Google Cloud Whitepaper
December 2024

Korea's Personal Information Protection Act



Table of Contents

Introduction 3

Overview of the Korea Personal Information Protection Act 3

Google Cloud data protection overview & the Shared Responsibility Model 4

- Google Cloud's approach to security and data protection 4
- Google Cloud's approach to data protection and privacy 5
- The Shared Responsibility Model 9

How Google Cloud helps customers meet the requirements of the South Korea Personal Information Privacy Act 11

Conclusion 20

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of December 2024 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 Korean Personal Information Protection Act 2023 (PIPA) 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 PIPA's requirements. We explain our data protection features and highlight how they map to the PIPA'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 Korea Personal Information Protection Act

The Personal Information Protection Act 2023 (as amended in March 2023) (PIPA), along with a related Presidential Enforcement Decree, regulates the collection, usage, provision, and other processing of personal information by governmental and private entities.

The PIPA primarily applies to controllers and processors of personal information, with both held to similar standards under the law. The law prescribes separate requirements for the "provision" and "outsourcing" of personal information to third parties.

The PIPA contains precise provisions regarding consent: express consent is generally required prior to the collection, use, and provision of personal information, subject to certain exceptions. Furthermore, the consent for a provision of personal information must be obtained separately from the consent for the collection and use of personal information. However, personal information may be used and provided without a data subject's consent if it is reasonably related to the original purpose of the collection. The prior consent of data subjects is also not generally required for outsourcing.

Among other updates, the 2020 amendments distinguished between pseudonymous, anonymous, and personal information processing; permitted the use of personal information without consent under certain circumstances; allowed for the combination of data sets under certain circumstances; and granted additional powers to the Personal Information Protection Commission (the PIPC, which

[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).

enforces the PIPA). Regulators may impose various administrative sanctions, such as corrective orders, administrative fines and penalties for violations of the PIPA. The law also permits a private right of action in some circumstances.

Key updates in the 2023 amendments notably include:

- Overseas Data Transfers: the legal basis for overseas data transfers must be disclosed in privacy policies, including the names of the countries where South Korean data subjects' personal information is collected and processed.

- Automated Decision-Making: Data subjects now have the right to request explanations for fully automated decisions and refuse such decisions if they significantly impact their rights or obligations. Data controllers must transparently disclose the criteria and procedures for automated processing.

- Chief Privacy Officer (CPO) Requirements: companies and public institutions processing large amounts of personal or sensitive information must appoint CPOs with at least four years of experience in personal information protection. Current CPOs must meet this requirement by March 14, 2026.

Korean regulators have published guidance on a variety of topics relating to the PIPA, including Guidelines on Applying the Personal Information Protection Act to Foreign Business Operators and Guidelines for De-identification of Personal Data.

Google Cloud data protection overview & the Shared Responsibility Model

Google Cloud's robust security and privacy controls give customers the confidence to utilise Google Cloud services and Google Workspace in a manner aligned with the requirements of the PIPA. 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 privacy trust principles
- Dedicated privacy team
- Data access and customer control
- Restricted access to customer data
- Law enforcement data requests

Google Cloud's approach to data security
- Strong security culture
- Security team
- Trusted infrastructure
- Infrastructure redundancy
- State-of-the-art data center security
- Data encryption
- Cloud-native technology
- The Shared Responsibility Model

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 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 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.

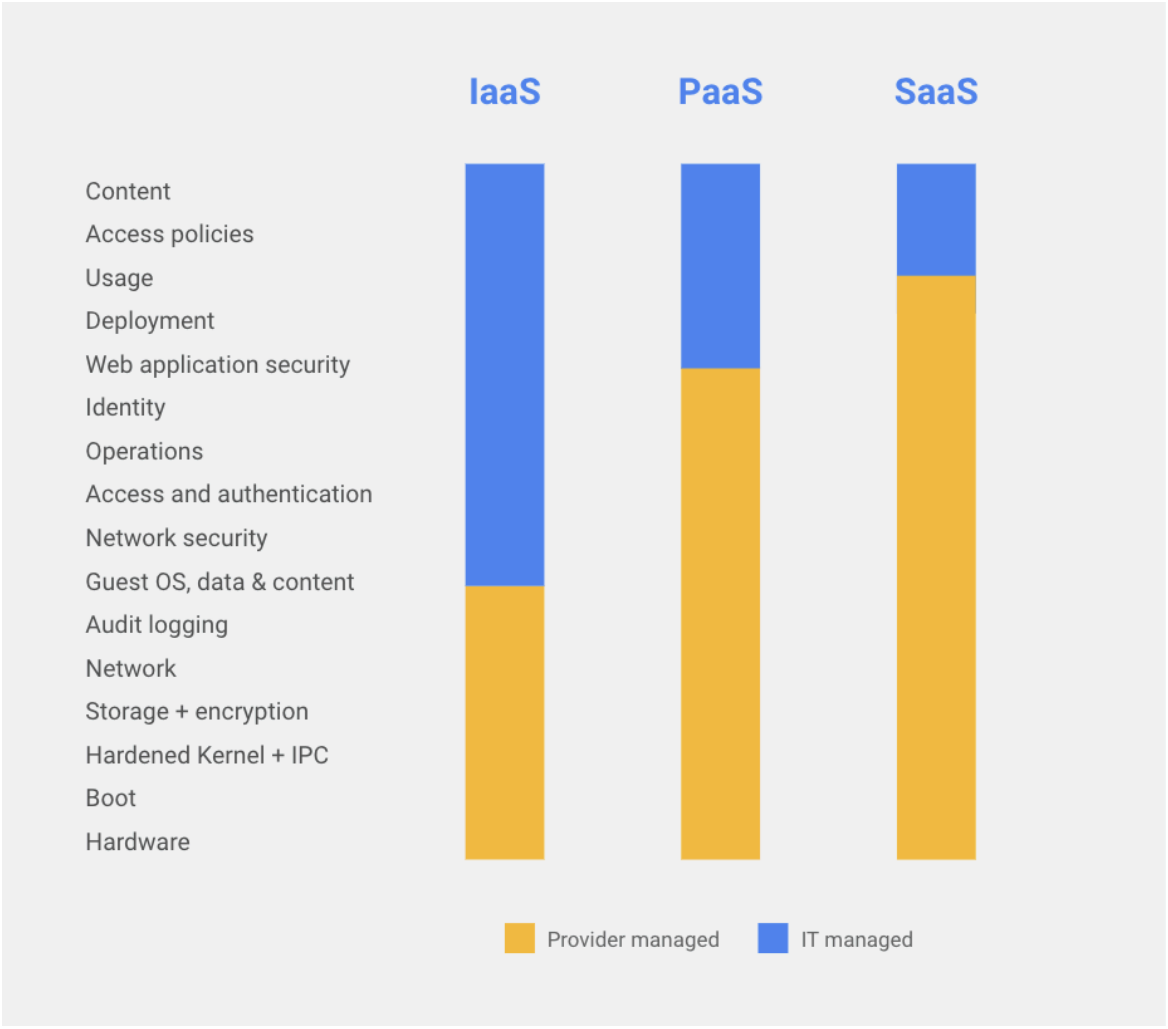
Cloud-native technology

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 South Korea Personal Information Privacy Act

Data Protection Obligations	How Google Supports PIPA Requirements
Collection, use, and disclosure of personal information	
Notice of Collection • Under Art. 3 of the PIPA (Principles for Protecting Personal Information), personal information controllers must make public their privacy policies and other matters related to personal information processing. • Privacy policies must contain certain information as required by the PIPA, such as the purposes for processing personal information, relevant retention periods, whether personal information will be provided to third parties, procedures for destroying personal information, whether the personal information will be outsourced, and other disclosures. • The PIPA also grants data subjects the right to be informed of the processing of their personal information.	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. 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 controllers must explicitly specify the purposes for which personal information is processed. • Personal information controllers must collect personal information lawfully and fairly and only to the minimum extent necessary for the purposes for which it is to be processed.	Customer Responsibility: • To ensure collection, use, or disclosure of personal information is limited to the lawful purposes specified. 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.

Anonymization ● Personal information controllers should endeavor to process personal information through anonymisation, where possible, or through pseudonymisation, to the extent it is still possible to fulfil the purposes of collecting personal information through these methods.	Customer Responsibility: ● Prior to collecting personal information, Customers should consider whether their processing purposes can be fulfilled without individuals identifying themselves, or using a pseudonym. ● If personal information is collected, customers should consider implementing anonymisation or pseudonymisation processes before further processing. Google Cloud Commentary: ● Google Cloud offers Data Loss Prevention, a service designed to help with discovery, classification, and anonymization of sensitive data via an API that can be used by any app / service.
Personal Information Use ● Personal information controllers may only use personal information if they have obtained the data subject's consent or if there is another legal basis for processing, such as when it is necessary to execute a contract with the data subject. ● Personal information controllers are obligated to process personal information in an appropriate manner necessary for the purposes for which the personal information is processed, and to not use it beyond such purposes. ● Data subjects have the right to determine whether or not to consent to the processing of their personal information and the scope of that consent.	Customer Responsibility: ● To ensure collection, use, or disclosure of personal information is lawful. 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 ● Note that separate consent and disclosure requirements apply to the provision and outsourcing of personal information. ● When a personal information controller outsources personal information processing to a third party, it must enter into an agreement with the processor that contains certain information and restrictions specified by the PIPA, including that the processor should be prevented from processing personal	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

information for purposes other than the purpose for which it was disclosed to the processor and the technical and managerial safeguards of personal information that will be in use. ● Personal information controllers may only provide personal information with third parties in certain circumstances, such as if a data subject consents or where the personal information is provided within the scope of purposes for which it is collected. ● Personal information controllers maintain liability for violations of the PIPA by outsourced service providers.	Security whitepaper.
Cross-Border Data Disclosure ● A personal information controller must provide notice to data subjects of overseas transfers and must obtain consent for such cross-border transfers. However, consent is not required if the provision of personal information is reasonably related to the purposes for which the personal information was initially collected and appropriate safeguards are in place.	Customer Responsibility: ● Customers should ensure proper consent and justification (in the event consent is not required) for cross-border transfers are in place. ● Customers can comply with disclosure requirements for cross-border transfers based on the information provided in the Google data processing agreements mentioned below. 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	
Privacy impact assessments ● Public institutions that meet thresholds specified in Art. 35 of the Presidential Enforcement Decree must conduct privacy impact assessments (PIAs) if there is a risk of an infringement with respect to data subjects' personal information.	Customer Responsibility: ● If you are a public institution you conduct a privacy impact assessment, if required. Google Cloud Commentary: ● Google Cloud recognizes that you need certain information in order to conduct a privacy impact assessment. Our data

• A PIA must address: The amount of personal information being processed; whether the personal information is provided to a third party; the probability of violating the rights of data subjects and the degree of risk; whether sensitive information or personally identifiable information will be processed; and the retention period of personal information.	processing agreements for Google Workspace and Google Cloud services clearly articulate our privacy and security commitment to customers. • In addition, you can review Google's current certifications and audit reports via See Cloud's compliance reports.
Requests to access or correct personal information • Data subjects have the right to confirm whether or not personal information is being processed and to request access to, or the correction of, such personal information. • Mechanisms for fulfilling such requests are set forth in the Presidential Enforcement Decree.	Customer Responsibility: • To develop procedures and capabilities to allow individuals to access and correct their 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 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 to restrict processing of personal information; Requests to delete personal information • Data subjects have the right under the PIPA to suspend the processing of their personal information. • Data subjects have the right under the PIPA to request deletion and destruction of their personal information. • Mechanisms for fulfilling data subjects' requests are set forth in the Presidential Enforcement Decree.	Customer Responsibility: • If you wish to stop using our services, you can do so at any time. • Where required, delete personal 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.
Care of Personal Information	
Accuracy ● Personal information controllers must ensure personal information is accurate, complete, and up to date to the extent necessary for purposes of the processing.	Customer Responsibility: ● Customers must take reasonable steps to ensure the personal information it collects, uses or discloses is accurate, up to date, and complete, having regard to the purpose of the use or disclosure. 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.
Data Breach Notification ● Personal information controllers are obligated to notify data subjects in the event of a breach involving their personal information. ● The notification must include particular elements (such as the information divulged and how the breach occurred), as listed in the PIPA. ● Personal information controllers must also report data breaches to the PIPC under certain conditions. ● Breaches can be reported to the PIPC using this form.	Customer Responsibility: ● Customers should develop policies and procedures for effectively addressing and responding to data breaches. Google Cloud Commentary: ● 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 also 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.
Retention • Personal information controllers must destroy personal information when the personal information once a retention period is reached (except as mandated by law). • Where a personal information controller is obliged to retain, rather than destroy, personal information, the relevant personal information or personal information files must be stored and managed separately from other personal information.	Customer Responsibility: • Customers should delete the personal information it holds once its purpose has expired. Google Cloud Commentary: • Google will retain, return, destroy, or delete customer data in accordance with the contract. • Google Cloud and Google Workspace administrative consoles and services provide functionality to delete customer data 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 additional cost.
Storage and Security • Personal information controllers must maintain the security of personal information, taking into account the likelihood and risk of infringement of data subjects' privacy.	Customer Responsibility: • Customers should implement sufficient security controls to protect the personal information including proper configuration of features in the cloud under customer management.

• This includes taking technical, managerial, and physical measures so that personal information is not lost, stolen, divulged, forged, altered, or damaged. • The Presidential Enforcement Decree sets forth particular security measures personal information controllers should adopt to safeguard personal information, such as encryption, log retention, and regular system updates. • When processing pseudonymised information, personal information controllers are obligated to take technical, organizational and physical measures to protect against loss, theft, exposure, forgery, alteration, or damage to the personal information.	Google Commentary: (1) Security of Google's infrastructure Google manages the security of our infrastructure (i.e., 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. **Key Management** Cloud Key Management ● Cloud Key Management Service allows you to create, import, and manage cryptographic keys and perform

	cryptographic operations in a single centralized cloud service. You can use these keys and perform these operations by using Cloud KMS directly, by using Cloud HSM or Cloud External Key Manager, or by using Customer-Managed Encryption Keys (CMEK) integrations within other Google Cloud services. **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

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 organizations 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 PIPA.