Google Cloud

Google Cloud Whitepaper

July 2023

Israel Protection of Privacy Law, 5741-1981

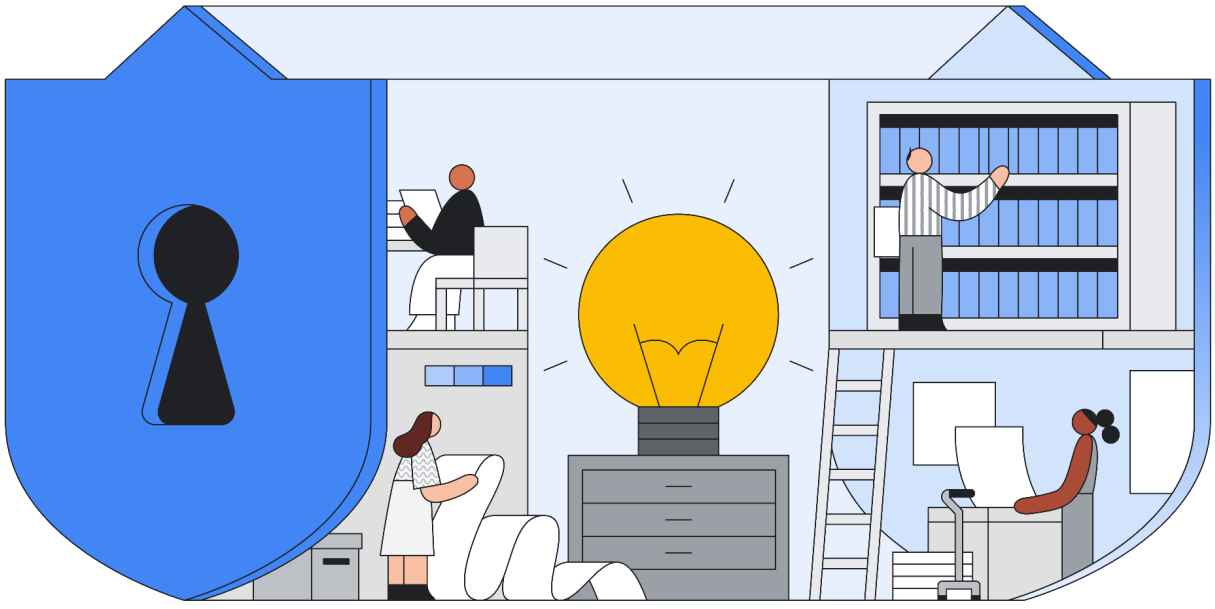


Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of July 2023 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.

Introduction

At Google Cloud, privacy plays a critical role in the development and operation of our products and services. We've set a high bar for what it means to host, serve, and protect customer data by centering security and data protection at the core of how we design and build our products. We start from the fundamental premise that as a Google Cloud customer, you[1] own your customer data. We implement stringent security measures to help safeguard your customer data and provide you with tools and features to help control it on your terms.

This whitepaper provides information to our customers about the Protection of Privacy Law, 5741-1981 ("PPL") and how Google Cloud uses Google's industry-leading data privacy and security capabilities to help store, process, maintain, and secure customer data[2]. We are committed to partnering with our customers so they can deploy workloads using Google Cloud services and Google Workspace for their productivity needs in a manner that aligns with the PPL requirements. We describe our data protection features and outline how they map to its requirements. However, please note that, as a provider of cloud services, we are not in a position to provide you with legal advice - that is something only your legal counsel can provide.

Overview of the Protection of Privacy Law, 5741-1981

The PPL and its implementing regulations govern the collection, use, disclosure and other processing of personal data (including sensitive personal data) in Israel by public and private entities and provides data subjects with rights over their personal data.

The PPL applies to Database Owners (akin to the concept of a "Controller") and Database Holders (akin to the concept of a "Processor"). It governs personal data ("Information"), defined under current law as "data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person," as well as sensitive personal data ("Sensitive Information"), defined as data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person or Information as determined by the Minister of Justice.

Chapter One of the PPL ("Infringement of Privacy") defines the right to privacy and provides the main principle by which no person shall infringe the privacy of another without their consent, thus acknowledging consent as a primary legal basis for data processing. **Chapter Two** of the PPL

---

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

[2] In this whitepaper "customer data" and "your data" refers to the customer data we process according to your Google Cloud agreement(s).

("Protection of Privacy in Database") refers to the protection of personal data in a "Database", which is defined as "a collection of data, kept by a magnetic or optic means and intended for computer processing," excluding a collection of data for personal use or a collection of data that does not "produce a characterization which infringes the privacy of the persons" as defined in the PPL. **Chapter Three** of the PPL ("Defenses") defines several defenses against a breach of privacy civil claims and criminal proceedings, including, for example, with respect to legitimate interests and a legal, moral, social or professional obligation for Information processing.

The Privacy Protection Authority ("PPA"), through its statutory power as the Registrar of Databases, supervises compliance of private and public entities with the PPL and all regulations thereunder, including the Privacy Protection Regulations (Information Security) ("Security Regulations"), and the Privacy Protection (Transfer of Data to Databases Abroad) Regulations, 5761-2001 ("Transfer Regulations"). The PPA regularly publishes guidance materials, including Q&A and additional guidance with respect to the Security Regulations, as well as guidance on the use of outsourcing services for processing personal information and the responsibilities of Data Protection Officers. In addition to its administrative and criminal investigatory powers, the PPA is granted with authority to impose administrative fines in certain circumstances.

Entities that violate the PPL may be liable for civil or criminal penalties. Criminal penalties include the potential for up to five years' imprisonment. In addition to its investigatory powers, the PPA may impose administrative fines ranging from ILS 10,000 for certain violations to ILS 15,000 or ILS 25,000 depending on various factors.

Google Cloud data protection overview & the Shared Responsibility Model

Google Cloud's robust security and privacy controls can give customers the confidence to utilize Google Cloud services and Google Workspace in a manner aligned with the requirements of the PPL. Moreover, we are constantly working to expand our privacy and security capabilities. To help customers with compliance and reporting, Google shares information and best practices, and provides easy access to documentation. In this section, we describe our comprehensive data protection and privacy capabilities and our robust data security features most relevant to the PDPA. We then explain how we share security and compliance responsibilities according to the Shared Responsibility Model.

Google Cloud's approach to security and data protection

Google's focus on security and protection of information is among our primary design criteria. Security is at the core of everything we do; it is embedded in our culture and our architecture, and we focus on improving it every day. In this section, we provide an overview of the organizational and technical controls we use to protect your data. To learn more about our approach to security and compliance,

refer to the Google security whitepaper for Google Cloud services and the Google Workspace Security whitepaper.

Topics

Google Cloud's approach to data protection and privacy

Data protection and privacy are fundamental to Google. We design our products and services from the start with privacy and trust as guiding principles. Google Cloud works to help ensure the protection and privacy of customers' data in three ways: 1) we provide superior data protection through a secure core infrastructure that is designed, built, and operated to help prevent threats; 2) we give customers robust security controls to help them meet policy, regulatory, and business objectives; and 3) we work to fulfill our compliance responsibilities and to make compliance easier for our customers.

Data protection and privacy trust principles

We want our customers to feel confident when using Google Cloud and Google Workspace products. We believe that trust is created through transparency, and we want to be open about our commitments and offerings to our customers when it comes to protecting their data in the cloud.

Our commitments to you about your data

Your data is critical to your business, and you take great care to keep it safe and under your control. We want you to feel confident that taking advantage of Google Workspace and Google Cloud services doesn't require you to compromise on security or control of your business's data.

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.

When you use Google Workspace or Google Cloud services, you can:

1. **Know that your security comes first in everything we do.**

   We promptly notify you if we detect a breach of security that compromises your data.

2. **Control what happens to your data.**

   We process customer data according to your instructions. You can access it or take it out at any time.

3. **Know that customer data is not used for advertising.**

   We do not process your customer data to create ads profiles or improve Google Ads products.

4. **Know where Google stores your data and rely on it being available when you need it.**

   We publish the locations of our Google data centers; they are highly available, resilient, and secure.

5. **Depend on Google's independently-verified security practices.**

   Our adherence to recognized international security and privacy standards is certified and validated by independent auditors — wherever your data is located in Google Cloud.

6. **Trust that we never give any government entity "backdoor" access to your data or to our servers storing your data.**

   We reject government requests that are invalid, and we publish a transparency report for government requests.

To learn more about our commitments to safeguarding customer information, refer to the Google Cloud Privacy page. See the Cloud Data Processing Addendum for Google Workspace and Google Cloud.

Dedicated privacy team

The Google privacy team operates separately from product development and security organizations, but participates in Google product launches by reviewing design documentation and performing code reviews to help ensure that privacy requirements are followed. They help release products that reflect strong privacy practices: transparent collection of user data, providing users and administrators with meaningful privacy configuration options, and continuing to be good stewards of information stored on our platform. To learn more about our privacy team, refer to the privacy team section of the Google security whitepaper for Google Cloud services and the Google Workspace Security whitepaper.

Data access and customer control

Google Cloud customers own their data, not Google. Google will only process customer data in accordance with contractual obligations. We also provide customers with solutions that allow granular control of resource permissions. For example, using Cloud Identity and Access Management, customers can map job functions to groups and roles so users only access the data they need to get the job done. Furthermore, customers may delete customer data from our systems or take it with them if they choose to stop using our services.

Restricted access to customer data

To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when the data is stored on the same physical server. Only a small group of Google employees has access to customer data pursuant to explicit reasons based on job function and role. Any additional access is granted according to stringent procedures and tracked through audit records which are available in near real-time via Access Transparency.

Google Cloud's approach to data security

In this section, we provide an overview of the organizational and technical controls that we use to protect your data at Google Cloud. Please refer to Google security whitepaper, and Google Workspace Security whitepaper for additional information on our security practices.

Strong security culture

Security is central to Google culture. It is reinforced in employee security training and company-wide events to raise awareness and drive innovation in security and privacy.

To learn more about our security culture, refer to the security culture sections in our Google security whitepaper and our Google Workspace Security whitepaper.

Security team

Google employs more than 850 security professionals, including some of the world's foremost experts. This team maintains the company's defense systems, develops security review processes, builds security infrastructure, implements Google's security policies, and actively scans for security threats. Our team also takes part in research and outreach activities to protect the wider community of Internet users, beyond just those who choose Google solutions. Our research papers are available to the public. As part of our outreach efforts, we have a team known as Project Zero that aims to prevent targeted attacks by reporting bugs to software vendors.

In addition, our security team works 24/7 to quickly detect and resolve potential security incidents. Our security incident management program is structured around industry best practices and tailored into our "Incident Management at Google (IMAG)" program, which is built around the unique aspects of Google and its infrastructure. We also test our incident response plans regularly, so that we always remain prepared.

To learn more, refer to the security team, vulnerability management, and monitoring sections in the Google security whitepaper. In addition, refer to the security team, vulnerability management, and monitoring sections in the Google Workspace Security whitepaper.

Trusted infrastructure

We conceived, designed, and built Google Cloud to operate securely. Google is an innovator in hardware, software, network, and system management technologies. We custom design our servers, proprietary operating system, and geographically distributed data centers. Using "defense in depth" principles, we have created an IT infrastructure that is generally more secure and easier to manage than most other deployment options. Our infrastructure can 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. We maintain the security of this infrastructure in progressive layers, starting from the physical security of our data centers, building with underlying security-designed hardware and software, continuing with secure service deployment, secure data storage, and secure internet communication, and finally, operating the infrastructure in a secure fashion.

To learn more, refer to the Google Cloud Infrastructure Security Design Overview, as well as the Cloud Data Processing Addendum, Appendix 2: Security Measures.

Infrastructure redundancy

Google's infrastructure components are designed to be highly redundant. This redundancy applies to server design and deployment, data storage, network and Internet connectivity, and the software services themselves. This "redundancy of everything" creates a robust solution that is not dependent on a single server, data center, or network connection. Our data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as natural disasters and local outages. In the event of hardware, software, or network failure, platform services and control planes are capable of automatically changing configuration so that customers can continue to work without interruption. Our highly redundant infrastructure also helps customers protect themselves from data loss. Customers can create and deploy our cloud-based resources across multiple regions and zones, allowing them to build resilient and highly available systems. To learn more, refer to the low latency and highly available solution in the Google security whitepaper and the Google Workspace Security whitepaper.

State-of-the-art data center security

Google data centers feature layers of physical security protections. We limit access to these data centers to only a very small fraction of employees and have multiple physical security controls to protect our data center floors such as biometric identification, metal detection, vehicle barriers, and custom-designed electronic access cards. We monitor our data centers 24/7/365 to detect and track intruders. Data centers are routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more, refer to our Data Center Innovation page.

Data encryption

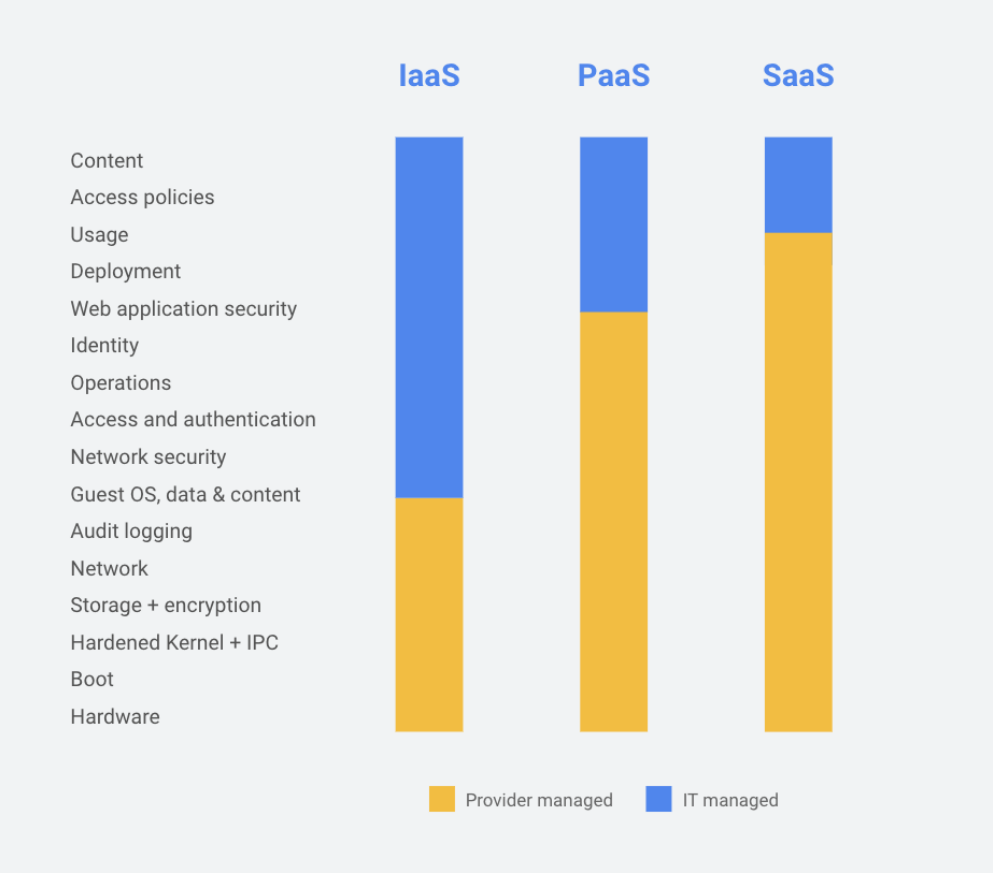
Google encrypts data at rest and encrypts data in transit, by default. The type of encryption used depends on the OSI layer, the type of service, and the physical infrastructure component. By default, we encrypt and authenticate data in transit at one or more network layers when data moves outside physical boundaries not controlled by or on behalf of Google. To learn more, refer to the Encryption in Transit in Google Cloud whitepaper.

Cloud-native technology

We continue to invest heavily in security, both in the design of new features and the development of cutting-edge tools so customers can more securely manage their environments. Some examples are the Cloud Security Command Center for Google Cloud and the Security Center for Google Workspace that bring actionable insights to security teams by providing security analytics and best practice recommendations from Google, and VPC Service Controls, which help to establish virtual security perimeters for sensitive data. To learn more about our security technologies, refer to our security products & capabilities page.

The Shared Responsibility Model

Under our Shared Responsibility Model, the cloud customer and its CSP share the responsibilities of managing the IT environment, including those related to security and compliance. As a trusted partner, Google Cloud's role in this model includes providing services on a highly secure and controlled platform and offering a wide array of security features from which customers can benefit. Shared responsibility enables our customers to allocate resources more effectively to their core competencies and concentrate on what they do best. The shared responsibility model does not remove the accountability and risk from customers using Google Cloud services, but it does help relieve the burden as we manage and control system components and physical control of facilities. It also shifts a portion of the cost of security and compliance onto Google Cloud and away from our customers. The figure below visually demonstrates an example of the shared responsibility model across on-prem, infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings. Keep in mind that responsibilities will vary depending on the specific services being used.



For more information on Google Cloud product and security configurations, customers should reference the applicable product documentation.

How Google Cloud helps customers meet the requirements of the PPL

This table collates obligations as defined in the PPL or from the Security Regulations or Transfer Regulations enacted by the PPA in its statutory power as the Registrar of Databases. For ease of reference, we've specified when the obligation is from one of the accompanying regulations as opposed to the PPL directly.

Data Protection Obligations	How Google Supports PPL Requirements
Collection, use, and disclosure of Information	
Notice of Collection ● When requesting to collect Information, a Database Owner must provide a notice to data subjects	Customer Responsibility: ● Ensure the Information is collected in a lawful manner. ● Customers must also make disclosures about how they collect and process Information. Google Cloud Commentary: ● Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms.
Purpose Limitation ● The PPL restricts the use of Information in a Database for purposes other than the purpose for which the Database was established.	Customer Responsibility: ● To ensure collection, use, or disclosure of Information is limited to the lawful purposes specified. Google Cloud Commentary: ● Google gives you control to decide what information to put into the services and which services to use, how to use them, and for what purpose. ● Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms. Google will not use your data for any other products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.
Manner of Collection ● In general, consent is the primary legal basis for Database Owners who collect Information directly from data subjects to process Information. A	Customer Responsibility: ● To ensure the collection of Information is conducted through lawful, fair, and not unreasonably intrusive means. ● Such information collection should at all times be fair, lawful, and be directly related to the provisioning of services.

request for Information is subject to a notice at collection.	Google Cloud Commentary: • Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms.
Information/Data Disclosure • Database Owners must enter into written agreements with Holders or other third parties that process Information in a Database. • Such agreements must contain certain provisions, as described in the Security Regulations.	Customer Responsibility: • To develop a disclosure handling process. Google Cloud Commentary: • Google Cloud makes robust confidentiality, data protection, and security commitments in our contracts. • Google commits to processing your data to provide the services ordered by you and in accordance with the contract terms. Google will not use it for any other products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.
Cross-Border Data Disclosure • The Transfer Regulations set certain requirements in order to transfer Information, as described in the regulations.	Customer Responsibility: • Customers should ensure proper legal basis for cross-border transfers are in place. Google Cloud Commentary: • Google applies the same robust security measures to customer data wherever it is located. Our data processing agreements for Google Workspace and Google Cloud services clearly articulate our privacy and security commitment to customers. • Google Workspace and Google Cloud services undergo several independent third-party audits on a regular basis to verify security, privacy, and compliance controls. See Cloud's compliance reports.
Accountability	
Requests to access or correct Information • Under the PPL, data subjects have the right to review their Information stored in a Database. Database Owners must comply with such a request subject to several exceptions. • Data subjects may request	Customer Responsibility: • To develop procedures and capabilities to allow individuals to access and correct their Information. Google Cloud Commentary: • Customers may access their data on Google Cloud services at any time. • If Google receives a request from an individual relating to their Information, our privacy team will advise the requester to submit the request to you, the Google Cloud customer. Google Cloud customers can then take

Database Owners to correct Information that is not correct, not complete, not clear or not up to date.	control for responding to these requests as per their internal procedures and requirements. ● Google Cloud's administrative consoles and services possess the functionality to access any data that you or your users put into our systems.
Requests to delete Information ● Data subjects may request Database Owners to delete Information that is not correct, not complete, not clear or not up to date.	Customer Responsibility: ● If you wish to stop using our services, you can do so at any time. ● Where required, delete Information in response to requests from data subjects. Google Cloud Commentary: ● Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data. You can use the following functionality of Google Cloud services: ○ Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources. ○ Admin Console: A web-based graphical user interface that customers can use to manage their Google Workspace resources. ○ gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. ○ Google APIs: Application programming interfaces which provide access to Google Cloud.
Privacy & Security Program ● Depending on the security level of a Database, data security risk assessments may be required every eighteen months.	Customer Responsibility: ● Customers should implement sufficient security controls to protect the Information including proper configuration of features in the cloud under customer management. Google Commentary: (1) Security of Google's infrastructure Google manages the security of our infrastructure (ie., the hardware, software, networking and facilities that support the services).

	Google provides detailed information to customers about our security practices at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page ● Our Cloud compliance page (2) Security of your data and applications in the cloud (a) Security by default ● Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. ● Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products Information on Google's security products is available on our Cloud Security Products page. The below illustrative list of Google Cloud and Google Workspace services may be used to help with your storage and security requirements: **Access control** 2-Step Verification ● 2-Step Verification puts an extra barrier between customer's business and cybercriminals who try to steal usernames and passwords to access business data. With 2-Step Verification, customer's users sign in to their account in two steps with something they know (their password) and something they have (their mobile phone with Google OTP installed)

	Identity and Access Management (IAM) • Identity and Access Management (IAM) can be used to assign roles and permissions to administrative groups, incorporating principles of least privilege and separation of duties. VPC Service Controls • VPC Service Controls allow customers to address threats such as data theft, accidental data loss, and excessive access to data stored in Google Cloud multi-tenant services. It enables clients to tightly control what entities can access what services in order to reduce both intentional and unintentional losses. • VPC Service Controls delivers zero-trust style access to multi-tenant services. Clients can restrict access to authorized IPs, client context, and device parameters while connecting to multi-tenant services from the internet and other services. Examples include GKE, BigQuery, etc. It enables clients to keep their entire data processing pipeline private. **Access Log** Cloud Logging • Cloud Logging is a fully managed service that allows you to store, search, analyze, monitor, and alert on logging data and events from Google Cloud and Amazon Web Services. You can collect logging data from over 150 common application components, on-premises systems, and hybrid cloud systems. Access Transparency • Access Transparency Maintain visibility of insider access to your data through near real-time logs from Access Transparency. **Protection from External Threats** Cloud Security Command Center • Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security posture by evaluating your security and data attack

	surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities, and threats; and helping you mitigate and remediate risks. Virtual Machine Threat Detection ● Virtual Machine Threat Detection, a built-in service of Security Command Center Premium, provides threat detection through hypervisor-level instrumentation. **Monitoring** ● The Google Cloud Status Dashboard provides status information on the services. ● The Google Workspace Status Dashboard provides status information on the services. ● Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. ● Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. (c) Security resources Google also publishes guidance on: ● Security best practices ● Security use cases ● Security blueprints
Accountability	
Audits ● Depending on the security level of a Database (as defined in the Security Regulations), data security audits may be required.	Customer Responsibility: ● Ensure proper inspection rights to the Director General. Google Cloud Commentary: ● Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. ● You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.
Care of Information	

Privacy Impact Assessment ● The PPL does not require that Database Owners conduct Privacy Impact Assessments (PIAs).	Google Cloud Commentary: ● Google will assist customers (PICs) in responding to PIAs.
Storage and Security ● The PPL states that a Database Owner, Possessor or Manager, are each responsible for the information security in a Database. ● The Security Regulations specify security measures to be implemented based on the security level of a Database.	Customer Responsibility: ● Customers should implement sufficient security controls to protect the Information including proper configuration of features in the cloud under customer management. Google Commentary: (1) Security of Google's infrastructure Google manages the security of our infrastructure (ie., the hardware, software, networking, and facilities that support the services). Google provides detailed information to customers about our security practices at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page ● Our Cloud compliance page (2) Security of your data and applications in the cloud (a) Security by default ● Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. ● Encryption in transit. Google encrypts and authenticates data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page.

	(b) Security products Information on Google's security products is available on our Cloud Security Products page. The below illustrative list of Google Cloud and Google Workspace services may be used to help with your storage and security requirements: **Access control** 2-Step Verification ● 2-Step Verification puts an extra barrier between customer's business and cybercriminals who try to steal usernames and passwords to access business data. With 2-Step Verification, customer's users sign in to their account in two steps with something they know (their password) and something they have (their mobile phone with Google OTP installed) Identity and Access Management (IAM) ● Identity and Access Management (IAM) can be used to assign roles and permissions to administrative groups, incorporating principles of least privilege and separation of duties. VPC Service Controls ● VPC Service Controls allow customers to address threats such as data theft, accidental data loss, and excessive access to data stored in Google Cloud multi-tenant services. It enables clients to tightly control what entities can access what services in order to reduce both intentional and unintentional losses. ● VPC Service Controls delivers zero-trust style access to multi-tenant services. Clients can restrict access to authorized IPs, client context, and device parameters while connecting to multi-tenant services from the internet and other services. Examples include GKE, BigQuery, etc. VPC Service Controls enable clients to keep their entire data processing pipeline private. **Access Log** Cloud Logging

	• Cloud Logging is a fully managed service that allows you to store, search, analyze, monitor, and alert on logging data and events from Google Cloud and Amazon Web Services. You can collect logging data from over 150 common application components, on-premises systems, and hybrid cloud systems. Access Transparency • Access Transparency can maintain visibility of insider access to your data through near real-time logs from Access Transparency. **Protection from External Threats** Cloud Security Command Center • Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security posture by evaluating your security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities, and threats; and helping you mitigate and remediate risks. Virtual Machine Threat Detection • Virtual Machine Threat Detection, a built-in service of Security Command Center Premium, can provide threat detection through hypervisor-level instrumentation. **Monitoring** • The Google Cloud Status Dashboard provides status information on the services. • The Google Workspace Status Dashboard provides status information on the services. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. • Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. (c) Security resources

	Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints

Conclusion

At Google, we recognize that your data is yours only and guaranteeing the privacy of your data is key. The protection of your data is a primary design consideration for all our infrastructure, products and personnel operations. We believe that Google can offer a level of protection that very few public cloud providers or private enterprise IT teams can match. Because protecting data is core to Google's business, we can make extensive investments in security, resources, and expertise at a scale that others cannot. Our investment can free you to focus on your business and innovation.

Data protection and privacy is more than just security. Google's strong contractual commitments help make sure 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.

The information within this whitepaper should be used to help customers determine whether Google Cloud and Google Workspace products or services are suitable for them in light of the PPL.