Google Cloud Whitepaper
April 2022

The Philippines Data Privacy Act

Table of Contents

Disclaimer

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

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 safeguard your customer data and provide you with tools and features to control it on your terms.

This whitepaper provides information to our customers about the Philippines Data Privacy Act 2012 (DPA) and how Google Cloud leverages Google's industry-leading data privacy and security capabilities to 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 DPA's requirements. We explain our data protection features and highlight how they map to the DPA's requirements. However, please note that, as a provider of cloud services, we are not in a position to provide you with legal advice - this is something only your legal counsel can provide.

Overview of the Philippines Data Privacy Act

The Data Privacy Act of 2012 (DPA) (also known as Republic Act No. 10173) took effect on 8 September 2012 and, along with the final implementing rules and regulations (IRR), is the comprehensive law governing data privacy in the Philippines. It sets forth obligations for both data controllers and data processors and extends certain rights to data subjects. The law also endowed a National Privacy Commission (NPC), responsible for enforcing and overseeing the law, with rulemaking power. Violations of the law may result in criminal penalties, including fines or imprisonment.

The Data Privacy Act generally applies to individuals and legal entities that process personal information and governs both controllers and processors. The law applies not only to businesses with offices in the Philippines but also when equipment based in the Philippines is used for processing. The DPA further applies to the processing of the personal information of Philippines citizens regardless of where they reside.

Similarly to other global privacy laws, the DPA governs the processing activities of both "personal information controllers" (PICs) and "personal information processors" (PIPs). A PIC is generally responsible for personal information under its control or custody, including information that has been outsourced or transferred to a PIP or a third party for processing. A PIP processes personal information on behalf of a PIC and only upon the documented instructions of the PIC. PICs and PIPs are both

[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)

accountable for complying with the requirements of the DPA, the IRR, and any issuances by the National Privacy Commission.

The DPA sets forth baseline conditions for processing; in order to process personal information, entities must obtain the consent of the data subject or have an alternative basis for processing, such as to fulfill or enter into a contract, comply with legal obligations, or for the purposes of a PIC's legitimate interests. The law also requires consent or another prescribed basis for the processing of "sensitive" personal information. Furthermore, the DPA contains a central set of "General Data Privacy Principles" that prescribe principles related to transparency, legitimate purpose, proportionality, collection, processing, retention, and data sharing.

On September 9, 2016, the final implementing rules and regulations came into force. The IRR provides additional specificity around both PIC and PIP obligations. They also include additional obligations, such as the requirement for entities to put in place a comprehensive privacy and security program. The NPC has also produced a number of guidance documents, including advisory opinions, circulars, and advisories (NPC Issuances), which describe the NPC's expectations for how to process personal information in compliance with the DPA and IRR.

When you transfer customer data to Google Cloud as part of your use of our services, we act as a personal information processor. This whitepaper provides information to our customers about the DPA and how Google Cloud leverages Google's industry-leading data privacy and security capabilities to store, process, maintain, and secure customer data. 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 DPA's requirements. We explain our data protection features, how they map to the DPA's requirements, and how we share compliance responsibilities with our customers.

Google Cloud data protection overview & the Shared Responsibility Model

Google Cloud's robust security and privacy controls give customers the confidence to utilize Google Cloud services and Google Workspace in a manner aligned with the requirements of the DPAA. 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 organisational 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 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 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.**
   You own your data. Google Cloud does not process your data for advertising purposes.
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 data processing terms for Google Workspace and Google Cloud.

Dedicated privacy team

The Google privacy team operates separately from product development and security organisations, but participates in every Google product launch by reviewing design documentation and performing code reviews to 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 any 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. In fact, Google Cloud is the only cloud service provider (CSP) to offer near real-time logs when its administrators access customers' content through Access Transparency.

Google Cloud's approach to data security

In this section, we provide an overview of the organisational 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 more secure and easier to manage than most other deployment options. Our infrastructure provides 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 ensure 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 Google Cloud Data Processing and Security Terms, Appendix 2: Security Measures and Google Workspace Data Processing Amendment, 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 all 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.

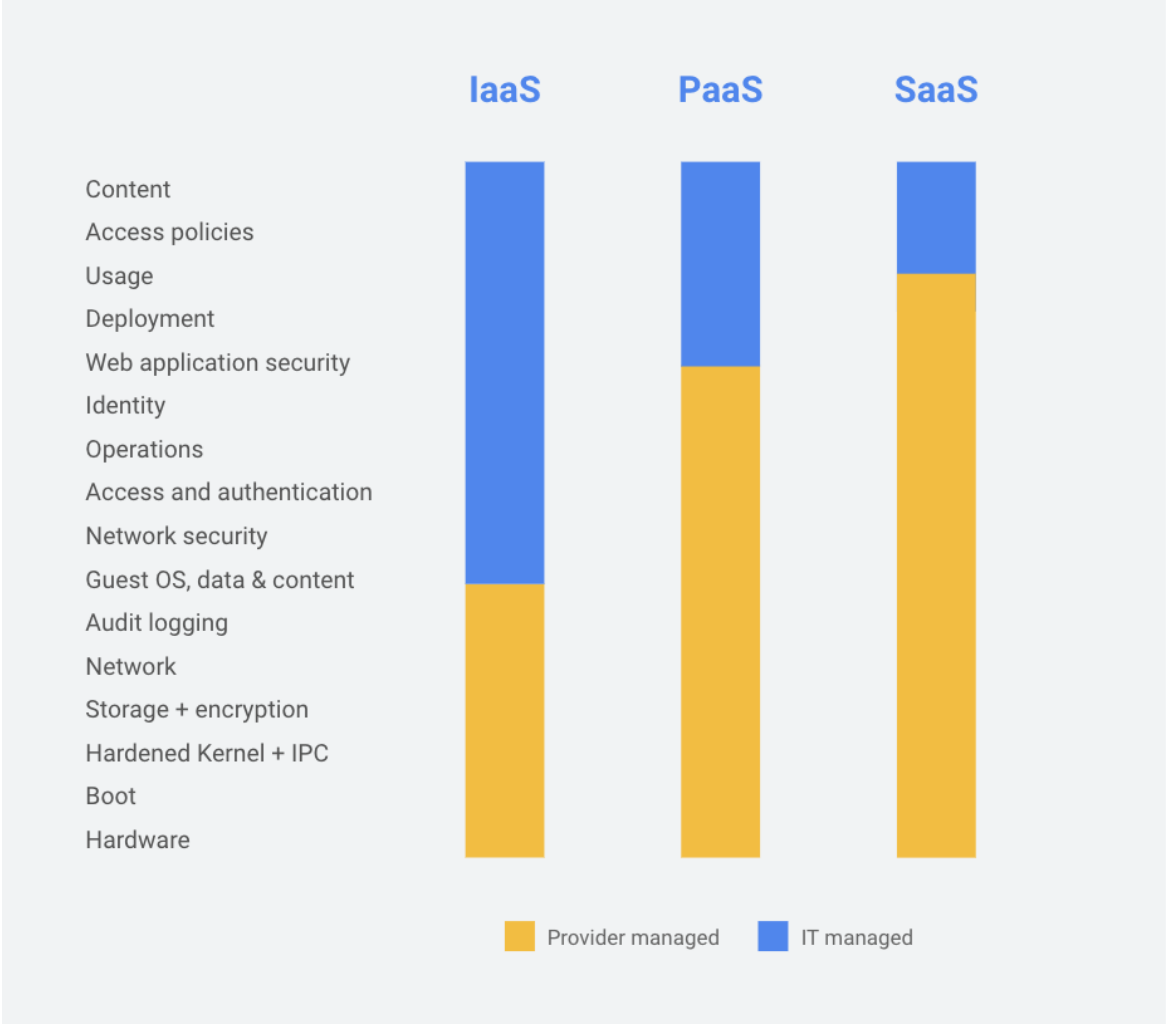
Cloud-native technology

We continue to invest heavily in security, both in the design of new features and the development of cutting-edge tools for customers to 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.


IaaS
PaaS
SaaS
Content
Access policies
Usage
Deployment
Web application security
Identity
Operations
Access and authentication
Network security
Guest OS, data & content
Audit logging
Network
Storage + encryption
Hardened Kernel + IPC
Boot
Hardware
Provider managed
IT managed

How Google Cloud helps customers meet the requirements of the Philippines Data Privacy Act

Data Protection Obligations	How Google Supports DPA Requirements
Collection, use, and disclosure of personal information	
Notice of Collection ● PICs must provide the following information to data subjects either before processing personal information or at the first practical opportunity: a description of the personal information to be processed; the purposes for processing; the scope and method of the processing; the recipients or classes of recipients to whom the information is or may be disclosed; methods used for automated access to the personal information, whether data subjects may use those methods, and the extent to which such access is authorized; the identity and contact details of the PIC or its representative; the retention period for the personal information; and the existence of data subjects' rights.	Customer Responsibility: ● Ensure the personal information is collected in a lawful manner. ● Customers must also make disclosures about how they collect and process personal information, including the purposes for processing. 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; Personal Information Use ● Entities must collect personal information only for specified and legitimate purposes. ● Personal information may only be processed in a way that is compatible with the purposes for which it was collected.	Customer Responsibility: ● To ensure collection, use, or disclosure of personal information is limited to the legitimate purposes notified to data subjects. Google Cloud Commentary: ● You 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 it for any other products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.
Personal Information Disclosure	Customer Responsibility:

• The IRR set forth General Principles for Data Sharing. Data sharing may only occur if it is either authorized by law or if the data subject gives consent and additional conditions are met, such as the execution of a data sharing agreement in cases where the sharing is for commercial purposes. • PICs may also outsource or subcontract the processing of personal information. While this generally does not require the consent of the data subject, PICs must enter into an outsourcing or subcontracting agreement with a PIP or use other reasonable means to ensure the confidentiality, integrity, and availability of the personal information processed, prevent its use for unauthorised purposes, and generally to comply with the law. • Processing by a PIP must be governed by a contract or other legal act that binds the PIP to the PIC. These agreements must meet certain requirements set forth in the IRR.	• To develop a disclosure handling process. Google Cloud Commentary: • Google Cloud makes robust confidentiality, data protection and security commitments in our contracts. • Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you and to only access and use your data to the extent required to perform the obligations subcontracted to them.
Cross-Border Data Disclosure • The PIC has the primary responsibility of securing personal information under its control or custody, even when the information is transferred across borders or jurisdictions.	Customer Responsibility: • Customers should verify that it provides appropriate safeguards to secure personal information transferred to Google Cloud as part of your use of our services. 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 for access to personal information • Data subjects have a right under the DPA to access the personal information	Customer Responsibility: • To develop procedures and capabilities to allow individuals to access their personal

processed about them.	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 personal information, our privacy team will advise the requester to submit the request to you, the Google Cloud customer. Google Cloud customers can then take 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 for correction of personal information ● Data subjects have a right to dispute the accuracy of or an error in the personal information concerning them and to have the PIC correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. ● Data subjects may also request that third parties who have previously received such processed personal information be informed of the inaccuracy and its rectification.	Customer Responsibility: ● To develop procedures and capabilities to correct individuals' personal 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 the correction of their personal information, our privacy team will advise the requester to submit the request to you, the Google Cloud customer. Google Cloud customers can then take control for responding to these requests as per their internal procedures and requirements. ● Google Cloud's administrative consoles and services possess the functionality to rectify any data that you or your users put into our systems.
Requests for deletion of personal information ● Data subjects have the right to request the blocking, removal, or destruction of personal information from a PIC's filing system upon discovery and substantial proof that the personal information is incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes, or are no longer necessary for the purposes for which they were collected.	Customer Responsibility: ● Ensure the accuracy of personal information and develop capabilities and procedures to comply with legal deletion obligations. Google Cloud Commentary: ● Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as

● In such cases, a PIC may notify third parties who have previously received such processed personal information.	retrieve or delete data. ● PICs 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.
Requests for portability of personal information ● Data subjects have a right to obtain from the PIC a copy of their personal information undergoing processing in an electronic or structured format which is commonly used and allows for further use by the data subject.	Customer Responsibility: ● Enable data subjects to obtain a copy of their personal information in a commonly used format. Google Cloud Commentary: ● Google enables customers to access and export their data throughout the duration of their contract and during the post-termination transition term. ● You can export your data from a number of Google Cloud services in a number of industry standard formats: For example: ○ Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. ○ Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. ○ You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage

	options here. ○ In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our services.
Registration ● Certain PICs and PIPs operating in the Philippines must register their data processing systems, unless exceptions apply. ● Further information on registration is described in NPC Circular 17-01.	Customer Responsibility: ● Customers are responsible for their registration obligations. Google Cloud Commentary: ● Google Cloud recognizes that you need certain information in order to conduct due diligence and comply with relevant registration requirements. 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.
Annual Security Reporting ● Both PICs and PIPs must submit an annual report to the NPC summarizing all security incidents and personal information breaches.	Customer Responsibility: ● Customers are responsible for satisfying their annual security reporting obligations. Google Cloud Commentary: ● Google recognizes that to effectively manage your use of the services you need sufficient information about the services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the services on an ongoing basis. ● Google will make information about developments (including security incidents) that materially impact Google's ability to perform the services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard for Google Cloud and the Status Dashboard for Google Workspace. ● In addition, Google Cloud will notify you of data incidents promptly and without undue delay. More information on Google Cloud's data incident response process is

	available in our Data incident response whitepaper.
Records of Processing ● Under the IRR, an entity involved in the processing of personal information must maintain records that sufficiently describe its data processing system and must identify the duties and responsibilities of those individuals who will have access to personal information.	Google Cloud Commentary: ● Google maintains electronic records related to its processing of customer data. ● The rights, responsibilities, roles, obligations, and duties of Google and customers are set out in the Google Cloud contract.
Privacy & Security Program ● The IRR requires that entities have a comprehensive privacy and security program in place. Specifically, entities involved in the processing of personal information must develop, implement and review procedures for collecting personal information, obtaining consent for processing, and limiting use of personal information to declared purposes. Entities must also develop policies for access management, system monitoring, and protocols to follow during security incidents or technical problems; policies and procedures for data subjects to exercise their rights under the Act; and a data retention schedule, including timeline or conditions for erasure or disposal of records.	Customer Responsibility: ● Customers should implement sufficient security controls to protect the personal 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
Care of Personal Information	
Accuracy ● The processing of personal information must be accurate, relevant and, where necessary for purposes of the processing, kept up to date.	Customer Responsibility: ● Customers must take reasonable steps to ensure the personal information it collects and processes is accurate, relevant, and up to date. Google Cloud Commentary: ● Google Cloud is not involved in maintaining the accuracy of personal information collected by customers. ● Google Cloud does, however, ensure the integrity of data placed in our services. ● Customers may also use the administrative consoles to maintain the accuracy of their data.

Retention ● Personal information may only be retained for the fulfillment of the declared, specified, and legitimate purpose, or when processing for the purpose has been terminated; for the establishment, exercise, or defence of legal claims; for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by the appropriate government agency; or as required by law. ● Entities must maintain personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed.	Customer Responsibility: ● Customers should retain personal information only for the purposes for which it is required or as permitted by law. Google Cloud Commentary: ● Google will retain, return, destroy, or delete the personal information in accordance with the contract or service level agreements. ● Google Cloud and Google Workspace administrative consoles and services possess the functionality to delete any data that they and their users put into our systems. If customers delete their data, we commit to deleting it from our systems within 180 days. To learn more about data deletion at Google, refer to our Data deletion on Google Cloud whitepaper. ● We also provide tools that make it easy for customers to take their data with them if they choose to stop using our services, without penalty or additional cost.
Privacy Impact Assessment ● Guidance issued by the NPC requires the completion of privacy impact assessments (“PIAs”) for every processing system of a PIC or PIP that involves personal information. ● Under the Guidelines, the PIC or PIP may forgo the conduct of a PIA only if it determines that the processing involves minimal risks to the rights and freedoms of individuals, taking into account recommendations from the DPO. ● PICs may require PIPs to conduct PIAs.	Google Cloud Commentary: ● Google will assist customers (PICs) in responding to PIAs.
Data Breach Notification ● PICs must generally notify the Commission and affected individuals in the event there is a breach that involves sensitive personal information or any other information that may be used to enable identity fraud; there is reason to believe that the information may have been acquired by an unauthorised person; and the PIC or the NPC believes that the	Customer Responsibility: ● Customers should develop policies and procedures for effectively addressing data breaches, including early warning systems, effective communication protocols, and robust remediation procedures. Google Cloud Commentary:

unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. ● The breach notification must contain certain information as required by law. ● A reporting template is available here.	● Google recognizes that to effectively manage your use of the services, including handling potential data breaches, you need sufficient information about the services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the services on an ongoing basis. ● Google will make information about developments that materially impact Google's ability to perform the services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard for Google Cloud and the Status Dashboard for Google Workspace. ● Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper. ● To fulfill this obligation, Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. Refer to our Data incident response whitepaper for more information.
Storage and Security ● PICs must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration, or disclosure, as well as against any other unlawful processing. These security measures must include, at a minimum, specific measures set forth by law. ● The IRR set forth additional security measures that PICs must implement, including appointing compliance officers, maintaining data protection policies, regular security monitoring, and implementing processes for regularly testing, assessing, and evaluating the effectiveness of security measures.	Customer Responsibility ● Customers should implement sufficient security controls to protect the personal information including proper configuration of features in the cloud under customer management. Google Cloud Commentary: ● See the Privacy & Security Program section.

• PICs are responsible for ensuring that third parties processing personal information on their behalf implement the security measures required by law.	

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 frees you to focus on your business and innovation. Data protection and privacy is more than just security. Google's strong contractual commitments 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.

For these reasons and more, over five million organisations across the globe, including 64 percent of the Fortune 500, trust Google with their most valuable asset: their information. Google will continue to invest in our platform to allow you to benefit from our services in a secure and transparent manner.

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 DPA.