Google Cloud

Google Cloud Whitepaper
September 2023

Vietnam's Decree No. 13/2023/ND-CP Personal Data Protection Decree

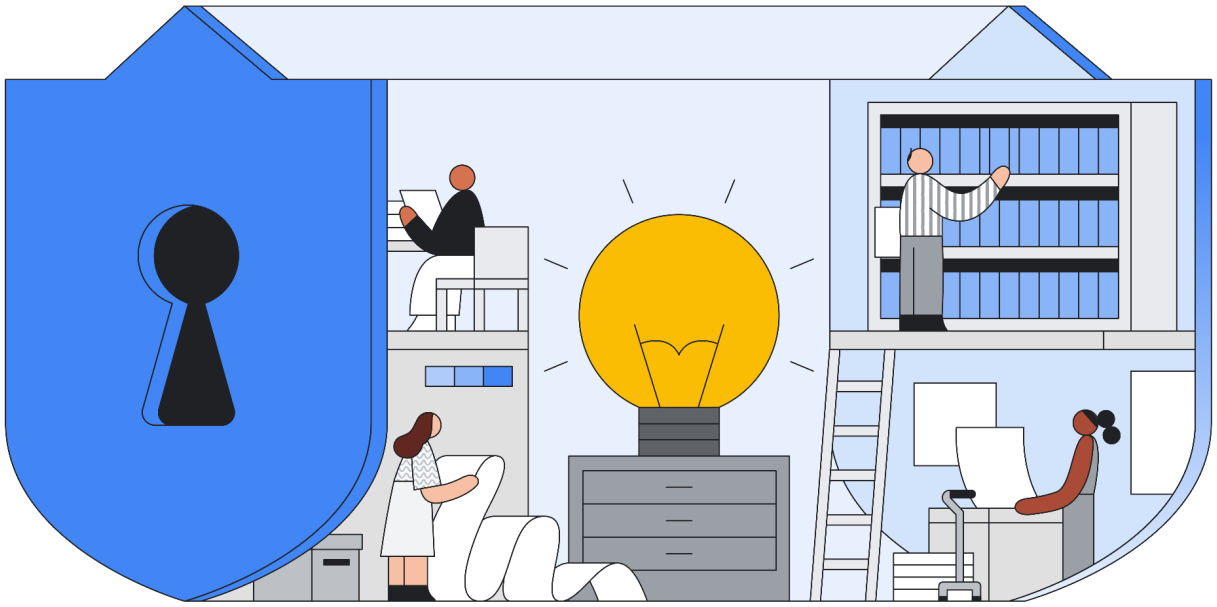


Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of September 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 Vietnam's Decree No. 13/2023/ND-CP or Personal Data Protection Decree ("**PDPD**") 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 for their productivity needs in a manner that aligns with the PDPD's 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 Vietnam Personal Data Protection Decree

The Personal Data Protection Decree (PDPD) came into full effect on July 1, 2023 and is the first comprehensive law governing data privacy in Vietnam. The PDPD applies to (a) Any agency, organization, or individual operating in Vietnam; (b) Vietnamese agencies, organizations, and individuals operating outside of Vietnam; and (c) foreign agencies, organizations, and individuals directly participating in, or related to, personal data processing activities in Vietnam.

The PDPD governs the processing activities of data controllers and data processors. Similar to other global privacy laws, the data controller determines the purposes and means of the processing and the data processor processes personal data on behalf of the data controller and only upon documented instructions of the data controller.

The PDPD defines personal data as information on an electronic medium that is associated with a particular person, or which helps to identify a particular person. It also distinguishes between basic personal data and sensitive personal data. Sensitive personal data refers to personal data which is associated with the rights to privacy of a person that, when violated, will have a direct impact on the data subject's legitimate rights and interests. This includes for example, political views, health status and private life recorded in medical records (excluding blood type), racial or ethnic origin, customer information at a credit institution, and location data of a person identified through location services, etc.

The PDPD sets out that data controllers must rely on consent as a lawful basis to process personal data, unless one of the limited exceptions set out in the PDPD apply. Data subjects must also be

[1] In this whitepaper, "you/your" refers to Google Cloud 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).

provided with certain information regarding the processing of their personal data (i.e. in the privacy notice). Security measures must be implemented to protect personal data.

Data subjects have various rights in relation to their personal data, including the right to access or delete their data, restrict the processing of their data, and withdraw consent.

When you transfer customer data to Google Cloud as part of your use of our services, we act as a data processor. This whitepaper provides information to our customers about the PDPD 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 for their productivity needs in a manner that aligns with the PDPD's requirements. We explain our data protection features, how they map to the PDPD's requirements, and how we share compliance responsibilities with our customers.

Google Cloud data protection overview & the Shared Fate Model

Google Cloud's robust security and privacy controls can give customers the confidence to utilize Google Cloud services in a manner aligned with the requirements of Vietnam's PDPD. 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 Fate 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.

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 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 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 fate for protecting and managing your data in the cloud.

When you use 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 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.

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 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.

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.

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.

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.

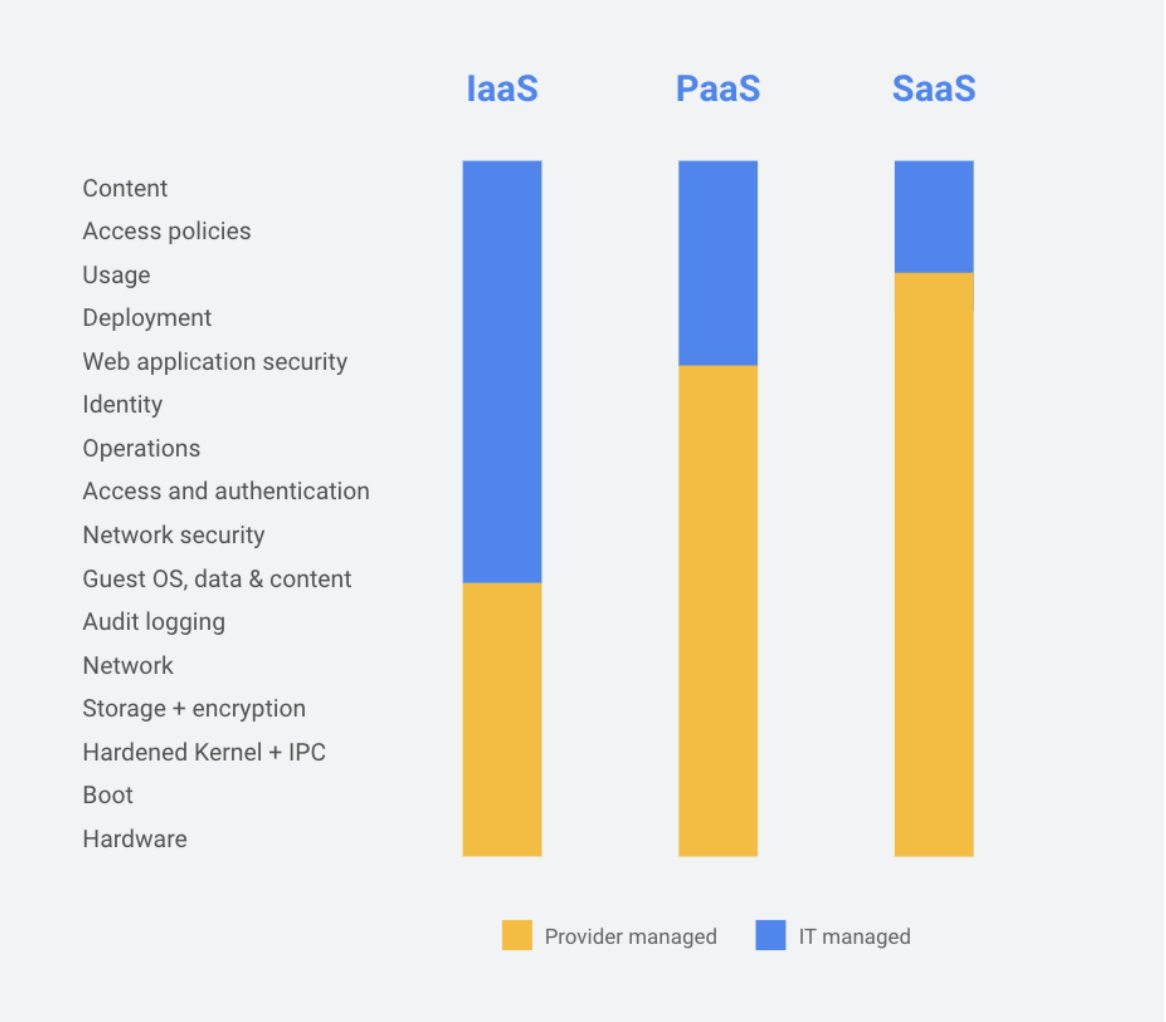
Cloud-native technology

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. One example is the Cloud Security Command Center for Google Cloud which brings 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 Fate Model

Under a traditional Shared Responsibility Model, the cloud customer and its CSP share the responsibilities of managing the IT environment, including those related to security and compliance. Understanding shared responsibility, however, can be challenging. The model requires an in-depth understanding of each service you utilize, the configuration options that each service provides, and what the cloud provider does to secure the service. Google believes that the shared responsibility model stops short of helping cloud customers achieve better security outcomes. Instead of shared responsibility, we believe in shared fate.

Google Cloud's role in the Shared Fate Model builds on the traditional shared responsibility. It includes us building and operating a trusted cloud platform for your workloads. We also provide best practice guidance and secured, attested infrastructure code that you can use to deploy your workloads in a secure way. We release solutions that combine various Google Cloud services to solve complex security problems and we offer innovative options to help you measure and mitigate the risks that you must accept. Shared fate involves us more closely interacting with you as you secure your resources on Google Cloud.



How Google Cloud helps customers meet the requirements of the Vietnam PDPD

Data Protection Obligations	How Google Supports PDPD Requirements
Collection, use, and disclosure of personal data	
Notice of Collection • The data controller must provide the following information in a format which can be printed or reproduced in writing to data subjects prior to processing personal data: (a) purpose(s) of processing; (b) personal data to be processed in relation to the purposes for the specified processing; (c) method for processing; (d) information relating to other organizations and/or individuals which/who will have access to the data; and (e) potential risks of the processing on data subjects	Customer Responsibility: • Ensure the personal data is collected in a lawful manner. • Customers must also make disclosures about how they collect and process personal data. 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 personal data collected must be appropriate and its processing must be limited to the scope and purpose.	Customer Responsibility: • To ensure collection, use, or disclosure of personal data 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 • The collection of personal data must be appropriate and limited to the scope and purpose. • The method of processing should be set out in the privacy notice (see "Notice of Collection" above).	Customer Responsibility: • To ensure the collection of personal data 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. 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.
Anonymization ● Where pseudonymized or anonymized personal data can be reversed or used to identify a data subject, it will be regarded as personal data. ● Pseudonymized or anonymized data that cannot directly/indirectly identify a data subject will not be regarded as personal data and is not subject to the PDPD.	Customer Responsibility: ● Prior to collecting personal data, Customers should consider whether their processing purposes can be fulfilled without individuals identifying themselves, or using a pseudonym. ● If personal data 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 most applications / services.
Personal Data/Data Use ● Consent is required to process personal data unless it is otherwise stipulated by law. ● Personal data may be processed without consent under the following legal bases: (a) an emergency situation where personal data needs to be processed immediately to protect the life and health of a data subject or others; (b) disclosure of personal data in accordance with the law; (c) processing of personal data by a competent State agency in emergency situations (such as to combat epidemics or terrorism); (d) to fulfill the contractual obligations of a contract entered into between a data subject and relevant agencies, organizations or individuals, in accordance with the law; and (e) to serve the activities of State agencies as prescribed by law. ● Where consent is relied upon as the lawful basis, consent must be voluntary and clearly expressed by the data subject. Silence or inactivity does not constitute valid consent. ● The data subject can withdraw consent him/herself, or it can be revoked by an order/request of the competent State agency in writing.	Customer Responsibility: ● To ensure that the collection and/or use of personal data is lawful and obtain any consents and provide notices required, unless another legal basis is permitted by the PDPD. Google Cloud Commentary: ● Google gives you control to decide what information/data 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 Data Disclosure ● Disclosure of personal data requires the consent of the data subject, unless otherwise permitted by PDPD (e.g. where there is another legal basis which permits the disclosure of personal data).	Customer Responsibility: ● To ensure that the disclosure of personal data is lawful and obtain any consents required, unless another legal basis is permitted by the PDPD. 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.
Accountability	
Requests to access or correct personal data ● Data subjects have the right to be provided with a copy of their personal data and may request access to view and correct/amend their personal data. ● In the event that the data subject could not correct/edit personal data due to technical or other reasons, the data subject may then request that the data controller carries out such an act.	Customer Responsibility: ● To develop procedures and capabilities to allow individuals to access and correct their personal data. 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 data, 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 the processing of personal data; Requests to delete personal data ● Data subjects have the right to request to restrict the processing of their personal data. ● Data subjects have the right to delete, or request the deletion of, their personal data in certain circumstances. ● Personal data must be deleted where: (a) the processing is for improper purposes, or the purpose for which the data was	Customer Responsibility: ● If you wish to stop using our services, you can do so at any time. ● Where required, delete personal data 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

collected has been fulfilled; (b) the storage of personal data is no longer necessary; (c) the data controller or processor is dissolved or is no longer in operation, or has declared bankruptcy, or had its business operations terminated in accordance with the law	graphical user interface that customers can use to manage their Google Cloud resources. ○ Cloud 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.
Records of Processing ● The data controller and data controller-processor must record and store logs for personal data processing. This obligation does not apply to data processors.	Customer Responsibility ● Customers are responsible for implementation and enabling appropriate processes to record and store relevant logs Google Cloud Commentary: ● The rights, responsibilities, roles, obligations, and duties of Google and customers are set out in the Google Cloud contract. ●
Privacy & Security Program ● Security measures must be implemented to prevent unauthorized or illegal access/collection of personal data from systems and equipment ("**Security Measures**"). These measures must include management, technical and confidentiality measures. ● Where basic personal data is processed, both the Security Measures and the following requirements ("Basic Measures") must be complied with : (a) the development and promulgation of a personal data protection policy which clearly states what needs to be done in accordance with the provisions of the PDPD; (b) application of personal data protection standards which are appropriate to the fields, industries, and activities relevant to the processing; (c) ensuring network security; and (d) ensuring the irrecoverable deletion. ● Where sensitive personal data is processed, in addition to the Security Measures and Basic Measures, the	Customer Responsibility: ● Customers should implement sufficient security controls to protect the personal data 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

following requirements must be met: (a), a department and personnel responsible for the protection of personal data must be designated (and notified to the Department of Cybersecurity and Hi-Tech Crime Prevention (**A05**)); and (b) data subjects must be notified that sensitive personal data will be processed.	(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 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. ● 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	
Assistance with Investigations Data controllers and processors must: ● cooperate with the Ministry of Public Security (**MPS**) and/or other competent authorities with respect to PDPD compliance; and ● provide information to assist MPS and/or other competent authorities when handling investigations and/or violations of the PDPD.	Google Cloud Commentary ● Google is committed to supporting regulated entities with audits of our services. As this support is not included in our usual publicly listed service fees, Google may, to the extent permitted by applicable law, charge an additional fee in connection with an audit. ● Google will provide further details of any fee in advance of the activity when the scope of the activity is known.
Care of Personal data	
Accuracy ● Personal data must be kept up to date as is necessary for the purposes of processing.	Customer Responsibility: ● Customers must take reasonable steps to ensure the personal data 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 data collected by customers. ● Google Cloud does, however, help 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 ● The data processor must notify the data controller as soon as possible after becoming aware of a violation of the PDPD.	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. ● 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. ● 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 data must only be stored for a period which is suitable for the purposes of processing, unless otherwise provided for by law.	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 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 data must be stored in a form which is appropriate for the operation of the data controller, data processor, or third party, as the case may be; and in a manner which protects the personal data in accordance with law. This includes the implementation of Security Measures as described in the *Privacy & Security Program* section above.	Customer Responsibility: ● Customers should implement sufficient security controls to protect the personal data 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 (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 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 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. ● 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 products or services are suitable for them in light of the PDPD.