Google Cloud Whitepaper
January 2023

Singapore's Personal Data Protection Act

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 January 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

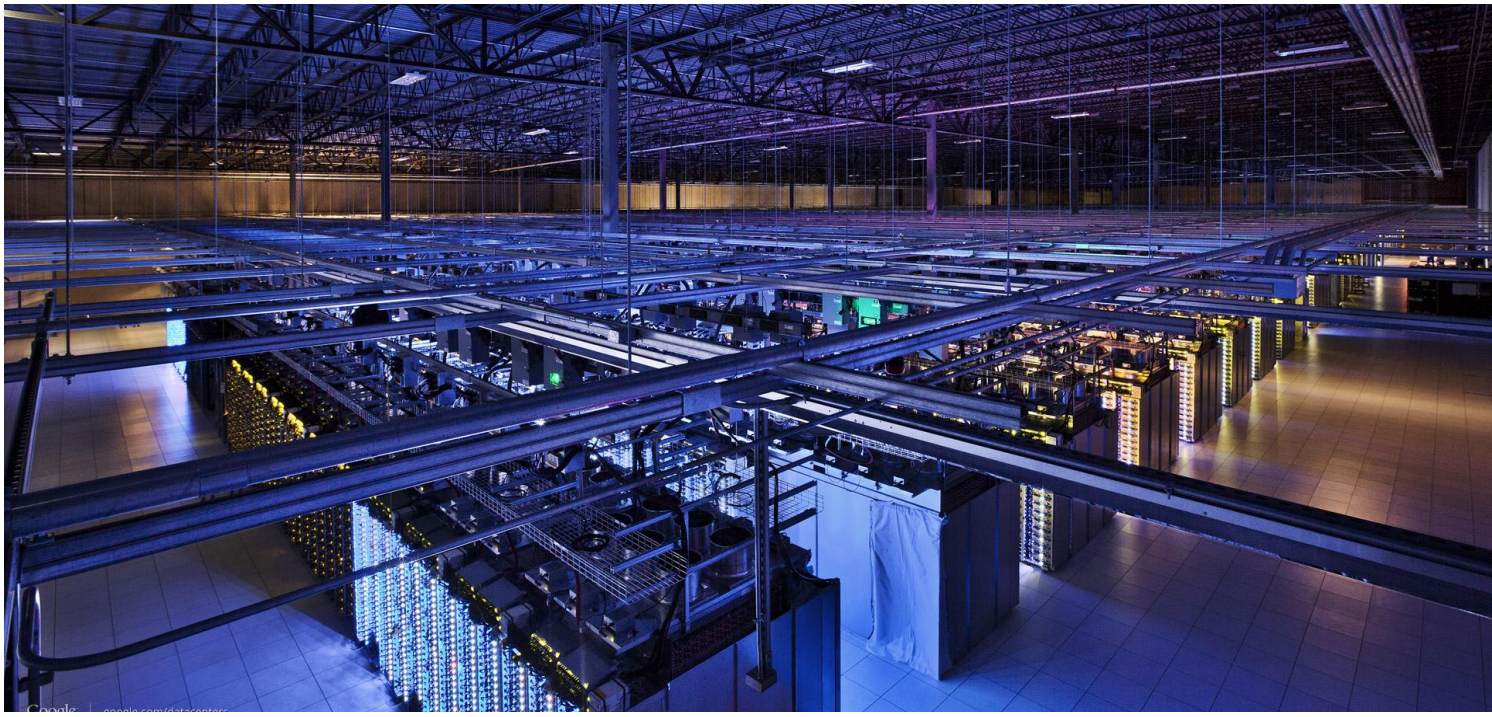
Singapore is a global tech epicenter, topping the rankings of the 2017 Global Smart City Performance Index. In addition, the city-state has launched the Digital Economy Framework for Action to make it the world's leading digital economy and a Smart Nation.

Cloud computing is an integral element of Singapore's digital objectives. As a result of governmental authorities' strong promotion of cloud adoption across the economy, the city-state led the Asia-Pacific region in the Asia Cloud Computing Association's 2018 Cloud Readiness Index., The 2018 BSA Global Cloud Computing Scorecard ranked Singapore sixth out of 24 leading IT economies for its cloud computing preparedness based on its legal and regulatory environment, including its data protection regime.

Singapore's Personal Data Protection Act (PDPA) governs the collection, use, disclosure, and care of personal data, as described in the official Quick Guide to the PDPA. At the core of the PDPA are the 9 Main Data Protection Obligations, which attempt to strike a balance between individuals' rights to protect their personal data and organizations' needs for this data for legitimate and reasonable business purposes.

Like Singapore, Google Cloud is a world leader with its Google Cloud Platform (GCP), Google Workspace services, and advanced data protection controls. With Google Cloud as their trusted partner, our customers can gain the strategic benefits of cloud computing, backed by our robust information protection and privacy infrastructure. In fact, Forrester Research recently named Google Cloud as a leader among public cloud platforms in native security capabilities and features. Moreover, GCP and Google Workspace are both certified as compliant with the highest security level of the city-state's Multi-Tier Cloud Security (MTCS) Singapore Standard 584. As a result, approximately 114 Google Cloud services and 20 datacenter sites have MTCS Tier 3 certifications, highlighting Google Cloud's ongoing and continuous commitment to ensuring sound operational and security controls across all three service models — infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software- as-a-service (SaaS).

With Google Cloud as a trusted partner, customers can gain the strategic benefits of cloud computing, backed by our robust information protection and privacy infrastructure. In fact, Forrester Research recently named Google Cloud as a leader among public cloud platforms in native security capabilities and features.



This whitepaper provides information to our customers about the PDPA 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 GCP and Google Workspace for their productivity needs in a manner that aligns with the PDPA's requirements. We explain our data protection features, how they map to the PDPA's requirements, and how we share compliance responsibilities with our customers.

Personal Data Protection Act overview

The PDPA applies to the processing of personal data by organizations within Singapore, even where an organization might collect the personal data overseas and transfer it into the city-state. The Personal Data Protection Commission (the Commission) administers, promotes, and enforces the PDPA. To learn more, refer to the Act and related subsidiary legislation and the Commission's guidance.

Cloud users should ensure that they fully comply with the PDPA; thus, we encourage them to utilize the Commission's recommended steps to manage personal data, Data Protection Starter Kit, PDPA Assessment Tool,

Purpose of the PDPA

"To govern the collection, use and disclosure of personal data by organizations in a manner that recognises both the right of individuals to protect their personal data and the need of organizations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances."

Guide to Developing a Data Protection Management Programme, and Guide to Data Protection Impact Assessments.

This section defines the PDPA's key terms and concepts. In particular, we briefly describe the PDPA's 9 Main Data Protection Obligations. To learn more, see the Act, the Commission's Overview of the Obligations, and the Advisory Guidelines for Key Concepts in the PDPA.

Topics

Key terms & concepts

Key term definitions

The PDPA explicitly defines the following terms:

Personal data	Data, "whether true or not, about an individual who can be identified — from that data; or from that data and other information to which the organization has or is likely to have access."
Organization	Any "individual, company, association or body of persons, corporate or unincorporated, whether or not — formed or recognised under the law of Singapore; or resident, or having an office or a place of business, in Singapore."
Processing	The "carrying out of any operation or set of operations in relation to the personal data," including, but not limited to, recording; holding; organization, adaptation, or alteration; retrieval; combination; transmission; erasure or destruction.
Data intermediary	An "organization which processes personal data on behalf of another organization but does not include an employee of that other organization."

Key concepts

Although the PDPA does not define the following concepts, the Commission provides explanatory guidance on interpreting them:

Purpose	The term refers to an organization's "objectives or reasons" for collecting, using, or disclosing personal data, not the activities it may intend to take with that data.
Reasonable	In attempting to comply with the PDPA, organizations must "act based on what a reasonable person would consider appropriate in the circumstances." The "reasonable person" concept is an "objective standard" and essentially represents "a person who exercises the appropriate care and judgment in the particular circumstances."

Data intermediaries under the PDPA

Data intermediary obligations

A data intermediary processes data on another organization's behalf. Where the processing contract is evidenced or in written form, the organization and the data intermediary have different responsibilities:

Organization	The organization bears the same obligations under the PDPA as if it processed the personal data itself.
Data intermediary	The data intermediary needs to only comply with the PDPA provisions classified as the "Protection Obligation" and the "Retention Limitation Obligation" (explained below). However, the data intermediary must comply with all of the PDPA's data protection obligations where it engages in other activities that do not constitute processing on behalf of or for the purposes of the organization pursuant to the contract.

Google Cloud as a data intermediary

Google Cloud qualifies as a data intermediary under the PDPA because it processes personal data on behalf of, or for the purposes of, the organization pursuant to a contract for cloud services. As a result, Google Cloud needs to comply with the PDPA's Protection and Retention Limitation Obligations. A subsequent section of this paper explains how Google Cloud satisfies its own PDPA obligations and how it helps customer organizations meet their PDPA obligations.

9 data protection obligations

Organizations that handle and control personal data must comply with the obligations under the PDPA. The 9 Main Data Protection Obligations can be classified as shown in the table below.

Category	Obligations
Collection, use, and disclosure of personal data	• Notification • Consent • Purpose limitation
Accountability	• Openness • Access to and correction of personal data
Care of personal data	• Accuracy • Protection • Retention limitation • Transfer limitation

Google Cloud data protection overview & the Shared Responsibility Model

Google Cloud's robust security and privacy controls give customers the confidence to utilize GCP 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.

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 GCP 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 Platform 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 Platform, you can:

1. **Know that your security comes first in everything we do.**
   We promptly notify you if we detect a breach of security that compromises your data.
2. **Control what happens to your data.**
   We process customer data according to your instructions. You can access it or take it out at any time.
3. **Know that customer data is not used for advertising.**
   You own your data. Google Cloud does not process your data for advertising purposes.
4. **Know where Google stores your data and rely on it being available when you need it.**
   We publish the locations of our Google data centers; they are highly available, resilient, and secure.
5. **Depend on Google's independently-verified security practices.**
   Our adherence to recognized international security and privacy standards is certified and validated by independent auditors — wherever your data is located in Google Cloud.
6. **Trust that we never give any government entity "backdoor" access to your data or to our servers storing your data.**
   We reject government requests that are invalid, and we publish a transparency report for government requests.

To learn more about our commitments to safeguarding customer information, refer to the Google Cloud Privacy page. See the Cloud Data Processing Addendum for further details.

Dedicated privacy team

The Google privacy team operates separately from product development and security organizations, 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.

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, GCP 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 organizational and technical controls that we use to protect your data at Google Cloud. Please refer to Google security whitepaper, and Google Cloud Security and Compliance 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 Cloud Security and Compliance 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 GCP security whitepaper. In addition, refer to the security team, vulnerability management, and monitoring sections in the Google Cloud Security and Compliance 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 Cloud Data Processing Addendum.

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 Cloud Security and Compliance whitepaper.

State-of-the-art data center security

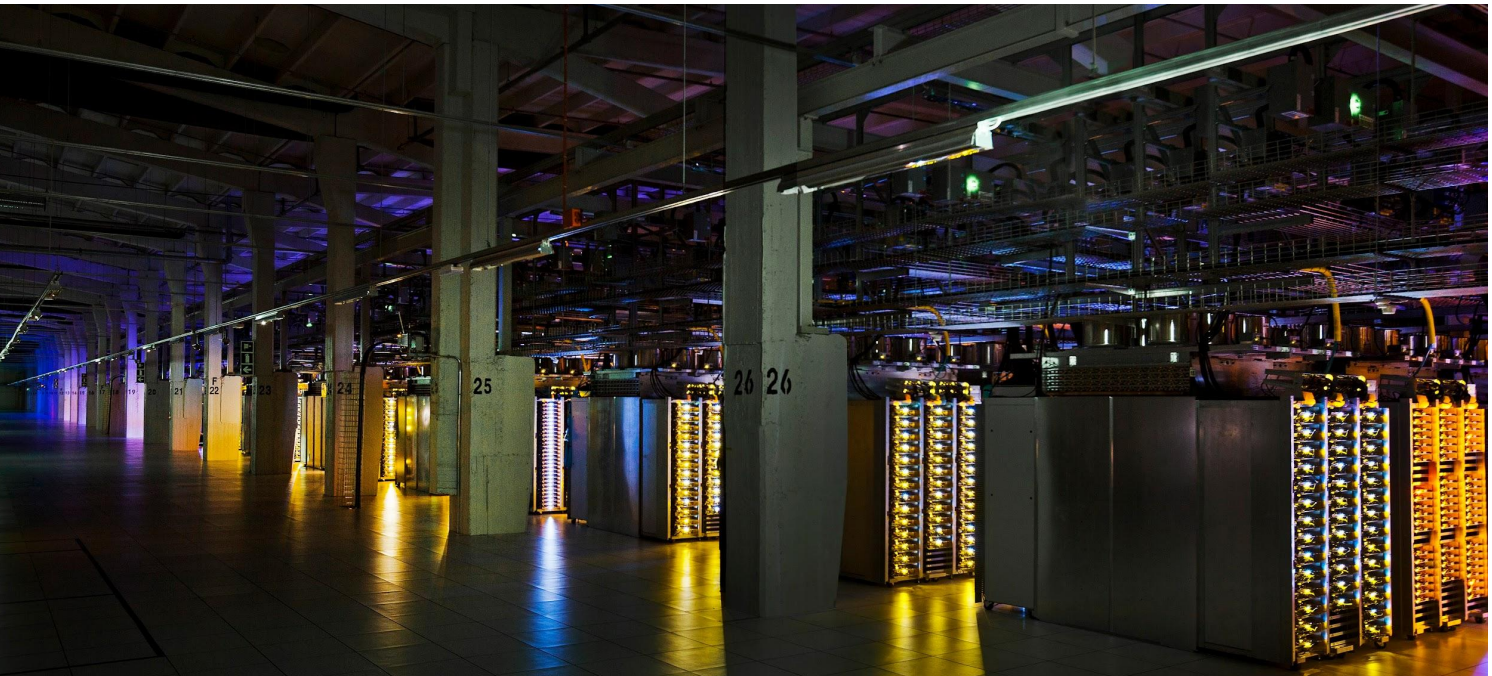
Google data centers feature layers of physical security protections. We limit access to these data centers to only a very small fraction of employees and have multiple physical security controls to protect our data center floors such as biometric identification, metal detection, vehicle barriers, and 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.

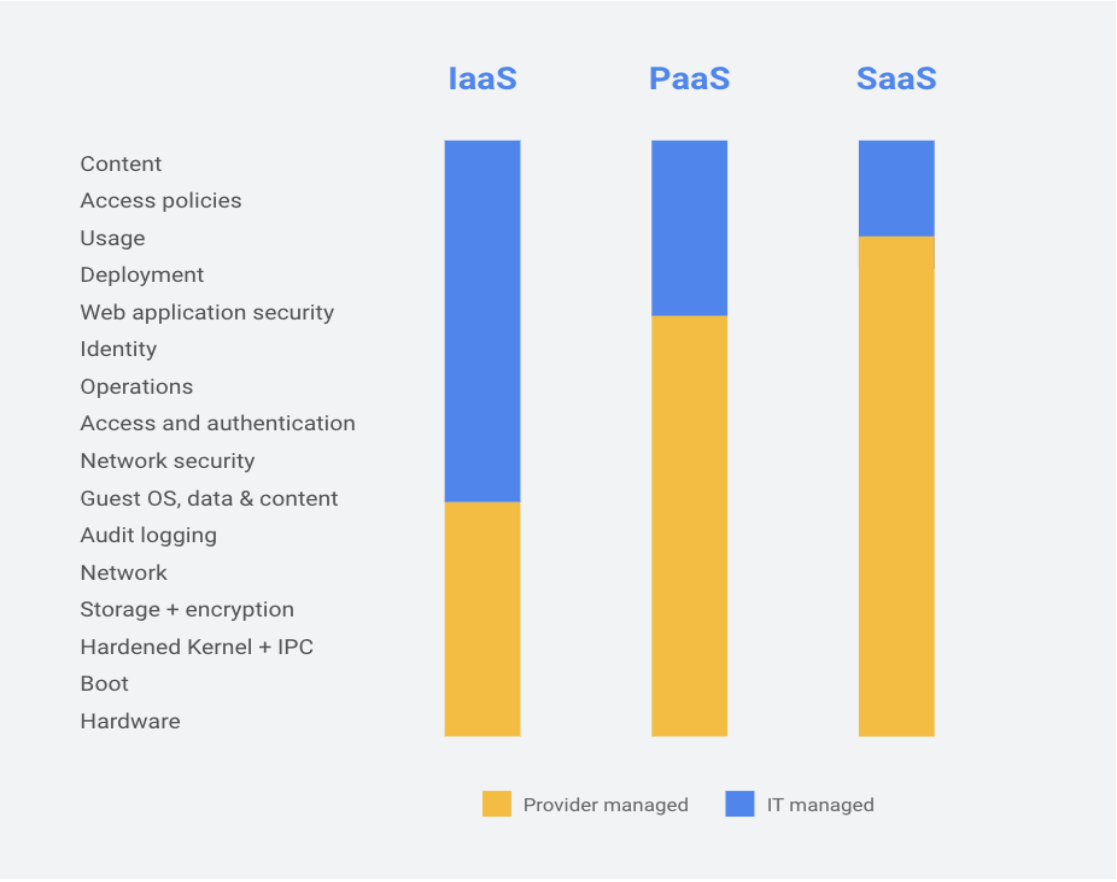
Cloud-native technology

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 GCP 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 the 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. 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 physically controlling facilities. Moreover, using our cloud services is a more cost-effective approach for customers because we manage a substantial portion of the security and compliance efforts. The figure below visually demonstrates an example of the Shared Responsibility IaaS, PaaS, and SaaS offerings. Keep in mind that responsibilities will vary depending on the specific services being used.



Google Cloud and the PDPA

The Personal Data Protection Commission (the Commission) advises organizations that they may bear responsibility if their service providers violate the PDPA. The Commission recommends that an organization ensure that the contract with a service provider contain provisions requiring the service provider to take sufficient measures to comply with the PDPA. Additionally, organizations should establish standard operating procedures for the service provider's handling of personal data and initiate processes to monitor the provider's compliance with the standard operating procedures.

Compliance is built upon our security and privacy infrastructure. We are committed to complying with applicable data protection laws and undergo regular audits, maintain certifications, provide industry-standard contractual protections, and share tools and information with customers. Google Cloud continues to make significant investments in security, privacy, and compliance management to support customers in meeting their current and emerging regulatory compliance and risk management obligations. Our approach to supporting regulatory compliance includes collaborating with customers to understand and address their specific compliance obligations, delineating responsibilities, conducting internal and independent audits, and delivering transparency.

Google Cloud continues to make significant investments in security, privacy, and compliance management.

Topics

Data intermediary compliance with the PDPA

Our internal compliance-focused teams

Google Cloud's certifications and independent third-party attestations

- Multi-Tier Cloud Security Singapore Standard 584
- ISO 27001
- ISO/IEC 27018

Mapping Google Cloud data protection capabilities to the PDA & our shared responsibilities

- Collection, use, and disclosure of personal data
- Accountability of data subjects

Care of personal data

Data intermediary compliance with the PDPA

Where an organization employs a data intermediary to process personal data, the Commission recommends that the organization perform a due diligence review of the data intermediary's data protection and security policies, practices, and processes to ensure that the intermediary is able to comply with the PDPA's requirements.

As a trusted cloud service provider, Google Cloud is committed to fulfilling our protection and retention limitation obligations under the PDPA. Moreover, we strive to support our customers in meeting their legal obligations under the PDPA.

Our internal compliance-focused teams

At Google Cloud, we employ an extensive team of lawyers, regulatory compliance experts, and public policy specialists who oversee privacy and security compliance. These teams engage with customers, industry stakeholders, and supervisory authorities to shape our cloud 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 certifications and independent third-party attestations

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 Standards, regulations & certifications page.

Multi-Tier Cloud Security Singapore Standard 584

The Multi-Tier Cloud Security (MTCS) Singapore Standard 584 is a cloud security certification managed by the Singapore Info-communications Media Development Authority. The standard has three tiers designed to certify cloud service providers at different levels of operational security, with Tier 3 having the most stringent requirements. In obtaining the MTCS certification, a cloud service provider must complete a self-disclosure form that details its level of security and covers, among other things, data retention, data portability, liability, availability, business continuity, disaster recovery, as well as incident and problem management.

GCP underwent assessments for the MTCS certification, which included an audit by an independent MTCS certifying body. At the conclusion, 114 Google Cloud services and 20 datacenter sites received Tier Level 3 certification, the highest level. The scope of services included in the certifications highlights Google Cloud's ongoing and continuous commitment to ensuring sound operational and security controls across all three service models — IaaS, PaaS, and SaaS. Because Google's Tier Level 3 certification is appropriate for regulated organizations, such as those involved in financial and health services, GCP meets the most rigorous security standards.

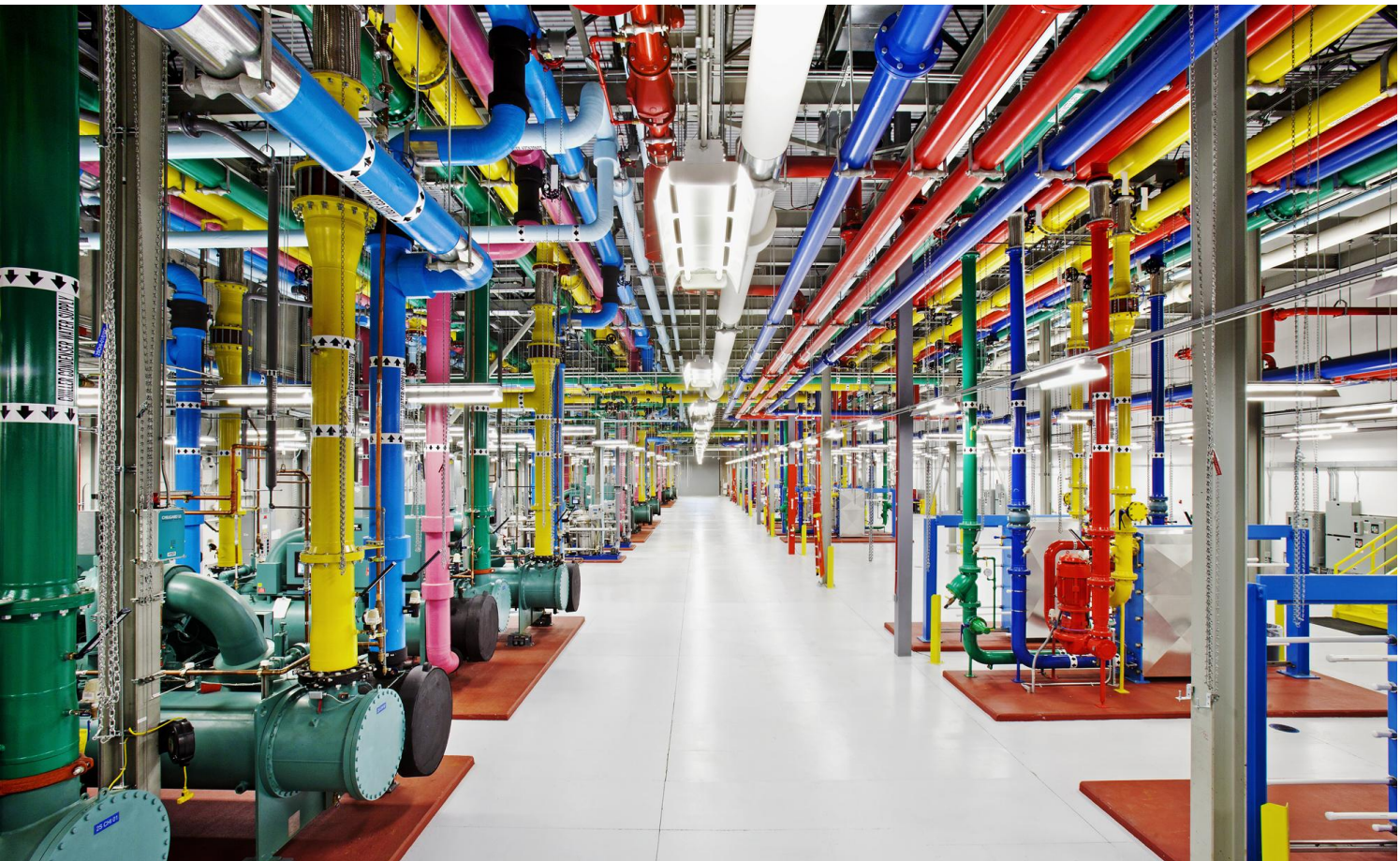
GCP and Google Workspace are certified as MTCS compliant. For a full list of Google Cloud products and services that have received MTCS Level 3 certifications, refer to our MTCS page.

ISO 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 allow Google to ensure a comprehensive and continually improving model for security management. GCP and Google Workspace are certified as ISO 27001 compliant.

ISO/IEC 27018

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. GCP and Google Workspace are certified as ISO 27018 compliant.



Mapping Google Cloud data protection capabilities to the PDPA & our shared responsibilities

In this table, we identify who bears the responsibility to meet the PDPA's 9 Main Data Protection Obligations. The table indicates each legal obligation and whether our customers or Google must satisfy the obligation, as well as where we can support our customers in meeting their legal requirements.

While customers are ultimately responsible for compliance with the PDPA, our commitment to complying with data protection and privacy principles and regulations gives customers the confidence to take advantage of GCP and Google Workspace services.

Collection, use, and disclosure of personal data

Data protection obligations	Who has the responsibility
Notification of purpose **Section 20** ● The organization must notify individuals of the purposes for the collection, use, or disclosure of their personal data. A notification should also provide other information, such as the business contact information of the data protection officer, how an individual may withdraw consent, how an individual may access or correct his personal data, and the organization's retention policies, among other matters.	**Customer responsibility** to provide notification of the purposes for the collection, use, or disclosure of individual personal data. ● To learn more, refer to the Commission's Advisory Guidelines on the Notification Obligation and its Guide to Notification. **Google Cloud Support** ● Google features such as the Identity-Aware Proxy can support customers in this activity.
Consent **Sections 13-17** ● The organization must obtain individuals' consent to collect, use, or disclose their personal data, unless an exemption applies. The request for personal data should be reasonable for providing the product or service. ● The organization must allow individuals to withdraw consent. Upon withdrawal of consent, the organization must cease such collection, use, or disclosure of the personal data.	**Customer responsibility** to obtain individuals' consent to collect, use or disclose their customers' personal data. ● To learn more, we recommend the Commission's Advisory Guidelines on the Consent Obligation. **Google Cloud Support** ● Google features such as the Identity-Aware Proxy can support customers in this activity.

Data protection obligations	Who has the responsibility
Purpose limitation Section 18 • An organization may collect, use, or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, only after it has notified the individual of those purposes. • The organization must collect, use, or disclose personal data only for the purposes for which the individuals gave consent.	**Customer responsibility** to ensure collection, use, or disclosure of personal data is limited to the purposes for which the individuals gave their consent. **Google Cloud support** • The data you entrust to Google Cloud belongs to your organization. We process your organization's data according to your explicit instructions under our contractual obligations to you. Our automated systems process your data to provide you services and protection, such as performing spam and malware detection, sorting email for features like Priority Inbox, and returning fast search results for information in your accounts. We may only access data in your account in strict compliance with our privacy policy and your customer agreement. We offer customers detailed terms of service that describe our commitment to protecting your data. To read more, please visit Section 5.2 of the Cloud Data Processing Addendum.

Accountability of data subjects

Data protection obligations	Who has the responsibility
Openness Sections 11 and 12 • The organization must appoint a data protection officer (DPO) who is responsible for the organization's compliance with the PDPA and make the DPO's business contact information publicly available so that data subjects can contact the DPO for PDPA-related queries or complaints. • The organization must publish information on its data protection policies, practices, and complaint-handling process.	**Customer responsibility** to appoint a data protection officer (DPO) and satisfy this obligation. • To learn more, we recommend the Commission's Advisory Guidelines on the Openness Obligation. **Google Cloud support** • Google believes transparency is essential to build trust and recommends that data users inform their data subjects about their use of GCP and Google Workspace. • 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 emphasize 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 information governance best practices. • In addition, customers may contact Google's data privacy officer for questions or comments.
Requests for access to and correction	**Customer responsibility** to provide access to and correction of

of personal data Sections 21-22 • Upon request, an organization must provide individuals with their personal data and inform them of the ways in which it collected, used, or disclosed their personal data with the past year (i.e., 12 months). • An organization must correct any error or omission in individuals' personal data upon their request (unless an exception applies).	personal data collected, used, or disclosed within the past year. • To learn more, we recommend the Commission's Advisory Guidelines on the Access and Correction Obligations and its Guide to Handling Access Requests. **Google Cloud support** • 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. • Google Cloud is certified to ISO 27018, which demonstrates the controls and guidelines Google implements to protect personal data held within a public cloud environment. More context on the ISO 27018 standard and audit can be found at ISO/IEC 27018:2014 general information.
Data protection obligations	**Who has the responsibility**
Requests for access to and correction of personal data (continued)	• 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 GCP and Google Workspace customers per our terms 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 PDPA. • We encourage you to view sections 9.2.1 and 9.2.2 of these terms of service for more information about data subject rights.

Care of personal data

Data protection obligations	Who has the responsibility
Accuracy **Section 23** ● An organization must make reasonable efforts to ensure that an individual's personal data collected is accurate and complete, if it is likely to use that data to make a decision that impacts that individual or to disclose that data to another organization.	**Customer responsibility** to satisfy this obligation. ● To learn more, we recommend the Commission's Advisory Guidelines on the Accuracy Obligation. **Google Cloud support** ● GCP and Google Workspace administrative consoles and services possess the functionality to maintain the accuracy of their data.
Protection **Section 24** ● An organization must implement reasonable security processes to protect the personal data against unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The organization should have: 1) comprehensive policies and procedures to ensure appropriate levels of security for personal data of different sensitivities 2) security measures appropriate to the nature of the personal data and the potential impact to individuals from unauthorized use or disclosure 3) reliable, well-trained personnel 4) robust security breach response plans, including a data breach management program and a procedure to notify the Commission as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals. ● With respect to data intermediaries, the organization should contractually define the responsibility of reporting, investigating, and taking remedial actions.	**Shared Google and customer responsibility.** ● To learn more, we recommend the Commission's Advisory Guidelines on the Protection Obligation, its Guide to Securing Personal Data in Electronic Medium, and its Guide to Basic Data Anonymisation Techniques. **How Google Cloud meets the Data Protection Obligation Industry certifications and third-party attestations** ● **Security team:** Google employs more than 850 security and privacy professionals who maintain the company's defense systems, develop security review processes, build security infrastructure, implement Google's security policies, and actively scan for security threats. We also take part in research and outreach activities to protect the wider community of Internet users, beyond just Google customers. ● **Industry certifications and third-party attestations**: GCP and Google Workspace products regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards to earn customer trust. We are constantly working to expand our coverage. GCP and Google Workspace are both Multi-Tier Cloud Security (MTCS) and ISO/IEO 27018 compliant/certified. To learn more about the certifications we have achieved, the laws and regulations we comply with, and the frameworks we align to, refer to our Standards, regulations & certifications page. ● **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. Should a physical security incident occur, we will provide access logs, activity records, and camera footage to the customer's designated personnel as defined in the service level agreement.

Data protection obligations	Who has the responsibility
Protection (continued)	• **Defense in depth:** Google Cloud builds our cloud infrastructure security through layers to provide defense in depth. The security of the infrastructure is designed in progressive layers starting from the physical security of data centers, continuing on to the security of the hardware and software that underlie the infrastructure, and finally, the technical constraints and processes in place to support operational security. Our infrastructure was designed to be multi-tenant from the start, and multiple mechanisms are utilized to establish and maintain trust between services. We design and manufacture purpose-built servers and network hardware without unnecessary components, such as video cards, chipsets, or peripheral connectors, eliminating vulnerabilities introduced by third-party manufacturers. Furthermore, we operate the infrastructure securely by defending against threats to the infrastructure from both insiders and external actors. We protect our employees' credentials from compromise by replacing phishable, one-time-password second factors with mandatory use of U2F-compatible security keys. We aggressively limit and actively monitor the activities of employees who are granted administrative access to the infrastructure. Google Cloud continually works to eliminate the need for privileged access for particular tasks by providing automation that can accomplish the same tasks in a safe and controlled way. This includes requiring two-party approvals for some actions and introducing limited APIs that allow debugging without exposing sensitive information. • **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. • **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.

Data protection obligations	Who has the responsibility
Protection (continued)	• **Unauthorized access prevention:** To prevent unauthorized 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. These techniques include normal Linux user separation, language and kernel-based sandboxes, and hardware virtualization. Furthermore, we perform encryption at the application layer, which allows our infrastructure to isolate itself from potential threats at the lower levels of storage such as malicious disk firmware. To prevent unauthorized access to your data from external threat actors, we employ a defense-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 unauthorized changes can be made without detection. This starts from low-level components, such as the BIOS, and includes all key components of the boot process, such as the bootloader, kernel, and the base operating system. All of these are controlled, built, and hardened by us. In addition, 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 unauthorized 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 employees' access rights and levels are based on their job functions and roles. Technical controls are applied to enforce the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. Furthermore, Google's security team actively monitors Google employees' access patterns and investigates unusual events. Finally, Google employees are required to sign a confidentiality agreement and complete mandatory training on our Code of Conduct, data protection, data confidentiality, and data privacy. Google's Code of Conduct specifically addresses responsibilities and expected behavior with respect to the protection of information.

Data protection obligations	Who has the responsibility
Protection (continued)	• **Incident response plan and data breach notification:** We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. We assign the highest priority to events that directly impact our customers. Our process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event. We test incident response plans for key areas, such as systems that store sensitive customer information.The Google security team operates 24/7. Additionally, we will promptly notify customers if we detect a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized 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 process whitepaper. • **Business continuity and disaster recovery:** At Google Cloud, we plan on our services being always available, even when we are upgrading our services or maintaining our systems. The service level agreements (SLAs) for Google Cloud's service offerings meet or exceed system availability requirements for enterprises across various industries. We have data centers geographically distributed across the Americas, Europe, and Asia to minimize the effects of disruptions caused by local and regional incidents. Our application and network architecture design maximizes reliability and uptime. We utilize robust software failover within our cloud computing platform to minimize the impact of unlikely hardware disruptions. All systems within the Google infrastructure that support Google Cloud services are redundant by design, and each subsystem is not dependent on any particular physical or logical server for ongoing operation. Data is replicated multiple times across active servers so in the case of a machine failure, data will still be accessible through another system. Data is also replicated across secondary data centers to ensure protection from data center failures. For more information regarding our SLAs, please see our GCP SLAs and Google Workspace SLA. Furthermore, we have a business continuity plan for our data centers and production operations to account for major disasters such as earthquakes or other incidents like health crises. This plan allows us to continue delivery of our services to our customers. Likewise, our DR program enables continuous and automated disaster readiness, response, and recovery of our business, systems, and data.

Data protection obligations	Who has the responsibility
Protection (continued)	We conduct DR testing on a regular basis to provide a coordinated venue for infrastructure and application teams to test communication plans, failover scenarios, operational transition, and other emergency responses. All teams that participate in the DR exercise develop testing plans and post mortems which document the results, lessons learned, and remediation plans (if applicable). Finally, GCP provides many of the facilities customers need to implement a business continuity plan or disaster recovery plan, such as redundancy, scalability, compliance, and security. The Disaster Recovery Cookbook provides some scenarios to show how GCP can help. ● **Identity and security products and services:** GCP offers capabilities that include cloud identity and access management, cloud data loss prevention, cloud security scanner, stackdriver logging, and cloud key management service that help meet your policy, regulatory, and business objectives. Moreover, Google Workspace's centralized administrator console provides unique security capabilities including two-step verification, single sign-on, usage monitoring, mobile app management, and audit logging. ● **Subcontractors:** Google reviews the information governance practices and security posture of third-party vendors and services 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 sub-processors and the services they provide is available for both GCP and Google Workspace. The IPA defines the security and privacy obligations sub-processors must meet to satisfy Google's requirements regarding customer data.

Data protection obligations	Who has the responsibility
Retention limitation **Section 25** ● An organization must cease to retain personal data or remove the means by which the personal data can be associated with particular individuals when the data is no longer necessary for any business or legal purposes.	**Shared Google and customer responsibility.** ● To learn more, we recommend the Commission's Advisory Guidelines on the Retention Limitation Obligation, Advisory Guidelines on Anonymization, and Guide to Basic Data Anonymisation Techniques.

• Ceasing to retain personal data means safely disposing of personal data or anonymizing it. • The organization should set a retention period for various types of personal data.	**How Google Cloud satisfies the Data Retention Limitation Obligation** • Google will retain, return, destroy, or delete the personal data in accordance with the contract or service level agreements. GCP and Google Workspace administrative consoles and services possess the functionality to delete any data that they and their users put into our systems. If customers delete their data, we commit to deleting it from our systems within 180 days. We also provide tools that make it easy for customers to take their data with them if they choose to stop using our services, without penalty or additional cost. To learn more about data deletion at Google, refer to our Data deletion on Google Cloud Platform whitepaper. • All Google data centers adhere to a strict policy for equipment disposal and reuse. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process that includes a crusher and shredder followed by recycling at a secure facility.
Transfer limitation **Section 26** • When transferring personal data overseas, an organization must 1) take steps to ensure that it protects the data in compliance with the PDPA while the data is still in its possession or control; and 2) ensure that the standard of protection afforded to that data in a separate jurisdiction or region is comparable to the PDPA.	**Customer responsibility** to satisfy this obligation. • To learn more, we recommend the Commission's Advisory Guidelines on the Transfer Limitation Obligation. **Google Cloud support** • GCP services are available in various geographical regions and zones across North America, South America, Europe, Asia, and Australia. With respect to cloud locations, GCP has 18 regions, 55 zones, over 100 points of presence across 35 countries, and a well-provisioned global network with 100,000s of miles of fiber optic cable. • Google Workspace's data centers are located in the U.S., Europe, Chile, Singapore, and Taiwan. Customers may verify the data protection standards in these countries and regions prior to any transfer. • Google offers a range of international data-transfer mechanisms and is committed to having a lawful basis for data transfers in compliance with applicable data protection laws worldwide. Indeed, Google follows the highest standards for cross-border data transfer protections as required by the EU's General Data Protection Regulation: we contractually commit under our current data processing agreements to maintain a mechanism that facilitates transfers of personal data outside of the EU. Moreover, the European data protection authorities have confirmed the compliance of our model contract clauses, affirming that our contractual commitments for Google Workspace and GCP fully meet the requirements to legally transfer personal data from the EU to the rest of the world. • Google informs its customers of the storage locations and legal

	jurisdictions of the personal data. For many GCP and Google Workspace services, customers can choose where their data is stored.

Frequently asked questions

The PDPA sets forth rigorous data protection requirements but leaves some issues unaddressed. In addition to the PDPA, several industries may face sector-specific privacy or security requirements. In this section, we identify several potential questions regarding compliance risks and briefly describe how we can support our customers in assessing and mitigating them. Customers ultimately bear the responsibility for complying with the PDPA and should seek legal counsel to understand their specific compliance obligations.

Does the PDPA impose data breach notification requirements?

The PDPA does not explicitly require organizations to have incident response plans or to report data breaches. Nevertheless, the PDPA's Protection Obligation requires organizations and data intermediaries to safeguard personal data with reasonable security arrangements. To meet this obligation, the Commission encourages organizations to establish data breach management and response plans and to notify it promptly of any data breaches that might cause public concern or pose a risk to a group of individuals. Such measures may serve as mitigating factors in the Commission's determination of a financial penalty for a violation of the Protection Obligation caused by a data breach. To learn more, read the Commission's Guide to Managing Data Breaches.

What's more, the Commission intends to amend the PDPA to include explicit data breach notification requirements that will prescribe the criteria for notification, the time period for giving notice, and exceptions to the requirement. Upon incorporating them into the law, the Commission will issue guidelines to help organizations comply with the new obligations.

Google's security team 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. In the event of a breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, customer data on systems managed by or otherwise controlled by Google, our expert team of incident responders works to protect customers' data, restore normal service as quickly as possible, and meet both regulatory and contractual compliance requirements.

Google Cloud maintains and continues to invest in advanced threat detection and avoidance technologies, from machine learning to data analytics. We also test our incident response plans regularly, so that we are always ready. Google Cloud promptly informs our customers of incidents

involving their customer data in line with the data incident terms in our current and any updated agreements. To learn about Google's principled approach to managing and responding to data incidents for Google Cloud, refer to the Data incident response process whitepaper.

Does the PDPA permit cross-border transfers of personal data?

The PDPA's Transfer Limitation Obligation lays out the parameters for cross-border transfers of personal data. An organization may transfer personal data outside of Singapore if it takes appropriate measures to guarantee its compliance with the data protection requirements. Furthermore, if the organization intends to transfer personal data to an overseas recipient, it must take appropriate steps to ascertain and ensure that the data recipient, such as the data intermediary, will afford the personal data "a standard of protection that is at least comparable to" the PDPA pursuant to "legally enforceable obligations," including those imposed by law, contract, binding corporate rules, or any other legally binding instrument.

In short, the PDPA requires that the organization carry out appropriate due diligence of the data protection and privacy law or rules in place in the foreign country. To learn more, refer to the Commission's Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data, and Guide to Data Sharing.

Google Cloud offers a range of international data-transfer mechanisms and continues 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 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 to best meet their latency, availability, durability, and security requirements.

What terms and conditions do we provide our 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 Cloud Data Processing Addendum supplement the licensing agreement and describe our commitment to protecting customer data. In the terms, we and our customers agree to 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.

What is the Cybersecurity Act of 2018 and what does it require for cloud service providers (CSPs)?

As one of the most digitally connected nations, Singapore recognizes the importance of building a cyber-resilient digital infrastructure. The Cybersecurity Act of 2018 (the Act) establishes a regulatory framework to prevent, manage, and respond to cybersecurity threats and incidents in Singapore. The Act regulates computers or computer systems explicitly designated as critical information infrastructure (CII) in Singapore, which currently include essential services related to energy, info-communications, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, government functions, and media.

The Cybersecurity Act of 2018

In general, critical information infrastructure owners need to

- Comply with codes of practice and performance standards
- Perform cybersecurity audits and risk assessments
- Participate in cybersecurity exercises
- Notify the commissioner of the Cyber Security Agency of Singapore of prescribed cybersecurity incidents that occur in the CII or systems under their control

The Act empowers the commissioner to prevent and investigate cybersecurity incidents, among other related matters. Because the Act does not classify the computer systems in the supply chain that support a CII's operations as CII, third-party vendors such as cloud service providers currently fall outside the Act's scope.

Does Singapore have industry-specific privacy laws or regulations?

Although the PDPA establishes an industry-wide data protection framework, certain organizations might also need to comply with applicable sector-specific laws and regulations or common law. Here, we highlight two sectors that must comply with the PDPA and sector-specific rules.

Financial services

The Monetary Authority of Singapore (MAS) approves of financial institutions' use of cloud services in its Guidelines on Outsourcing. For more information, refer to Google Cloud's Guidelines for Financial Institutions in Singapore Using Cloud Services whitepaper. In addition to the outsourcing guidelines, financial institutions should review other applicable laws and guidance to determine their responsibilities when using a CSP.

In addition, the MAS requires financial institutions to notify the MAS of data incidents that have a severe and widespread impact on the institution's operations or materially affects its service to customers. Banks seeking further guidance on complying with the PDPA should consult the Association of Banks in Singapore's Code of Banking Practices - PDPA.

Healthcare services

Singapore authorities promote cloud use within the healthcare sector. Although adoption of the Multi-Tiered Cloud Computing Security (MTCS) Singapore Standard (SS584) is voluntary, CSPs must be MTCS-certified to provide cloud services to the government, such as public healthcare institutions.

To advance cloud use in the private healthcare sector, the Info-communications Media Development Authority and the Ministry of Health mapped the MTCS to the Healthcare IT Security Policy & Standards (HITSecP). The mapping aims to help MTCS-certified CSPs understand the HITSecP's expectations. Healthcare service providers that seek to host their applications on such CSPs must perform due diligence and deploy additional security and risk controls that are appropriate based on their own security policies and risk assessments. To learn more, refer to the Alignment of MTCS to Healthcare IT Security Policy & Standards Gap Analysis Report.

Finally, to better understand their obligations under the PDPA, we encourage healthcare service providers to review the Commission's Advisory Guidelines for the Healthcare Sector.

Conclusion

We have described how information is securely stored, processed, maintained, and accessed in Google Cloud. Whether the customer processes personal data within Singapore or processes personal data of individuals in Singapore but outside the city-state, this information can help them determine whether the Google Cloud Platform and Google Workspace products or services are suitable for them in light of the PDPA.