



# Malaysia's Personal Data Protection Act



## Table of Contents

<b>Introduction</b>	<b>3</b>
<b>Overview of the Malaysia Personal Data Protection Act</b>	<b>3</b>
<b>Google Cloud data protection overview &amp; the Shared Responsibility Model</b>	<b>4</b>
Google Cloud's approach to security and data protection	5
Google Cloud's approach to data protection and privacy	5
The Shared Responsibility Model	9
<b>How Google Cloud helps customers meet the requirements of the Malaysia Personal Data Protection Act (PDPA)</b>	<b>11</b>
<b>Conclusion</b>	<b>20</b>

### Disclaimer

This whitepaper applies to Google Cloud products described at [cloud.google.com](https://cloud.google.com). The content contained herein is correct as of April 2022 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

## Introduction

At Google Cloud, privacy plays a critical role in the development and operation of our products and services. We've set a high bar for what it means to host, serve, and protect customer data by centering security and data protection at the core of how we design and build our products. We start from the fundamental premise that as a Google Cloud customer, you<sup>1</sup> own your customer data. We implement stringent security measures to safeguard your customer data and provide you with tools and features to control it on your terms.

This whitepaper provides information to our customers about Malaysia's Personal Data Protection Act 2010 (PDPA) and how Google Cloud leverages Google's industry-leading data privacy and security capabilities to store, process, maintain, and secure customer data<sup>2</sup>. We are committed to partnering with our customers so they can deploy workloads using Google Cloud services and Google Workspace for their productivity needs in a manner that aligns with the PDPA's requirements. We explain our data protection features and highlight how they map to the PDPA's requirements. However, please note that, as a provider of cloud services, we are not in a position to provide you with legal advice - this is something only your legal counsel can provide.

## Overview of the Malaysia Personal Data Protection Act

The [Personal Data Protection Act 2010 \(PDPA\)](#), was passed by the Malaysian Parliament on 2 June, 2010 and came into force on 15 November, 2013. It governs the collection, use, and disclosure of personal data and requires [certain entities](#) to register their processing activities. It also grants [rights](#) to data subjects, including rights to access, correction, consent withdrawal, and objection to certain types of processing. Violations of the law may result in criminal penalties, including fines or imprisonment.

The PDPA applies to the processing of personal data in commercial transactions by persons (i) established in Malaysia, including any other person employed or engaged by a person established in Malaysia (regardless of whether or not the personal data is processed in the context of that establishment); or (ii) not established in Malaysia, but who use equipment in Malaysia to process personal data for purposes other than transit through Malaysia. Most private organisations are subject to the law (with the exception of credit reporting agency businesses); processing of personal data by the Malaysian federal or state government is outside the scope.

Unlike many global data protection laws, which govern the data processing activities of both controllers and processors, the PDPA imposes obligations only on "data users" (similar to the concept of "data controllers"). However, the law does contemplate the processing of personal data by data processors and includes some provisions regarding these processing activities (e.g., the Commissioner may carry out inspections on systems of both data users and data processors).

---

<sup>1</sup> In this whitepaper, "you/your" refers to Google Cloud and Google Workspace customers as well as Google Cloud partners. Unless indicated otherwise, references to "customers" will include Google Cloud partners and references to "customer data" will include Google Cloud partner data.

<sup>2</sup> In this whitepaper "customer data" and "your data" refers to the customer data we process according to your Google Cloud agreement(s).

At the core of the PDPA are seven Personal Data Protection Principles (Principles) that govern the processing of personal data. Only data users are required to comply with the Principles; they do not directly apply to processors. And while these Principles are generally applicable, there are some exceptions to their applicability in certain circumstances, such as for purposes relating to law enforcement, tax, emergency health circumstances, and research, among others.

The first Principle, the “General Principle,” sets forth the conditions under which an organisation may process personal data. It requires that a data subject provide consent for the processing of their personal data (except for sensitive data, which may only be processed under certain conditions), unless the processing is necessary for certain purposes, such as the fulfillment of a contract, to protect the vital interests of the data subject, or as required by law. The other Principles relate to transparency, disclosure, security, retention, integrity, and access and correction rights.

There are several companion laws that supplement the PDPA. The Attorney General’s Chambers has promulgated related regulations, such as those regarding [data user registration](#), [data user groups](#), [offenses](#), [data access fees](#), and the [Personal Data Protection Principles](#). The Office of the Personal Data Protection Commissioner has also published [Standards](#) relating to security, retention, and data integrity, and [FAQs](#) related to the law.

When you transfer customer data to Google Cloud as part of your use of our services, we process data on your behalf. 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 Google Cloud services 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.

## Google Cloud data protection overview & the Shared Responsibility Model

Google Cloud’s robust security and privacy controls give customers the confidence to utilise Google Cloud services and Google Workspace in a manner aligned with the requirements of the PDPA. Moreover, we are constantly working to expand our privacy and security capabilities. To help customers with compliance and reporting, Google shares information and best practices, and provides easy access to documentation. In this section, we describe our comprehensive data protection and privacy capabilities and our robust data security features most relevant to the PDPA. We then explain how we share security and compliance responsibilities according to the Shared Responsibility Model.

## Google Cloud's approach to security and data protection

Google's focus on security and protection of information is among our primary design criteria. Security is at the core of everything we do; it is embedded in our culture and our architecture and we focus on improving it every day. In this section, we provide an overview of the organisational and technical controls we use to protect your data. To learn more about our approach to security and compliance, refer to the [Google security whitepaper](#) for Google Cloud services and the [Google Workspace Security whitepaper](#).

### Topics

#### Google Cloud's approach to data protection and privacy

- Data privacy trust principles
- Dedicated privacy team
- Data access and customer control
- Restricted access to customer data
- Law enforcement data requests

#### Google Cloud's approach to data security

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

## Google Cloud's approach to data protection and privacy

Data protection and privacy are fundamental to Google. We design our products and services from the start with privacy and trust as guiding principles. Google Cloud works to ensure the protection and privacy of customers' data in three ways: 1) we provide superior data protection through a secure core infrastructure that is designed, built, and operated to help prevent threats; 2) we give customers robust security controls to help them meet policy, regulatory, and business objectives; and 3) we work to fulfill our compliance responsibilities and to make compliance easier for our customers.

### Data protection and privacy trust principles

We want our customers to feel confident when using Google Cloud and Google Workspace products. We believe that trust is created through transparency, and we want to be open about our commitments and offerings to our customers when it comes to protecting their data in the cloud.

**Our commitments to you about your data**

Your data is critical to your business, and you take great care to keep it safe and under your control. We want you to feel confident that taking advantage of Google Workspace and Google Cloud services doesn't require you to compromise on security or control of your business's data.

At Google Cloud, we believe that trust is created through transparency, and we want to be transparent about our commitments and what you can expect when it comes to our shared responsibility for protecting and managing your data in the cloud.

When you use Google Workspace or Google Cloud services, you can:

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

To learn more about our commitments to safeguarding customer information, refer to the [Google Cloud Privacy page](#). See data processing terms for [Google Workspace](#) and [Google Cloud](#).

**Dedicated privacy team**

The Google privacy team operates separately from product development and security organisations, but participates in every Google product launch by reviewing design documentation and performing code reviews to ensure that privacy requirements are followed. They help release products that reflect strong privacy practices: transparent collection of user data, providing users and administrators with meaningful privacy configuration options, and continuing to be good stewards of any information

stored on our platform. To learn more about our privacy team, refer to the privacy team section of the [Google security whitepaper](#) for Google Cloud services and the [Google Workspace Security whitepaper](#).

## **Data access and customer control**

Google Cloud customers own their data, not Google. Google will only process customer data in accordance with contractual obligations. We also provide customers with solutions that allow granular control of resource permissions. For example, using Cloud Identity and Access Management, customers can map job functions to groups and roles so users only access the data they need to get the job done. Furthermore, customers may delete customer data from our systems or take it with them if they choose to stop using our services.

## **Restricted access to customer data**

To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when the data is stored on the same physical server. Only a small group of Google employees has access to customer data pursuant to explicit reasons based on job function and role. Any additional access is granted according to stringent procedures and tracked through audit records. In fact, Google Cloud is the only cloud service provider (CSP) to offer near real-time logs when its administrators access customers' content through Access Transparency.

## **Google Cloud's approach to data security**

In this section, we provide an overview of the organisational and technical controls that we use to protect your data at Google Cloud. Please refer to the [Google security whitepaper](#), and [Google Workspace Security whitepaper](#) for additional information on our security practices.

### **Strong security culture**

Security is central to Google culture. It is reinforced in employee security training and company-wide events to raise awareness and drive innovation in security and privacy.

To learn more about our security culture, refer to the security culture sections in our [Google security whitepaper](#) and our [Google Workspace Security whitepaper](#).

### **Security team**

Google employs more than 850 security professionals, including some of the world's foremost experts. This team maintains the company's defense systems, develops security review processes, builds security infrastructure, implements Google's security policies, and actively scans for security threats. Our team also takes part in research and outreach activities to protect the wider community of Internet users, beyond just those who choose Google solutions. Our research papers are available to the public. As part of our outreach efforts, we have a team known as Project Zero that aims to prevent targeted attacks by reporting bugs to software vendors.

In addition, our security team works 24/7 to quickly detect and resolve potential security incidents. Our security incident management program is structured around industry best practices and tailored into our "Incident Management at Google (IMAG)" program, which is built around the unique aspects of Google and its infrastructure. We also test our incident response plans regularly, so that we always remain prepared.

To learn more, refer to the security team, vulnerability management, and monitoring sections in the [Google security whitepaper](#). In addition, refer to the security team, vulnerability management, and monitoring sections in the [Google Workspace Security whitepaper](#).

## **Trusted infrastructure**

We conceived, designed, and built Google Cloud to operate securely. Google is an innovator in hardware, software, network, and system management technologies. We custom design our servers, proprietary operating system, and geographically distributed data centers. Using "defense in depth" principles, we have created an IT infrastructure that is more secure and easier to manage than most other deployment options. Our infrastructure provides secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the Internet, and safe operation by administrators. We ensure the security of this infrastructure in progressive layers, starting from the physical security of our data centers, building with underlying security-designed hardware and software, continuing with secure service deployment, secure data storage, and secure internet communication, and finally, operating the infrastructure in a secure fashion.

To learn more, refer to the [Google Cloud Infrastructure Security Design Overview](#), as well as the Google Cloud [Data Processing and Security Terms](#), Appendix 2: Security Measures and Google Workspace [Data Processing Amendment](#), Appendix 2: Security Measures.

## **Infrastructure redundancy**

Google's infrastructure components are designed to be highly redundant. This redundancy applies to server design and deployment, data storage, network and Internet connectivity, and the software services themselves. This "redundancy of everything" creates a robust solution that is not dependent on a single server, data center, or network connection. Our data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as natural disasters and local outages. In the event of hardware, software, or network failure, platform services and control planes are capable of automatically changing configuration so that customers can continue to work without interruption. Our highly redundant infrastructure also helps customers protect themselves from data loss. Customers can create and deploy our cloud-based resources across multiple regions and zones, allowing them to build resilient and highly available systems. To learn more, refer to the low latency and highly available solution in the [Google security whitepaper](#) and the [Google Workspace Security whitepaper](#).



## State-of-the-art data center security

Google data centers feature layers of physical security protections. We limit access to these data centers to only a very small fraction of employees and have multiple physical security controls to protect our data center floors such as biometric identification, metal detection, vehicle barriers, and custom-designed electronic access cards. We monitor our data centers 24/7/365 to detect and track intruders. Data centers are routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more, refer to our [Data Center Innovation](#) page.

## Data encryption

Google encrypts data at rest and encrypts data in transit, by default. The type of encryption used depends on the OSI layer, the type of service, and the physical infrastructure component. By default, we encrypt and authenticate all data in transit at one or more network layers when data moves outside physical boundaries not controlled by or on behalf of Google. To learn more, refer to the [Encryption in Transit in Google Cloud](#) [whitepaper](#).

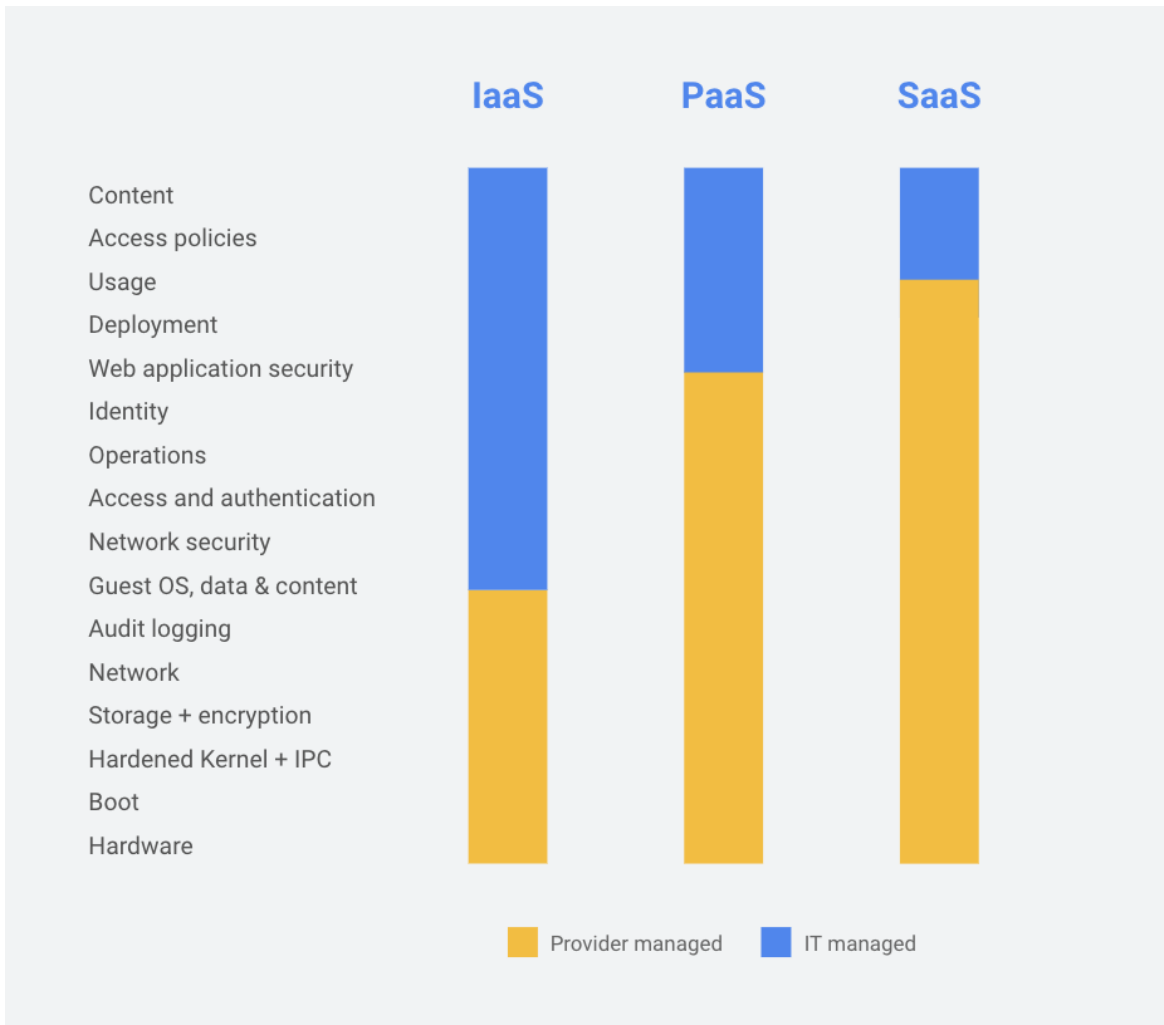
## Cloud-native technology

We continue to invest heavily in security, both in the design of new features and the development of cutting-edge tools for customers to more securely manage their environments. Some examples are the Cloud Security Command Center for Google Cloud and the Security Center for Google Workspace that bring actionable insights to security teams by providing security analytics and best practice recommendations from Google, and VPC Service Controls, which help to establish virtual security perimeters for sensitive data. To learn more about our security technologies, refer to our [security products & capabilities](#) page.

## The Shared Responsibility Model

Under our Shared Responsibility Model, the cloud customer and its CSP share the responsibilities of managing the IT environment, including those related to security and compliance. As a trusted partner, Google Cloud's role in this model includes providing services on a highly secure and controlled platform and offering a wide array of security features from which customers can benefit. Shared responsibility enables our customers to allocate resources more effectively to their core competencies and concentrate on what they do best. The shared responsibility model does not remove the accountability and risk from customers using Google Cloud services, but it does help relieve the burden as we manage and control system components and physical control of facilities. It also shifts a portion of the cost of security and compliance onto Google Cloud and away from our customers. The figure below visually demonstrates an example of the shared responsibility model across on-prem, infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings. Keep in mind that responsibilities will vary depending on the specific services being used.

For more information on Google Cloud product and security configurations, customers should reference the applicable product documentation.



# How Google Cloud helps customers meet the requirements of the Malaysia Personal Data Protection Act (PDPA)

Data Protection Obligations	How Google Supports PDPA Requirements
<b>Collection, Use, and Disclosure of Personal Data</b>	
<p><b>Notice of Collection</b></p> <ul style="list-style-type: none"> <li>Under the Notice and Choice Principle, data users must inform data subjects via a written notice of the following information: that personal data is being processed, a description of the processing, the purposes for collection and processing, the source of the personal data (as available), the availability of data subject rights, third party disclosures, options to limit processing, and the potential impact of failing to supply a data user with personal data.</li> <li>Notice must be provided at or before the time of collection.</li> <li>Notice must be provided both in English and the national language.</li> </ul>	<p>Customer Responsibility:</p> <ul style="list-style-type: none"> <li>Ensure the personal data is collected in a lawful manner. Customers must also make disclosures about how they collect and process personal data.</li> </ul> <p>Google Cloud Commentary:</p> <ul style="list-style-type: none"> <li>Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms.</li> </ul>
<p><b>Purpose Limitation</b></p> <ul style="list-style-type: none"> <li>Under the General Principle, personal data shall not be processed unless— (a) the personal data is processed for a lawful purpose directly related to an activity of the data user; (b) the processing of the personal data is necessary for or directly related to that purpose; and (c) the personal data is adequate but not excessive in relation to that purpose.</li> </ul>	<p>Customer Responsibility:</p> <ul style="list-style-type: none"> <li>To ensure the processing of personal data is limited to lawful purposes notified to data users.</li> </ul> <p>Google Cloud Commentary:</p> <ul style="list-style-type: none"> <li>You decide what information to put into the services and which services to use, how to use them, and for what purpose.</li> <li>Google commits to only access or use customer data to provide the services ordered by you and in accordance with the contract terms. Google will not use it for any other products or to serve ads. Refer to the Data Usage section of the <a href="#">Google Security whitepaper</a>.</li> </ul>
<p><b>Personal Data Use</b></p>	<p>Customer Responsibility:</p>

<ul style="list-style-type: none"> <li>• Under the General Principle, data users may not process data without consent, unless it is necessary for particular purposes, such as the fulfillment of a contract, compliance with legal obligations, or other listed purposes.</li> <li>• Data subjects have a right under the PDPA to withdraw their consent to the processing of personal data by a data user.</li> <li>• <a href="#">The Personal Data Protection Regulations 2013</a> provide that the data user must keep a record of consents from data subjects. The burden of proof is on the data user to establish that consent was obtained.</li> <li>• Processing “sensitive personal data” requires explicit consent unless an exemption applies.</li> </ul>	<ul style="list-style-type: none"> <li>• To ensure the processing of personal data is limited to lawful purposes.</li> </ul> <p>Google Cloud Commentary:</p> <ul style="list-style-type: none"> <li>• You decide which services to use, how to use them, and for what purpose.</li> <li>• Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms. Google will not use it for any other products or to serve ads. Refer to the Data Usage section of the <a href="#">Google Security whitepaper</a>.</li> </ul>
<p><b>Personal Data Disclosure</b></p> <ul style="list-style-type: none"> <li>• Under the Disclosure Principle, no personal data shall be disclosed without consent of the data subject for purposes other than the purpose at initial collection or related purposes.</li> <li>• Data users are also restricted from disclosing personal data to third parties that fall outside of the categories of third parties disclosed in a privacy notice.</li> </ul>	<p>Customer Responsibility:</p> <ul style="list-style-type: none"> <li>• To ensure collection, use, or disclosure of personal data is limited to the initial or related purposes for which the data was collected or with the data subject’s consent.</li> </ul> <p>Google Cloud Commentary:</p> <ul style="list-style-type: none"> <li>• Google commits to only access, use or disclose your data to provide the services ordered by you and in accordance with the contract terms.</li> <li>• At times, Google may engage third party vendors to perform limited activities in connection with the services. Information about these vendors (including their locations) and the limited processing of customer data they are authorized to perform is available on our <a href="#">Google Cloud Subprocessor page</a> and the <a href="#">Google Workspace and Cloud Identity Subprocessor</a> page.</li> </ul>
<p><b>Cross-Border Data Disclosure</b></p> <ul style="list-style-type: none"> <li>• The PDPA specifies that data users may not transfer personal data outside Malaysia unless the transfer is to a jurisdiction that the Minister has specified as either having in force laws</li> </ul>	<p>Customer Responsibility:</p> <ul style="list-style-type: none"> <li>• Customers should confirm that an exception to the PDPA’s restriction on data transfers applies.</li> </ul> <p>Google Cloud Commentary:</p>

<p>substantially similar to the PDPA or ensures an adequate level of protection, or if an exception applies.</p> <ul style="list-style-type: none"> <li>• Exceptions that may permit transfers include if the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not be processed in contravention of the PDPA, if consent is obtained from the data user, if the transfer is necessary for the performance of a contract between the data user and data subject, the transfer is necessary for the performance of a contract between the data user and a third party which is for the benefit of the data subject.</li> </ul>	<ul style="list-style-type: none"> <li>• Google applies the same robust security measures to customer data wherever it is located. Our data processing agreements for <a href="#">Google Workspace</a> and <a href="#">Google Cloud</a> services clearly articulate our privacy and security commitment to customers.</li> <li>• Google Workspace and Google Cloud services undergo several independent third-party audits on a regular basis to verify security, privacy, and compliance controls. See Cloud's <a href="#">compliance reports</a>.</li> </ul>
<p><b>Accountability</b></p>	
<p><b>Requests for access to personal data</b></p> <ul style="list-style-type: none"> <li>• Under the Access Principle, data users must give data subjects access to the personal data held by a data user, with some exceptions.</li> </ul>	<p>Customer Responsibility:</p> <ul style="list-style-type: none"> <li>• To develop procedures and capabilities to allow individuals to access their personal data.</li> </ul> <p>Google Cloud Commentary:</p> <ul style="list-style-type: none"> <li>• Customers may access their data on Google Cloud services at any time.</li> <li>• If Google receives a request from an individual relating to their personal data, our privacy team will advise the requester to submit the request to you, the Google Cloud customer. Google Cloud customers can then take control for responding to these requests as per their internal procedures and requirements.</li> <li>• Google Cloud's administrative consoles and services possess the functionality to access any data that you or your users put into our systems</li> </ul>
<p><b>Requests for correction of personal data</b></p> <ul style="list-style-type: none"> <li>• Under the Access Principle, data users must give data subjects the opportunity to correct personal data where inaccurate, incomplete, misleading or not up-to-date, with some exceptions. The law sets forth particular steps a data user must take when fulfilling such a request.</li> <li>• Data users must take all practicable steps</li> </ul>	<p>Customer Responsibility:</p> <ul style="list-style-type: none"> <li>• To develop procedures and capabilities to correct data subjects' personal data.</li> </ul> <p>Google Cloud Commentary:</p> <ul style="list-style-type: none"> <li>• Customers may access their data on Google Cloud services at any time.</li> <li>• If Google receives a request from an individual relating to the correction of</li> </ul>

<p>to supply a third party to which it previously transferred personal data with a copy of the personal data as corrected, accompanied by a notice in writing stating the reasons for the correction.</p>	<p>their personal data, our privacy team will advise the requester to submit the request to you, the Google Cloud customer. Google Cloud customers can then take control for responding to these requests as per their internal procedures and requirements.</p> <ul style="list-style-type: none"> <li>Google Cloud’s administrative consoles and services possess the functionality to rectify any data that you or your users put into our systems.</li> </ul>
<p><b>Registration</b></p> <ul style="list-style-type: none"> <li>Data users that fall under any one or more of the classes specified in the Personal Data Protection (Class of Data Users) Order 2013 (“Order”) are required to <a href="#">register</a> with the PDPA Commissioner.</li> </ul>	<p><b>Customer Responsibility:</b></p> <ul style="list-style-type: none"> <li>Customers are responsible for their registration obligations.</li> </ul> <p><b>Google Cloud Commentary:</b></p> <ul style="list-style-type: none"> <li>Google Cloud recognizes that you need certain information in order to conduct due diligence and comply with relevant registration requirements. You can review Google’s current <a href="#">certifications and audit reports</a> at any time. <a href="#">Compliance reports manager</a> provides you with easy, on-demand access to these critical compliance resources.</li> </ul>
<p><b>Records of Processing</b></p> <ul style="list-style-type: none"> <li>The PDP obligates data users to keep and maintain a record of any application, notice, request, or any other information relating to personal data processed in a form and manner that may be determined by the Commissioner.</li> <li>A personal data system maintained by a data user must also be made available for inspection by the Commissioner.</li> </ul>	<p><b>Customer Responsibility:</b></p> <ul style="list-style-type: none"> <li>Customers are responsible for records of processing.</li> </ul> <p><b>Google Cloud Commentary:</b></p> <ul style="list-style-type: none"> <li>The contact terms and related documentation describe Google Cloud products’ functionality and data protection measures. In addition, Google’s Cloud Data Protection Team will provide reasonable assistance with your queries related to Google’s processing of your personal data.</li> </ul>
<p><b>Care of Personal Data</b></p>	
<p><b>Accuracy</b></p> <ul style="list-style-type: none"> <li>The Data Integrity Principle places an obligation on data users to take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date.</li> </ul>	<p><b>Customer Responsibility:</b></p> <ul style="list-style-type: none"> <li>Customers must take reasonable steps to ensure the personal data they collect is accurate, complete, not misleading, and up to date.</li> <li>A customer must also take reasonable</li> </ul>

	<p>steps to ensure the personal data it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.</p> <p>Google Cloud Commentary:</p> <ul style="list-style-type: none"> <li>• Google Cloud is not involved in maintaining the accuracy of personal data collected by customers.</li> <li>• Google Cloud does, however, work to ensure the integrity of data placed in our services.</li> <li>• Customers may also use the administrative consoles to maintain the accuracy of their data.</li> </ul>
<p><b>Data Breach Notification</b></p> <ul style="list-style-type: none"> <li>• The PDPA does not require notification in the event of a breach. However, the government issued PCP No.1/2018 to collect public feedback on various personal data issues, including the reporting of data breach and implementation of data breach notification.</li> <li>• Data users that wish to report a breach to the Malaysian government may do so <a href="#">here</a>.</li> </ul>	<p>Customer Responsibility:</p> <ul style="list-style-type: none"> <li>• Customers should develop policies and procedures for effectively addressing and responding to data breaches.</li> </ul> <p>Google Cloud Commentary:</p> <ul style="list-style-type: none"> <li>• Google recognizes that to effectively manage your use of the services, including handling potential data breaches, you need sufficient information about the services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the services on an ongoing basis.</li> <li>• Google will make information about developments that materially impact Google’s ability to perform the services in accordance with the SLAs available to you. More information is available at our <a href="#">Incidents &amp; the Google Cloud dashboard</a> for Google Cloud and the <a href="#">Status Dashboard</a> for Google Workspace.</li> <li>• Google will notify you of data incidents promptly. More information on Google’s data incident response process is available in our <a href="#">Data incident response whitepaper</a>.</li> <li>• To fulfill this obligation, Google’s incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. Refer to our <a href="#">Data</a></li> </ul>

	<p><a href="#">incident response whitepaper</a> for more information.</p>
<p><b>Retention</b></p> <ul style="list-style-type: none"> <li>• Data users must not retain personal data processed for a particular purpose longer than necessary for the fulfillment of that purpose, per the Retention Principle.</li> <li>• Data users are obligated to take all reasonable steps to ensure personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was processed.</li> <li>• The <a href="#">2015 Standards</a> address retention expectations.</li> </ul>	<p>Customer Responsibility:</p> <ul style="list-style-type: none"> <li>• Customers should delete the personal data it holds once its purpose has expired.</li> </ul> <p>Google Cloud Commentary:</p> <ul style="list-style-type: none"> <li>• Google will delete customer data in accordance with the contract.</li> <li>• Google Cloud 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. To learn more about data deletion at Google, refer to our <a href="#">Data deletion on Google Cloud whitepaper</a>.</li> <li>• 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.</li> </ul>
<p><b>Storage and Security</b></p> <ul style="list-style-type: none"> <li>• Under the Security Principle, data users must take practical steps to protect personal data from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.</li> <li>• Data users must also take steps to protect data that is processed by a data processor by ensuring that the data processor provides sufficient guarantees regarding technical and organisational security measures governing the processing to be carried out and takes reasonable steps to ensure compliance with those measures.</li> <li>• The <a href="#">2015 Standards</a> address security expectations.</li> </ul>	<p>Customer Responsibility:</p> <ul style="list-style-type: none"> <li>• Customers should implement sufficient security controls to protect personal data including proper configuration of features in the cloud under customer management.</li> </ul> <p>Google Commentary:</p> <p>(1) <a href="#">Security of Google's infrastructure</a></p> <p>Google manages the security of our infrastructure (ie., the hardware, software, networking and facilities that support the services).</p> <p>Google provides detailed information to customers about our security practices at:</p> <ul style="list-style-type: none"> <li>• Our <a href="#">infrastructure security</a> page</li> <li>• Our <a href="#">security whitepaper</a></li> <li>• Our <a href="#">cloud-native security whitepaper</a></li> </ul>



- Our [infrastructure security design overview](#) page
- Our [security resources](#) page
- Our [Cloud compliance](#) page

(2) Security of your data and applications in the cloud

(a) Security by default

- Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud [Encryption at rest](#) page.
- Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud [Encryption in transit](#) page.

(b) Security products

Information on Google's security products is available on our [Cloud Security Products](#) page.

The below illustrative list of Google Cloud and Google Workspace services may be used to help with your storage and security requirements:

**Access control**

2-Step Verification

- 2-Step Verification puts an extra barrier between customer's business and cybercriminals who try to steal usernames and passwords to access business data. With 2-Step Verification, customer's users sign in to their account in two steps with something they know (their password) and something they have (their mobile phone with Google OTP installed)

Identity and Access Management (IAM)

- Identity and Access Management (IAM) can be used to assign roles and permissions to administrative groups, incorporating principles of least privilege and separation of duties.

#### [VPC Service Controls](#)

- VPC Service Controls allow customers to address threats such as data theft, accidental data loss, and excessive access to data stored in Google Cloud multi-tenant services. It enables clients to tightly control what entities can access what services in order to reduce both intentional and unintentional losses.
- VPC Service Controls delivers zero-trust style access to multi-tenant services. Clients can restrict access to authorized IPs, client context, and device parameters while connecting to multi-tenant services from the internet and other services. Examples include GKE, BigQuery, etc. It enables clients to keep their entire data processing pipeline private.

#### **Access Log**

##### [Cloud Logging](#)

- Cloud Logging is a fully managed service that allows you to store, search, analyze, monitor, and alert on logging data and events from Google Cloud and Amazon Web Services. You can collect logging data from over 150 common application components, on-premises systems, and hybrid cloud systems.

##### [Access Transparency](#)

- Access Transparency Maintain visibility of insider access to your data through near real-time logs from Access Transparency.

#### **Protection from External Threats**

##### [Cloud Security Command Center](#)

- Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security posture by evaluating your security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities, and threats; and helping you mitigate and remediate risks.

#### [Virtual Machine Threat Detection](#)

- Virtual Machine Threat Detection, a built-in service of Security Command Center Premium, provides threat detection through hypervisor-level instrumentation.

#### **Monitoring**

- The Google Cloud [Status Dashboard](#) provides status information on the services.
- The Google Workspace [Status Dashboard](#) provides status information on the services.
- [Google Cloud Operations](#) is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services.
- [Admin Console Reports](#) allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more.

#### (c) [Security resources](#)

Google also publishes guidance on:

- [Security best practices](#)
- [Security use cases](#)
- [Security blueprints](#)

## Conclusion

At Google, we recognize that your data is yours only and guaranteeing the privacy of your data is key. The protection of your data is a primary design consideration for all our infrastructure, products and personnel operations. We believe that Google can offer a level of protection that very few public cloud providers or private enterprise IT teams can match. Because protecting data is core to Google's business, we can make extensive investments in security, resources and expertise at a scale that others cannot. Our investment frees you to focus on your business and innovation. Data protection and privacy is more than just security. Google's strong contractual commitments make sure you maintain control over your data and how it is processed, including the assurance that your data is not used for advertising or any purpose other than to deliver Google Cloud services.

For these reasons and more, over five million organisations across the globe, including 64 percent of the Fortune 500, trust Google with their most valuable asset: their information. Google will continue to invest in our platform to allow you to benefit from our services in a secure and transparent manner.

The information within this whitepaper should be used to help customers determine whether Google Cloud and Google Workspace products or services are suitable for them in light of the PDPA.