU regions becoming available in the future.

Physical storage of data

For Google Cloud, our data residency services allow customers to store customer data at rest exclusively in specific regions. These offerings may satisfy company-specific policies around locating data at rest. Customers with data residency requirements can set up a Resource Locations organization policy that constrains the location of new resources for their whole organization or individual projects. With these capabilities, customers can prevent their employees from accidentally storing customer data in an unintended Google Cloud region.

Location-based access

Google Cloud 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 otherwise authorized. Cloud Armor also allows customers to restrict locations from which traffic is allowed to their external load balancer.

For more details on Google Cloud's data location commitments, please read our Service Specific Terms.

2.5 Security Configuration Management

To take full advantage of Google Cloud security products and services, customers have to manage multiple security policies and configurations, including managing account access using IAM, Google Cloud hosted services access using VPC Service Controls, sensitive data classification using Cloud DLP, and encryption keys using KMS. Config Validator helps customers to enforce constraints that validate whether deployments can be provisioned, enabling developers to operate within safe guardrails. Administrators can publish Config Validator's results to Security Command Center (SCC) to keep track of configuration violations over time.

2.6 Third Party Security Solutions

While Google Cloud provides a significant number of native capabilities to protect data, an enterprise may already employ or plan to adopt third-party security solutions. Google Cloud curates a robust and expanding Security Partner Ecosystem, composed of some of the most respected vendors in cloud security. Customers can take advantage of the security solutions offered by our partners to improve their security posture in areas such as data leakage prevention and endpoint protection.

In addition, many Google Cloud services facilitate the adoption of third-party products by allowing for:

- export of Cloud Audit Logs
- export of Security Command Center alerts and findings
- use of extensible markup language for automated application and enforcement of security policies

A full list of third-party security offerings for the Google Cloud environment is available in the Cloud Marketplace.

2.7 Incident Detection & Response

With multiple security and privacy controls in place, organizations **need a centralized location where they can prevent, detect, and respond to threats**. Security Command Center (SCC) gives customers centralized visibility into their cloud assets as well as built-in security analytics to assess their overall security posture. Google Cloud's tools help customers identify and respond to security incidents such as **malware**, **cryptomining**, **unauthorized access to Google Cloud resources**, **outgoing DDoS attacks**, **port scanning**, and **brute-force SSH attacks**. Event Threat Detection (ETD) automatically scans large volumes of Google Cloud logs for suspicious activity to help customers quickly detect high-risk security incidents. You can learn more about how Google detects and manages our own incidents in our Data incident response process whitepaper.

Google has also launched our Autonomic Security Operations solution. We define Autonomic Security Operations as a combination of philosophies, practices, and tools that improve an organization's ability to withstand security attacks through an adaptive, agile, and highly automated approach to threat

management. To support this transformation, we've created a solution stack to offer products, integrations, blueprints, content, an accelerator program, and preferred partners. We discuss Autonomic Security Operations further in this whitepaper.

2.8 Business Continuity (BC) and Disaster Recovery (DR)

Google Cloud has a robust, flexible, and cost-effective selection of products and features that customers can use to build or augment the solution that is right for them. These include a **global network**, **redundancy**, **scalability**, **security** and **compliance.** Customers can use Google Cloud services such as Shared VPC, Google Cloud firewalls, Cloud Deployment Manager, Anthos and Cloud Storage to design and build robust DR patterns that can meet their specific recovery time objectives (RTOs) and recovery point objectives (RPOs).

Additionally, Disaster Recovery Plans (DRP) have always been a priority for enterprises seeking to provide a consistent customer experience regardless of potential risks such as **natural disasters**, **hardware failure**, **human errors**, and **cyber crimes**. Google Cloud offers a number of data archive and backup features across its database and storage solutions, such as Bigtable's regional replication, BigQuery's long term storage, Datastore's managed export service, Cloud SQL's automated backup and recovery, Spanner's export, and Cloud Storage's nearline & coldline.

You can learn more about disaster recovery planning on Google Cloud in our DR scenarios planning guide.

2.9 Interoperability and Portability

Google is committed to an open cloud that enables our customers to set up the optimal solution, spanning on-premise and multiple clouds, without being locked into a single provider. We offer tools that operate across systems and vendors and allow you to monitor your system from a single place.

Anthos provides a single platform for multi-cloud management, allowing you to deploy applications across hybrid and multi-cloud without changing the underlying code. Anthos' full suite of features, including Migration and Configuration Management, enable you to migrate and modernize your VMs to your container and cloud provider of choice in one streamlined motion, without upfront modifications to the original VMs or applications. This means that you don't have to jump through hoops or learn a new language - you can run all your container workloads on one consistent platform. Anthos is also a 100% software solution that works on your existing hardware.

Our belief in an open cloud stems from our deep commitment to open source. We believe that open source is the future of public cloud: It's the foundation of IT infrastructure worldwide and has been a part of Google's foundation since day one. Google is the #1 contributor to the Cloud Native Computing Foundation, an open source development community, with 50%+ of code commits. This is reflected in our contributions to projects like Kubernetes, TensorFlow, Go, and many more. We believe customers should use us because they love us, not because they are locked in.

3. Safeguarding access to your data

At Google, protecting the sensitive data that customers and enterprises trust us with is a top priority. Our zero trust-based architecture and least privilege principles includes the industry's strongest authentication protocols, is highly resistant to data exfiltration, and deploys 24/7 advanced monitoring and analytics to restrict the misuse of credentials, detect abnormal employee activity, and automatically respond to new or evolving threats.

With a team of security and privacy experts and inventive software design, we built our least-privilege framework from the ground up, guided by the following principles:

- **Strong authentication and role-based, non-unilateral access restrictions**: By default Google personnel do not have access to Google Cloud customer data. Google personnel must be a member of relevant access control lists to gain access to sensitive data. In addition, personnel must read and acknowledge Google's data access policies regularly.To access the data, Google personnel must use a trusted device and multi-factor authentication via Security Keys, which also minimizes the risk of credentials being phished. From this trusted device, they are able to access tooling that evaluates the justification provided (ie. support ticket, issue ID, etc), the user's role and context to determine if they can obtain access to the customer data. Some tools will require Google personnel to obtain authorization from another qualified Googler to access the data.
- **End-to-end workload protection**: With Confidential VM, Google Cloud provides end-to-end encryption of customer workloads in select services and protect data from unauthorized access at rest, in transit, and in use.
- **Continuous logging and auditing**: Access to customer data is logged and intelligent threat detection systems conduct real-time audits, alerting staff when log entries match threat indicators. Internal security teams evaluate alerts and logs to identify and investigate anomalous activities, limiting the scope and impact of any incident. We discuss our incident response further in our data incident response process whitepaper..
- **Transparency and customer control**: Using Customer Managed Encryption Keys (CMEK) customers can manage or supply their own encryption keys, allowing them to revoke access to their data at any time. Access Transparency and Access Approval can be used with certain Google services as described further below.

3.1 Access control for Google Cloud

Google Cloud believes that customers should have a robust level of control over data stored in the cloud and we've developed product capabilities that enhance your control over your data and provide expanded visibility into when and how your data is accessed.

Google Cloud has implemented access 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, customers 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**: Google Cloud also offers Access Approval, which allows customers to explicitly approve access to customer data or configurations on Google Cloud. Additional information can be found in our Access Approval documentation.
- **Service authorization**: Google Cloud offers Google Binary Authorization services to validate and continue monitoring the provenance and integrity of the containers processing customer data. Binary Authorization is an integrated part of customers' deployment software supply chain and their CI/CD flow.
- **European Support**: Google Cloud has expanded its existing Assured Support offering to the EEA. Customers using Assured Workloads for EEA have the ability to obtain support from EEA Personnel only, ensuring that their issues are supported by local staff to help minimize the risk of customer data leaving the EEA while customers are receiving support. The capability extends to administrative and operational support, and this control ensures that system administration actions involving customer data are only performed by EEA personnel from an EEA location.

3.2 Customer controls over Google access to data

Google Cloud is explicit in its commitment to customers: **you own your data**, and we will never use it for any purpose other than those necessary to fulfill our contractual/legal obligations. We also know that in addition to commitments, customers want additional transparency and control from their cloud service provider. Google Cloud offers **industry-leading controls to prevent unauthorized access** by our support and engineering teams to your customer data.

Cloud External Key Manager and Key Access Justifications

Cloud EKM provides several benefits:

- **Key provenance**: The customer controls the location and distribution of the externally-managed keys. Externally-managed keys are never cached or stored within Google Cloud. Whenever Google Cloud needs to decrypt data, it communicates directly with the external key manager.
- **Access control**: The customer manages access to externally-managed keys. To use an externally-managed key to encrypt or decrypt data in Google Cloud, customers must grant the

Google Cloud project explicit access to use the key manager. The customer can revoke this access at any time.
- **Centralized key management**: The customer can manage the keys and access policies from a single location and user interface, whether the data they protect resides in the cloud or on the customer's premises.

In addition to Cloud EKM, customers may leverage Key Access Justifications to understand why their externally-hosted keys are being requested 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).

Additionally, the overall solution comes with an integrity commitment that gives customers confidence in the controls working as described. Learn more about Key Access Justifications and External Key Manager.

Confidential Computing

Confidential Computing 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. 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. Google does not have access to these encryption keys.

Google also provides customers with a ubiquitous data encryption solution. The solution provides customers with unified control over their data-at-rest, in-use, and in-transit with keys under their control. This makes it possible to seamlessly encrypt customer data as it is sent to the cloud, using the customer's external key management solution, in a way that only a confidential VM can decrypt and compute on it. In order to make sure the key can only be used in a confidential environment, we leverage confidential VM's attestation feature, and work with partners, including Thales.

3.3 Google employee access authorization

Google employees undergo background checks, are required to execute a confidentiality agreement, and comply with Google's code of conduct. In addition, we've designed our systems to **limit the number of employees that have access to customer data** and to **actively monitor** the activities of those employees.

Google employees are only granted a **limited set of default permissions** to access company resources. Access to internal support tools is controlled via **Access Control Lists (ACLs)**. Google follows a formal

process to grant or revoke employee access to Google resources, and access is automatically removed for departing employees.

Access authorization is enforced at all relevant layers of the system. Approvals are managed by workflow tools and logged. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud products. Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams **actively monitor access patterns and investigate unusual events**.

For further information on employee onboarding and security and privacy training, please refer to our security white paper.

3.4 Organizational safeguards

3.4.1 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 Google Cloud that logs and surfaces 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.

3.4.2 Use of subprocessors

Google companies directly conduct the majority of data processing activities required to provide Google Cloud services. However, we do engage with some carefully selected third party vendors to perform limited activities in connection with Google Cloud services.

We recognize the importance of transparency about the third parties we engage with who may process your data. We share information about our vendors on our Google Cloud Platform Subprocessor page to provide our customers with visibility. This includes who they are, where they are located, the specific services they support, and the limited processing of customer data they are authorized to perform.

Google expects our Subprocessors to meet the same high standards that we do. Before onboarding Subprocessors, Google assesses their security and privacy practices. We do this to ensure that Subprocessors provide a level of security and privacy appropriate to their data access and the scope of the activities they are engaged to perform.

Once Google has assessed the risks, the Subprocessor is required to enter into appropriate security, confidentiality, and privacy contract terms. In particular, Google requires our Subprocessors to only

access and use your data to the extent required to perform the obligations subcontracted to them and to do so in accordance with our contract with you. Google will remain fully liable for all obligations subcontracted to our Subprocessors.

To enable you to retain oversight of our Subprocessors, we will notify you when we engage a new Subprocessor so that you know in advance before any new Subprocessor starts processing your data.

3.4.3 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.

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.

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.

4. Security and compliance standards

4.1 Independent verification of our control framework

Moving to the cloud means protecting sensitive workloads while achieving and maintaining compliance with complex regulatory requirements, frameworks, and guidelines. Failure to comply with regulations in any part of this network can lead to cascading compliance issues throughout the ecosystem.

Google Cloud's industry-leading security, third-party audits and certifications help support your compliance. Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Some of the key international standards we are audited against are:

- ISO 27001 (Information Security Management)
- ISO 27017 (Cloud Security)
- ISO 27018 (Cloud Privacy)
- ISO/IEC 27701 (Privacy - Data Processor)
- SOC 2 and SOC 3 reports
- NIST 800-53
- PCI DSS
- CSA Star
- GxP

Google also participates in sector and country-specific frameworks, such as FedRAMP (US government), BSI C5 (Germany), MTCS (Singapore), HIPAA (US government), iRAP (Australia), MeitY (India) and many others. We also provide resource documents and mappings to frameworks and laws where formal certifications or attestations may not be required or applied.

For a complete listing of our compliance offerings, please visit our compliance resource center.

Furthermore, Google Cloud's industry-leading controls, contractual commitments, and accountability tools have helped organizations across Europe meet stringent data protection regulatory requirements for years. This commitment to supporting the compliance efforts of European companies has earned us the trust of businesses like retailers, manufacturers and financial services providers.

As part of our continued efforts to uphold that trust, Google Cloud was one of the first cloud providers to support and adopt the EU GDPR Cloud Code of Conduct (CoC). The CoC is a mechanism for cloud providers to demonstrate how they offer sufficient guarantees to implement appropriate technical and organizational measures as data processors under the GDPR.

4.2 Compliance support for customers

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

5. Conclusion

Protecting customer data is a primary design consideration for Google Cloud's infrastructure, applications and personnel operations. Google's security practices are verified by independent third-parties, providing assurance to customers regarding our security controls and practices. Google offers strong contractual commitments to ensure our customers maintain control over their data and its processing, including the commitment that we only process your customer data according to your instructions.

Google Cloud is designed to meet stringent privacy and security standards based on industry best practices. Google has strong contractual commitments regarding data ownership, data use, security, transparency, and accountability. These commitments ensure you maintain control over your data and how it is processed, including the assurance that your data is not used for advertising or any purpose other than to deliver Google Cloud services. In addition, we give you the tools you need to help meet your compliance and reporting requirements.

Furthermore, because protecting data is core to Google Cloud, we can make extensive investments in security, resources and expertise at a scale that others cannot. Our investment frees you to focus on your business and innovation. Google's operations and collaboration with the security research community also enable us to address vulnerabilities quickly or prevent them entirely.

For these reasons and more, organizations across the globe trust Google with their most valuable asset: their information. Google will continue to invest in Google Cloud to allow you to benefit from our services in a secure and transparent manner.