Google Cloud Whitepaper
May 2022

Hong Kong's Personal Data (Privacy) Ordinance

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of May 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 Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) 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 PDPO's requirements. We explain our data protection features and highlight how they map to the PDPO'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 Hong Kong Personal Data (Privacy) Ordinance (PDPO)

The Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) originally came into force in 1996 and was significantly amended by the Personal Data (Privacy) (Amendment) Ordinance 2012 (2012 Amendment Ordinance). These amendments included provisions regarding direct marketing, legal assistance, the use of minors' personal data, outsourcing the processing of personal data, and introduced additional penalties. The PDPO was further amended in 2021 by the Personal Data (Privacy) (Amendment) Ordinance 2021 (2021 Amendment Ordinance), which took effect on October 8, 2021. The purpose of these amendments was primarily to address the disclosure of personal data without consent (i.e., doxxing).

Similar to many global privacy laws, the PDPO defines both "data users" (analogous to data controllers) and data processors (entities that process personal data solely on behalf of a data user). However, the PDPO imposes direct legal obligations only on data users, and does not directly regulate data processors. If a data user engages a data processor to process personal data on the data user's behalf, whether within or outside Hong Kong, the data user must adopt contractual or other means (i) to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data, and (ii) to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing. Furthermore, under the PDPO, a data user is liable as principal for the wrongful acts of its authorised data processor.

---

[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).

The territorial jurisdiction of the PDPO only extends to data users who have operations controlled in, or from, Hong Kong.

Key to the PDPO are a set of six Data Protection Principles (DPPs) that govern how entities should collect, handle and use personal information. These cover Collection Purpose and Means (DPP 1), Accuracy and Retention (DPP 2), Use (DPP 3), Security (DPP 4), Openness (DPP 5), and Data Access and Correction (DPP 6).

In addition to enforcing the PDPO, the Office of the Privacy Commissioner for Personal Data ("PCPD") has issued various codes of practice that provide practical guidance with respect to the requirements under the PDPO. While the codes of practice are not legally binding, a breach of them by a data user may give rise to a presumption against the data user in any legal proceedings under the PDPO. The PCPD has also published various guidance notes and other various publications that provide guidance on how to appropriately protect personal data, including guidance on engaging processors, guidance for data users engaging in cloud computing, and a Privacy Programme Management: Best Practice Guide.

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 PDPA. 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 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 the 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.

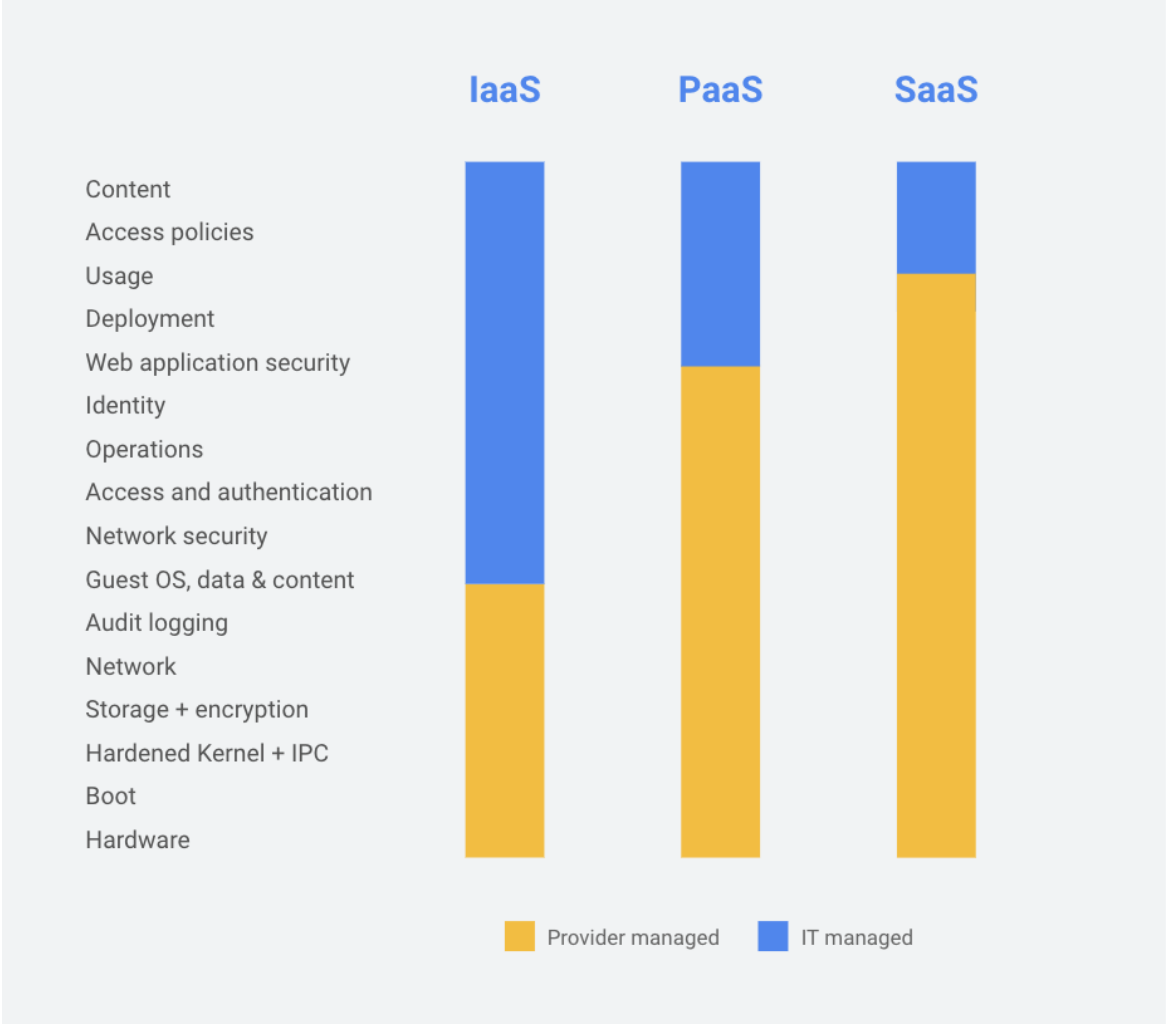
Cloud-native technology

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 Hong Kong Personal Data Protection Ordinance

Data Protection Obligations	How Google Supports PDPO Requirements
Collection, use, and disclosure of personal data	
Notice of Collection • Under the Collection Purpose and Means DPP, all practicable steps should be taken to notify data subjects of the purpose of data collection, the classes of persons to whom the data may be transferred, whether providing the data is required (and if it is obligatory, what the consequences would be for failure to provide it), rights to request access to and correction of the data, and the name or job title, and address, of the individual who is responsible for handling data subject requests. • Data users must disclose in their personal information collection statement and/or privacy policy statement that personal data processing may be outsourced to a cloud provider, that personal data may be stored or processed in another jurisdiction, and that it may be accessible to law enforcement and national security authorities of that jurisdiction. • Under the Openness DPP, data users must take practicable steps to publicly disclose the types of personal data they hold and how the data is used.	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. • To notify data subjects of the purposes of data collection and use, categories of persons to whom data may be shared (eg., service providers) and their ensure the personal information is collected in a lawful manner by notifying clearly stating its purpose of use. 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 • Under the Collection Purpose and Means DPP, personal data must be collected for a lawful purpose directly related to a function or activity of a data user.	Customer Responsibility: • To ensure collection, use, or disclosure of personal data is limited to lawful purposes. Google Cloud Commentary: • You decide what information to put into our 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 ads. Refer to the Data Usage section of the Google Security whitepaper.
Personal Information Use ● Under the Use DPP, personal data should be used only for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject or an exception applies.	Customer Responsibility: ● To ensure collection, use, or disclosure of personal data is limited to the purposes for which the data is collected. Google Cloud Commentary: ● You decide what information to put into our 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 ads. Refer to the Data Usage section of the Google Security whitepaper.
Personal Information Disclosure ● The PCPD has published an Information Leaflet on Outsourcing the Processing of Personal Data to Data Processors. ● The Guidance recommends including certain provisions intended to protect personal data in agreements with processors and conducting a review of the processor's policies and procedures prior to engagement .	Customer Responsibility: ● To conduct appropriate due diligence prior to engaging a cloud provider and require the cloud provider to comply with certain data protection commitments.. Google Cloud Commentary: ● Our data processing agreements for Google Workspace and Google Cloud services clearly articulate our privacy and security commitment to customers. ● Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: ○ ISO/IEC 27001:2013 (Information Security Management Systems)

	○ ISO/IEC 27017:2015 (Cloud Security) ○ ISO/IEC 27018:2014 (Cloud Privacy) ○ PCI DSS ○ SOC 1 ○ SOC 2 ○ SOC 3 ● 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.
Cross-Border Data Disclosure ● There are not currently restrictions on the cross-border transfer of personal data. However, the PCPD has published Guidance on Personal Data Protection in Cross-border Data Transfer.	Customer Responsibility: ● To conduct appropriate due diligence prior to engaging a cloud provider to ensure personal data will not be processed in a manner that violates the PDPO. 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 data ● Under the Data Access and Correction DPP, a data subject must be given access to their personal data. ● Access requests should be handled according to procedures prescribed in the Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users guidance note.	Customer Responsibility: ● To develop procedures and capabilities to allow data subjects to access their personal data. Google Cloud Commentary: ● Customers may access their data on Google Cloud services at any time. ● If Google receives a request from a data subject 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 for correction of personal data ● Under the Data Access and Correction DPP, a data subject must be given the opportunity to make corrections to personal data where the data is inaccurate. ● Correction requests should be handled according to procedures prescribed in the Proper Handling of Data Correction Request by Data Users guidance note.	Customer Responsibility: ● To develop procedures and capabilities to correct data subjects' personal data. Google Cloud Commentary: ● Customers may access their data on Google Cloud services at any time. ● If Google receives a request from a data subject relating to the correction of 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 rectify any data that you or your users put into our systems.
Care of Personal Information	
Accuracy ● Under the Accuracy and Retention DPP, practicable steps must be taken to ensure personal data is accurate.	Customer Responsibility: ● Customers must take reasonable steps to ensure the personal data it collects is accurate. Google Cloud Commentary: ● Google Cloud is not involved in maintaining the accuracy of personal data 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 ● The PDPO does not mandate notification to individuals, third parties, or the PCPD in the event of a data breach. However, the	Customer Responsibility: ● Customers should develop policies and procedures for effectively addressing data breaches, including early warning

PCPD's Guidance on Data Breach Handling and the Giving of Breach Notifications states that a data breach may amount to a contravention of DPP 4, (Security) and recommends notification. ● In the event of a breach involving a cloud provider, a data user may be liable if it has not verified that the processor meets standard security expectations.	systems, effective communication protocols, and robust remediation procedures. 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. 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 ● Under the Accuracy and Retention DPP, practicable steps must be taken to ensure personal data is not kept longer than is necessary to fulfil the purpose for which it is used. ● Data users that engage data processors either inside or outside of Hong Kong are responsible for adopting contractual or other means to prevent any personal data transferred to the processor from being kept longer than is necessary for processing of the data. ● When engaging data processors,	Customer Responsibility: ● Customers should delete the personal data they hold 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

including cloud providers, data users confirm there is a provision in the contract that sets out how personal data is to be erased or returned to data users upon data user requests, contract completion, or contract termination. • The PCPD's Guidance on Personal Data Erasure and Anonymisation provides that data that is sufficiently anonymised will not be considered "personal data" under the PDPO.	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 • Under the Security DPP, a data user must take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use. • Data users are ultimately responsible for the protection of the personal data collected and held by them. The outsourcing of any processing or storage of personal data to third-parties does not relieve the data users' legal responsibility for the protection of the personal data they collect and hold. • Data users that engage a data processor, whether within or outside Hong Kong, must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss, or use of the data transferred to the data processor for processing. • Data users are required to protect and prevent the misuse of personal data entrusted to them by data subjects regardless of whether personal data is stored within the data users' premises or is outsourced to cloud providers. • The Cloud Computing leaflet advises data users to ascertain the sub-contracting arrangements of cloud providers and obtain assurance from the cloud provider that the same level of protection (both technical and administrative) and compliance controls (monitoring and remedial actions) are equally applicable to sub-contractors.	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

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 PDPO.