Google Cloud Whitepaper
November 2020

Hong Kong's Personal Data Privacy Ordinance

Google Cloud

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of November 2020 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

Google Cloud is an industry leading cloud service provider (CSP) with many advanced data security products and features across Google Cloud Platform (GCP) and Google Workspace. Google Cloud enables customers around the globe to experience the strategic benefits of cloud computing, while leveraging its robust data protection and privacy controls. In fact, Forrester Research named Google Cloud as a leader among public cloud platforms in infrastructure and application development capabilities.

This whitepaper intends to help our customers understand the Personal Data Privacy Ordinance (PDPO) of Hong Kong, which is a law that protects individuals' privacy rights regarding personal data; and how Google Cloud implements data privacy and security capabilities to store, process, maintain, and secure customer data in a way that meets the PDPO's requirements.

We are committed to partnering with our customers so that they can deploy workloads using GCP and Google Workspace for their productivity needs in a manner that aligns with the PDPO's requirements.

As a trusted cloud service provider, Google Cloud enables customers to experience the strategic benefits of cloud computing, while leveraging its robust data protection and privacy controls.

Personal Data Privacy Ordinance (PDPO) Overview

Hong Kong's PDPO governs the collection, holding, processing, use, and disclosure of personal data by public and private data users within Hong Kong. The Office of the Privacy Commissioner for Personal Data ("the Privacy Commissioner") promotes, monitors, and enforces the PDPO, as well as publishes guidelines and best practices. To learn more, refer to the Privacy Commissioner's website and the Best Practice Guide on Privacy Management Programme.[1]

In this section, we describe key definitions outlined in the PDPO, including the Six Data Protection Principles (DPPs), as well as relevant information regarding data processors, such as CSPs, based upon the official legislation and the PDPO's best practice guidance for compliance .

Key Definitions

In order to help understand the PDPO and its application, key terms introduced by the PDPO are defined below [2]

Data subject	The individual who is the subject of the data.
Personal data	Any data: ● Relating directly or indirectly to a living individual; ● From which it is practicable for the identity of the individual to be directly or indirectly ascertained; and ● In a form in which access to or processing of the data is practicable.
Data users	A person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.
Data processor	A person who : ● Processes personal data on another person's behalf; and ● Does not process that data for any of its own purposes.
Processing	The use of automated means or otherwise to amend, augment, delete or rearrange the data.

[1] Privacy Management Programme - A Best Practice Guide, Office of the Privacy Commissioner for Personal Data, Hong Kong (August 2018).
[2] Personal Data (Privacy) Ordinance (Cap. 486), Version Date: 20.4.2018; Personal Data (Privacy) (Amendment) Ordinance 2012 (Ord. No. 18 of 2012).

The PDPO's Six Data Protection Principles

The PDPO's Six DPPs impose comprehensive protection measures across the lifecycle of personal data.[3] Data users are responsible for ensuring personal data under their control is processed in accordance with the Six DPPs. If you are a data user, you may find guidance related to your responsibilities under the PDPO on the Hong Kong Privacy Commissioner's website.

Requirements and Guidance for Data Users

A data user may utilise a data processor, whether located within or outside of Hong Kong, to process data on its behalf. When the data user employs a data processor, the PDPO requires the data user to adopt contractual or other means to ensure that the data processor:

- Does not retain personal data for longer than is necessary for the processing of that data (i.e., *DPP2 - Retention Principle*); and
- Has data security measures in place to prevent unauthorised or accidental access, processing, erasure, loss, or use of the data (i.e., *DPP4 - Data Security Principle*).

A data user should obtain contractual commitments from data processors that help the data user to fulfill its obligations under the Six DPPs.

[3] Personal Data (Privacy) Ordinance (Cap. 486)

Using Cloud Services

The Privacy Commissioner's Cloud Computing Information Leaflet provides specific recommendations for organisations interested in using cloud services in accordance with the PDPO.[4] For instance, the data user should consider whether the CSP is compliant with ISO/IEC 27018, a "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors," which addresses many of the requirements of the PDPO. In addition, the Leaflet recommends that data users consider the key aspects of the CSP relationship listed below.

Contractual assurances

As is the case in using a data processor, the data user must have contractual or other means in place to ensure that the CSP abides by the Data Retention and Security Principles. In addition, the contract should:

- Explicitly limit the CSP's use of the personal data to the same purpose for which the data was originally collected or a directly related purpose.
- Enable the data user to satisfy its obligations under the PDPO.
- Stipulate the CSP's erasure measures.
- Require the CSP to notify the data user of data breaches.
- Ensure that any of the CSP's subcontractors have the same technical and administrative protections and compliance controls in place as the CSP.

Transborder data transfers

For transfers of personal data to a jurisdiction outside of Hong Kong, the data user should ensure that the data will be subject to a level of privacy protection substantially similar to the PDPO.[5] To that end, the CSP should inform the data user of the locations data will be transferred. Moreover, data users should inform data subjects of the protections in place for transborder data flows.

---

[4] "Cloud Computing," Information Leaflet, Office of the Privacy Commissioner for Personal Data, Hong Kong (July 2015).

[5] Although the PDPO restricts transfers of personal data to specific jurisdictions pursuant to Section 33, that particular provision has not yet come into effect. As of now, the Privacy Commissioner recommends that data users ensure that personal data transferred to foreign jurisdictions is subject to a level of privacy protection substantially similar to the PDPO. To learn more, refer to the FAQ Question: "Does the PDPO permit data users to process, transfer, and/or store personal data outside of Hong Kong."

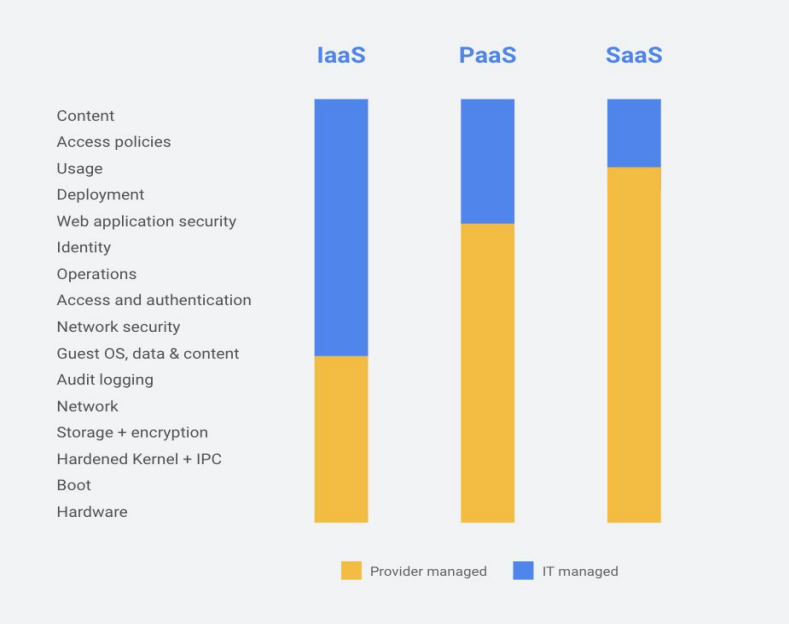
Google Cloud Data Protection Overview

Google Cloud's world-class security and privacy controls and infrastructure provide robust data protection, giving customers the confidence to utilise our products and services to aid in their compliance with the PDPO and other regulatory requirements across the globe.

An overview of the organisational and technical controls we use to protect your data may be found in the Google Security Whitepaper[6] and the Security and Compliance Whitepaper.[7]

The Shared Responsibility Model

Under the Shared Responsibility Model, the cloud customer and its cloud service provider (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. Although the Shared Responsibility Model does not remove the accountability and risk from customers using Google Cloud services, we help by operating and controlling system components and physical control of facilities. Moreover, using our cloud services is a more cost effective approach for customers because we manage a certain portion of the security and compliance efforts. The figure below visually demonstrates an example of the Shared Responsibility Model across 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.



[6]Google Cloud Security Whitepaper: https://cloud.google.com/security/overview/whitepaper
[7] Google Cloud Security and Compliance Whitepaper (for G Suite): How Google Protects Your Data, Google Cloud.

Google Cloud and the PDPO

At Google, compliance is built upon our security and privacy infrastructure. We are committed to complying with applicable data protection laws, and providing what is needed to help our customers comply as well. We undergo regular audits, maintain certifications, provide industry-standard contractual protections, and share tools and information with customers to help strengthen their compliance capacity.

As a trusted CSP, Google Cloud is committed to its responsibilities under the PDPO and strives to support its customers in meeting their current and emerging regulatory compliance and risk management obligations. Google Cloud continues to make significant investments in security, privacy, and compliance management and collaborates with customers to understand and address their specific compliance obligations. Moreover, Google Cloud delineates responsibilities, conducts internal and independent audits, and provides transparency.

Our Internal Compliance Focused Teams

At Google Cloud, we employ an extensive team of lawyers, regulatory compliance experts, and public policy specialists who look after privacy and security compliance. These teams engage with customers, industry stakeholders, and supervisory authorities to shape our services in a manner that helps customers meet their compliance needs. These teams work closely with our customers to understand their unique compliance requirements, and then collaboratively develop a strategy to address the requirements identified.

In addition, Google has a dedicated team of internal auditors and compliance specialists that reviews compliance with security laws and regulations around the world. As new auditing standards are created, the internal audit team determines what controls, processes, and systems are needed to meet them. This team facilitates and supports independent audits and assessments by third parties.

Google Cloud's Audits and Certifications

Google Cloud products regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards to earn the trust of our customers. We are constantly working to expand our coverage.

Below are certifications most relevant to the Asia-Pacific region. To learn more, refer to our Compliance Resource Center.

ISO/IEC 27001

The International Organization for Standardization (ISO) 27001 is a security standard that outlines and provides the requirements for an information security management system. The 27001 standard lays out a framework and checklist of controls that allows Google to ensure a comprehensive and continually improving model for security management. Google Cloud products that are certified for ISO 27001 are listed here.

ISO/IEC 27017

The ISO/IEC 27017:2015 gives guidelines for information security controls applicable to cloud services by providing additional implementation guidance for relevant controls specified in ISO/IEC 27002 and more controls with implementation guidance that specifically relate to cloud services. Google Cloud products that are certified for ISO 27017 are listed here.

ISO/IEC 27018

The ISO 27018 is a "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors." This standard primarily focuses on security controls for public-cloud service providers acting as PII processors. Google Cloud products that are certified for ISO 27018 are listed here.

ISO/IEC 27701

The ISO/IEC 27701 focuses on the collection and processing of personally identifiable information (PII) and was developed to help organizations comply with international privacy frameworks and laws. It provides a framework for implementing, maintaining, and continuously improving a Privacy Information Management System (PIMS). Google Cloud Platform and Google Workspace have received an accredited ISO/IEC 27701 certification as a PII processor after undergoing an audit by an independent third party; the products included are listed here.

Mapping Google Cloud Data Privacy Capabilities to the PDPO

The table below lays out the PDPO's Six Data Protection Principles (DPPs). In this table, we identify our customers' legal obligations and our capacity to support our customers in meeting their obligations. In turn, the table shows how Google Cloud's robust data protection infrastructure aligns to the Six DPPs. Our dedication to delivering services that meet the requirements with data privacy principles and applicable regulations gives customers the confidence to take advantage of GCP and Google Workspace services.

Data Protection Principle	Considerations for Data Users and Google Cloud
DPP1 - Data Collection • Data users must collect personal data in a lawful and fair way, for a purpose directly related to their function or activity. • Data users must notify data subjects of the purpose and the classes of persons to whom the data may be transferred. • Data collected should be necessary but not excessive.	**Data users' responsibility to satisfy this obligation** • To learn more, we recommend reviewing the Privacy Commissioner's Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement.[8] **Google Cloud Commentary** • This is a customer consideration.
DPP2 - Accuracy & Retention • Data users must take practicable steps to ensure the personal data they collect and hold is accurate and not retained longer than is necessary to fulfil the purpose for which it is used. If data users engage a data processor for the purposes of handling personal data, contractual terms should be adopted to ensure that the data processor complies with the retention obligations.	**Data users' responsibility to satisfy the Accuracy obligation** • To learn more, we recommend reviewing the Privacy Commissioner's Privacy Management Programme Best Practice Guide.[9] **Google Cloud and Customer share the retention obligation** **Google Cloud Responsibility** • Google will delete the personal data in accordance with the contract or service level agreements. If customers delete their data, we commit to deleting it from our systems within 180 days. Please see Google's Data Deletion on Google Cloud Platform whitepaper for more information on our deletion processes. We also provide tools that make it easy for customers to take their data with them if they choose to stop

[8] "Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement," Guidance Note, Office of the Privacy Commissioner for Personal Data, Hong Kong (July 2013).
[9] "Privacy Management Programme - A Best Practice Guide," Office of the Privacy Commissioner for Personal Data, Hong Kong (August 2018).

	using our services.
DPP2 - Accuracy & Retention (continued)	• We offer tools which can help customers manage their data. All Google data centers adhere to a strict policy for equipment disposal and reuse. **Google Cloud Commentary** • Google Cloud offers customers the ability to configure **Object Lifecycle Management** policies in Cloud Storage and dataset table expiration in **Cloud BigTable** and **Cloud BigQuery** platforms. This enables customers to specify the appropriate length of time to retain end user data. • **Cloud Storage** also offers object versioning to enable customers to revert back to a prior state should inaccurate or unauthorised changes occur to objects stored there.
DPP3 - Data Use Principle • Data users must use personal data only for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.	**Data users' responsibility to satisfy this obligation** • To learn more, we recommend reviewing the Privacy Commissioner's Privacy Management Programme Best Practice Guide.[10] **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. Google will not use it for any other Google products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.
DPP4 - Data Security Principle A data user must take all reasonably practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use, taking into account: • the kind of data and the harm that could result if any of those things should occur; • the physical location where the data is stored; • any security measures incorporated	**Customer and Google Cloud share the obligation** • To learn more, we recommend reviewing the Privacy Commissioner's Guidance on Personal Data Erasure and Anonymisation[11] and Guidance on Data Breach Handling and the Giving of Breach Notifications.[12] **Google Cloud Commentary** Security is at the core of our culture and our IT architecture. To learn more, we recommend reviewing the Google security whitepaper. Below are some highlights: • **Security Team:** Google employs more than 850 security and privacy professionals, including some of the world's foremost

[10] Privacy Management Programme - A Best Practice Guide, Office of the Privacy Commissioner for Personal Data, Hong Kong (August 2018).
[11] "Guidance on Personal Data Erasure and Anonymisation," Guidance Note, Office of the Privacy Commissioner for Personal Data, Hong Kong (April 2014).
[12] "Guidance on Data Breach Handling and the Giving of Breach Notifications," Guidance Note, Privacy Commissioner for Personal Data, Hong Kong (October 2015).

(whether by automated means or otherwise) into any equipment in which the data is stored; • any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and • any measures taken for ensuring the secure transmission of the data. If data users engage a data processor for the purposes of processing personal data, contractual terms should be adopted to ensure that the data processor complies with the appropriate data security obligations.	experts. This team maintains the company's defence systems, develops security review processes, builds security infrastructure, implements Google's security policies, and actively scans for security threats. • **Physical Security:** Google Cloud has a dedicated security team that supports state-of-the-art data centers. Our data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. Our data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. • **Threat and Vulnerability Management:** Google Cloud's dedicated security team actively scans and detects security threats to our infrastructure from both insiders and external actors, 24/7/365. We use a combination of commercially available and in-house tools, automated and manual penetration testing, quality assurance processes, software security reviews, and external audits to support the vulnerability management process. **Unauthorised Access Prevention:** • To prevent unauthorised access by other tenants sharing the same physical server, we logically isolate our customers' data. We also have a variety of isolation and sandboxing techniques for protecting a service from other services running on the same machine. • To prevent unauthorised access to your data from external threat actors, we employ a defence in depth approach starting with state-of-the-art physical security at our data centers. We have also designed our entire infrastructure stack for security, using cryptographic signatures to ensure no unauthorised changes can be made without detection. Our operations teams detect and respond to threats to the infrastructure from both insiders and external actors, 24/7/365. • To prevent unintended disclosure or unauthorised access to your data from Google insiders, we tightly restrict and monitor any internal access to user data. The small set of employees with access to your data is subject to rigorous authentication measures, detailed logging, and activity scanning to detect inappropriate access via log analysis. Google's Code of Conduct specifically addresses responsibilities and expected

	behaviour with respect to the protection of information.
	• **Subcontractors:** Google reviews the information governance practices and security posture of vendors, third-party suppliers, and their products that Google shares confidential or sensitive information with. We ensure that they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Google includes an Information Protection Addendum (IPA) to contracts with its sub-processors who have access to customer data. A list of GCP sub-processors and the services they provide is available here and for Google Workspace here. • **Incident Response Plan & Data Breach Notification:** The Google security team operates 24/7. We will promptly notify customers if we detect a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to their data on systems we manage. Moreover, we will assist with investigative efforts via our support team. To learn more, refer to our Data Incident Response Whitepaper.[13] **Google Cloud Commentary** • Google Cloud **Identity and Access Management (IAM)** offers customers with the ability to define granular resource permissions to mitigate against unauthorised data access. Users can be added to groups and IAM policies attached to those groups for better manageability of access governance. To further validate the authenticity of users, customers can enable **multi-factor authentication** through the use of security keys, passcodes, or mobile device pushes. • Google Cloud's **Access Transparency** feature provides visibility into the actions that Google's engineers request and take when it impacts your organiszations' data. Data owners can access these audit logs within Stackdriver and monitor when approvals are made for Google Cloud support engineer access and when that access occurs. • Google Cloud's **Data Loss Prevention (DLP)** feature can enable organisations to identify where sensitive user data resides and take action to either obfuscate such data,

[13] Data Incident Response Whitepaper, Google Cloud (September 2018).

	secure it through IAM policies, or remove it. • Google Cloud automatically **encrypts data at rest**. The default **Key Management Solution (KMS)** utilizes keys generated and managed by Google Cloud. For selected services, customers can also generate their own keys with Google Cloud's **KMS API,** and have Google Cloud perform auto-rotation and key management activities. To further mitigate against confidentiality and integrity risks to sensitive health information, customers have options to supply their own encryption keys and to personally manage the keys' lifecycles. • 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. Customers deploying their own applications to Google Cloud on platforms such as Compute Engine, Kubernetes Engine, or App Engine have options to consider for encryption-in-transit. For example, global **HTTPS Load Balancer** or **SSL Proxy Load Balancer** can terminate TLS-protected traffic for custom applications.
DPP5 - Openness • A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.	**Data users' responsibility to satisfy this obligation** • It is the responsibility of organisations that collect personal information to inform end-users about their data policies and data handling practices. Google Cloud offers the ability to do so through Identity-Aware Proxy's consent form, but a customer can also do so through another custom consent interface. • To learn more, we recommend reviewing the Privacy Commissioner's Privacy Management Programme Best Practice Guide.[14] **Google Cloud Commentary** • Google believes transparency is essential to create trust and recommends that data users inform their data subjects about their use of GCP and Google Workspace. We provide transparency by communicating aspects of our security and control environment that are relevant to you, publishing information about our security and control practices through various media types, and providing reports and other documentation directly to customers as

[14] "Privacy Management Programme - A Best Practice Guide," Office of the Privacy Commissioner for Personal Data, Hong Kong (August 2018).

	necessary. • Google has up-to-date security and privacy policies that have been reviewed and approved by management and are published and communicated to employees and vendors with access to the Google environment. These policies describe information governance objectives, provide information security guidelines, and emphasise the importance of data protection and privacy to Google's business. Policies are reviewed at least annually and tested as part of the SOC 2 audit. Google reviews and updates our policies as needed to comply with the latest regulatory requirements and IG best practices. • In addition, customers may contact Google's Cloud Data Protection Team at https://support.google.com/cloud/contact/dpo for questions or comments.
DPP6 - Data Access & Correction • A data user must give its data subjects access to their personal data and allow them to make corrections if a piece of data is inaccurate.	**Data users' responsibility to satisfy this obligation** • To learn more, we recommend reviewing the Privacy Commissioner's Guidance Notes on the Proper Handling of Data Correction Request by Data Users[15] and the Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data User.[16] **Google Cloud Commentary** • GCP and Google Workspace allow customers to easily and safely access and correct the personal data stored in the cloud in order to fulfill their data subjects' requests. • For data subject requests or enquiries relating to their personal data, our privacy team will advise requesters to submit their request to the Google Cloud customer. Google Cloud customers can then take control for responding to these requests as per their internal procedures and requirements. Google will assist Google Cloud customers as far as possible in responding to these data subject requests. • GCP and Google Workspace administrative consoles and services possess the functionality to access or rectify any data that they and their users put into our systems. This functionality will help our customers fulfill their obligations to respond to requests from data subjects to exercise their rights under the PDPO. • We encourage you to view sections 9.2.1 and 9.2.2 of

[15] "Proper Handling of Data Correction Request by Data Users," Guidance Note, Office of the Privacy Commissioner for Personal Data, Hong Kong (May 2017).
[16] "Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data User," Guidance Note, Office of the Privacy Commissioner for Personal Data, Hong Kong (June 2016).

	these Terms of Service for more information about data subject rights.

Frequently Asked Questions

While the PDPO applies to all organisations, several industries may face sector-specific privacy or security requirements. In this section, we identify potential questions regarding compliance risks and highlight where Google Cloud can support our customers in assessing and mitigating them.

What does the PDPO require with respect to data breaches?

A data breach may constitute a violation of the Data Security Principle (DPP4), including where the data user's data processor suffers a data breach within or outside of Hong Kong. The PDPO does not explicitly require data users to establish incident response plans or report data breaches. However, the Privacy Commissioner encourages data users to implement an incident response plan and breach notification system as a matter of best practice. For more details, see its Guidance on Data Breach Handling and the Giving of Breach Notifications.[17] To handle data breaches properly, data users should (1) immediately gather relevant information; (2) contact interested parties to identify the cause of or to stop the breach and contain it; (3) assess the risk of harm; and (4) consider notifying the interested parties and affected data subjects when the risk of harm is reasonably foreseeable. Additionally, a data user's contract with a CSP should require the CSP to notify the data user of data breaches.

Our security team at Google works 24/7 to quickly detect and resolve potential security or privacy incidents. Our security incident management program is structured around industry best practices and tailored into our "Incident Management at Google" program, which is built around the unique aspects of Google and its infrastructure. We maintain and continue to invest in advanced threat detection and avoidance technologies and test our incident response plans regularly. Google Cloud is committed to

[17] "Guidance on Data Breach Handling and the Giving of Breach Notifications," Guidance Note, Privacy Commissioner for Personal Data, Hong Kong (October 2015).

informing our customers of incidents involving their data in line with the Data Incident terms in section 7.2 of our agreement. To learn more, refer to our Data Incident Response Process Whitepaper.[18]

Does the PDPO permit data users to process, transfer, and/or store personal data outside of Hong Kong?

In general, Section 33 of PDPO prohibits a data user from transferring personal data outside of Hong Kong, unless it meets one of several conditions.[19] However, Section 33 is not yet in force. Until Section 33 comes into force, data users should follow the Privacy Commissioner's Guidance on Personal Data Protection in Cross-border Data Transfer in order to transfer data across borders with confidence and minimal exposure to privacy risks and potential legal disputes or liabilities.[20]

Besides obtaining a data subject's express and voluntary written consent, the data user may transfer personal data to a jurisdiction that has in force "any law which is substantially similar to, or serves the same purposes as" the PDPO, as determined by the Privacy Commissioner or based on the data user's reasonable objective assessment.

Among other exceptions to the transfer restriction is for the data user to take all reasonable precautions and exercise full due diligence to ensure that the personal data in the foreign jurisdiction receives protection equivalent to the PDPO's. The data user may fulfill this Due Diligence Requirement via contractual means, such as adopting or adapting the Commissioner's recommended model data transfer clauses. Google Cloud provides customers with data protection terms for its products, and customers could review and consider the sufficiency of such terms for the purpose of the Due Diligence Requirement.

According to the Privacy Commissioner, when data users transmit data over the Internet, they should deploy adequate security measures, such as encryption. Finally, data users should inform data subjects of the classes of transfer recipients and, if appropriate, the recipient's location or jurisdiction.

Additionally, the Privacy Commissioner advises data users that storing personal data in the cloud may constitute a cross-border transfer if the cloud server is accessible outside of Hong Kong. In such circumstances, the data user must ensure that the jurisdiction provides a level of personal data protection substantially similar to the PDPO, including judicial oversight over law enforcement agencies authorities to prevent arbitrary access to personal data. Furthermore, the contract with the CSP must allow the data user to fulfill its PDPO obligations, including data subject requests to access and correct their personal data.

Google Cloud offers a range of international data-transfer mechanisms and continue to monitor the evolution of international data-transfer mechanisms. We are committed to having a lawful basis for data transfers in compliance with applicable data protection laws worldwide. We inform our customers

[18] Data Incident Response Whitepaper, Google Cloud (Sept. 2018)
[19] Personal Data (Privacy) Ordinance (Cap. 486).
[20] "Guidance on Personal Data Protection in Cross-border Data Transfer," Guidance Note, Office of the Privacy Commissioner, Hong Kong (December 2014).

of the storage locations and legal jurisdictions of the personal data. Google Cloud Platform services are available in locations across North America, Europe, and Asia. Google Cloud customers can transfer data so as to best meet their latency, availability, durability, and security requirements.

What terms and conditions does Google Cloud provide to its customers regarding data protection?

Google Cloud contractually agrees to a range of terms with its customers, including that it will comply with the applicable legal and regulatory requirements depending on the jurisdiction. The GCP Data Processing and Security Terms and Google Workspace Data Processing Amendment supplement the licensing agreement and describe our commitment to protecting customer data.

In the Data Processing and Security Terms, we mutually agree upon a various terms governing the processing, deletion, and security of customer data. Similarly, we agree to assist customers in respect of data protection impact assessments, data subject request assistance, and international data transfers. Service Level Agreements apply to many of our service offerings in which we agree with our customers on various aspects of the service (e.g. uptime, downtime, error rates) depending on the offering used.

Besides the PDPO, does Hong Kong have other security or privacy laws?

Besides the PDPO, Hong Kong does not have other sector-specific privacy or data protection legislation in place. However, several government authorities, including the Privacy Commissioner, have released personal data protection and cybersecurity guidelines for specific sectors. While these guidelines are non-binding, customers should seek independent legal advice to ensure that they meet all applicable legal and regulatory requirements based on their particular industry. As a trusted partner, we work with our customers to understand the applicable regulations and our shared responsibilities.

Here, we highlight only the financial services and healthcare industries. Because the PDPO applies to all industries, we encourage customers to review the Privacy Commissioner's industry-specific resources.

Banking, Finance, and Insurance Industries

The Privacy Commissioner has issued specific PDPO guidance for the Banking & Finance industry and Insurance industry. Furthermore, the Hong Kong Monetary Authority (HKMA) and the Insurance Authority (IA) both advise authorised banking institutions and authorised insurers, respectively, to ensure that outsourcing arrangements meet the PDPO's requirements and safeguard the integrity and confidentiality of customer data. For more details, refer to the HKMA's Outsourcing Guidelines[21] and the IA's Guideline on Outsourcing.[22]

In addition to data privacy, Hong Kong recognizes the importance of cybersecurity. Hong Kong's Securities and Futures Commission (SFC) published "Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading" to improve the industry's cybersecurity resilience.[23] Subsequently, the HKMA gave notice that licensed corporations should follow the SFC's cybersecurity guidelines. Moreover, to improve the banking industry's cybersecurity and cyber resilience, the HKMA launched both the "Enhanced Competency Framework on Cybersecurity,"[24] along with a companion guide, and the "Cybersecurity Fortification Initiative."[25]

Healthcare Industry

Under the Electronic Health Record Sharing System Ordinance (EHRSSO), public and private healthcare providers, with patient consent, may lawfully collect, share, use, and safeguard patients' health data within the Electronic Health Record Sharing System ("the System"). Because patients' health records in

[21] "Outsourcing," Supervisory Policy Manual, Hong Kong Monetary Authority (V.1 – 28.12.01).
[22] "Guideline on Outsourcing," Insurance Authority, Hong Kong (GL 14).
[23] "Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading," Securities and Futures Commission, Hong Kong.
[24] Enhanced Competency Framework on Cybersecurity (B9/166C), Hong Kong Monetary Authority (December 2016).
[25] Cybersecurity Fortification Initiative (B1/15C; B9/29C, Hong Kong Monetary Authority (December 2016).

the System constitute personal data, the PDPO protects that data. Therefore, when handling such records, healthcare providers, as well as the Commissioner for Electronic Health Record, must comply with both the EHRSSO and the PDPO. In regard to healthcare records in the System, the Privacy Commissioner for Personal Data has authority to handle complaints of suspected breaches of the PDPO and initiate an investigation; perform an inspection of the System; provide guidance on personal data privacy with respect to the System; and manage any data breach notification related to the System.

To learn more, review the Privacy Commissioner's "Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals)." Additionally, check out the Commissioner for the Electronic Health Record's website and its Code of Practice for Using Electronic Health Record for Healthcare, which details healthcare providers' responsibilities.[26]

Conclusion

We have described how information is securely stored, processed, maintained, and accessed in Google Cloud. This information can help customers operating within Hong Kong, or those processing personal data of Hong Kong residents outside of Hong Kong, determine whether the Google Cloud Platform and Google Workspace products or services are suitable for them in light of the PDPO.

[26] Code of Practice for Using Electronic Health Record for Healthcare [Document Reference No. G80 - V1.4], Electronic Health Record Office, Hong Kong (December 2017).