Google Cloud Whitepaper
July 2022

Thailand Personal Data Protection Act

Table of Contents

Disclaimer

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

Introduction

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

This whitepaper provides information to our customers about the Thailand Personal Data Protection Act and how Google Cloud uses Google's industry-leading data privacy and security capabilities to help store, process, maintain, and secure customer data[2]. We are committed to partnering with our customers so they can deploy workloads using Google Cloud services and Google Workspace for their productivity needs in a manner that aligns with the Personal Data Protection Act requirements. We describe our data protection features and outline how they map to its requirements. However, please note that, as a provider of cloud services, we are not in a position to provide you with legal advice - that is something only your legal counsel can provide.

Overview of the Thailand Personal Data Protection Act

The Personal Data Protection Act, B.E. 2562 (2019) ("PDPA"), Thailand's comprehensive data protection law, regulates the collection, usage, provision, and other processing of personal data by private and certain governmental entities. The law was published in the Thai Government Gazette in May 2019 and became enforceable as of June 1, 2022. Violations may result in civil, criminal, and administrative penalties.

The PDPA applies to data controllers and data processors and defines those terms similarly to other global data protect frameworks: "data controllers" are persons or juristic persons who have the power and duties to make decisions regarding the collection, use, or disclosure of personal data and "data processors" are persons or juristic persons who operate in relation to the collection, use, or disclosure of personal data pursuant to the orders given by or on behalf of a data controller. An agreement to process data on behalf of a data controller must include an agreement between the data controller and data processor to process data in accordance with the PDPA.

Data controllers and data processors are required by law to process personal data in ways that generally align with other global data protection frameworks. For example, the law contains purpose limitation and transparency requirements. Additionally, organizations may only process personal data, including sensitive personal data, pursuant to a legal basis. Such legal bases include consent,

[1] In this whitepaper, "you/your" refers to Google Cloud and Google Workspace customers as well as Google Cloud partners. Unless indicated otherwise, references to "customers" will include Google Cloud partners and references to "customer data" will include Google Cloud partner data.
[2] In this whitepaper "customer data" and "your data" refers to the customer data we process according to your Google Cloud agreement(s).

performing tasks in the public interest, for the data controller's legitimate interest, and when processing is required for compliance with the law. The law also grants rights to data subjects, including the right to access, correct, and delete data; to restrict and object to processing; and to data portability.

The PDPA applies both in Thailand and extraterritorially. The PDPA applies to entities in Thailand that collect, use, or disclose personal data, regardless of whether the collection, use, or disclosure occurs in Thailand. Furthermore, the PDPA applies to both data controllers and data processors outside Thailand that collect, use, or disclose personal data of data subjects who are in Thailand when the processing activities are related to offering goods or services to data subjects in Thailand or when the processing activities are related to the monitoring of a data subject's behavior, where the behavior takes place in Thailand. Additionally, while the law applies generally to the processing of personal data, there are some exceptions to the scope, including not applying to processing for the purposes of mass media, fine arts, or literature in accordance with professional ethics or the public interest.

Data controllers may only transfer personal data outside of Thailand if the transfer is carried out in accordance with criteria established by the Committee and the destination country or international organization that receives the personal data has an adequate data protection standard, or if an exception applies. These exceptions include transfers for compliance with law, where data subject consent has been obtained and adequate notice has been given, and where the transfer is necessary to perform a contract where the data subject is a party, or which is for the data subject's benefit.

Data controllers and data processors who are located outside Thailand are required to appoint a local representative physically located in Thailand with unlimited liability for any breaches of the PDPA incurred by the foreign data controllers or data processors they represent. The only exception is in cases where collected data is not in large numbers and not sensitive personal data.

The Ministry of Digital Economy and Society, through the Office of the Personal Data Protection Commission (the "Commission"), is responsible for administering and enforcing the PDPA. The PDPA tasks the Office of the Personal Data Protection Committee, which is overseen by the Commission, with issuing subordinate regulations to the PDPA.

Google Cloud data protection overview & the Shared Responsibility Model

Google Cloud's robust security and privacy controls can give customers the confidence to utilize Google Cloud services and Google Workspace in a manner aligned with the requirements of the Thailand Personal Data Protection Act. 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 organizational and technical controls we use to protect your data. To learn more about our approach to security and compliance, refer to the Google security whitepaper for Google Cloud services and the Google Workspace Security whitepaper.

Topics

Google Cloud's approach to data protection and privacy

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

Data protection and privacy trust principles

We want our customers to feel confident when using Google Cloud 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 organizations, but participates in Google product launches by reviewing design documentation and performing code reviews to help ensure that privacy requirements are followed. They help release products that reflect strong privacy practices: transparent collection of user data, providing users and administrators with meaningful privacy configuration options, and continuing to be good stewards of information stored on

our platform. To learn more about our privacy team, refer to the privacy team section of the Google security whitepaper for Google Cloud services 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 which are available in near real-time via Access Transparency.

Google Cloud's approach to data security

In this section, we provide an overview of the organizational and technical controls that we use to protect your data at Google Cloud. Please refer to Google security whitepaper, 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 generally more secure and easier to manage than most other deployment options. Our infrastructure can provide secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the Internet, and safe operation by administrators. We maintain the security of this infrastructure in progressive layers, starting from the physical security of our data centers, building with underlying security-designed hardware and software, continuing with secure service deployment, secure data storage, and secure internet communication, and finally, operating the infrastructure in a secure fashion.

To learn more, refer to the Google Cloud Infrastructure Security Design Overview, as well as the 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 data in transit at one or more network layers when data moves outside physical boundaries not controlled by or on behalf of Google. To learn more, refer to the Encryption in Transit in Google Cloud whitepaper.

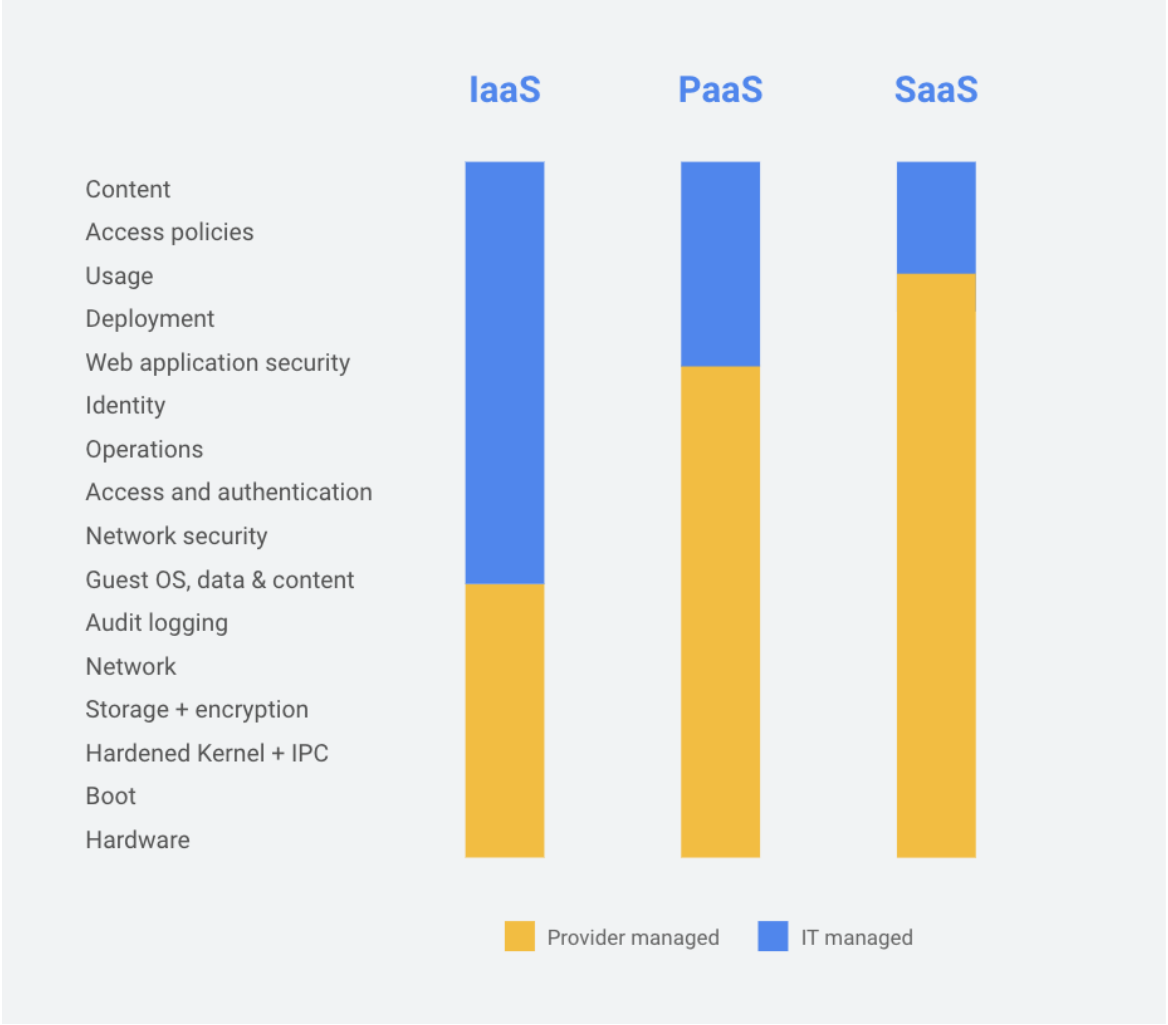
Cloud-native technology

We continue to invest heavily in security, both in the design of new features and the development of cutting-edge tools so customers can more securely manage their environments. 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 personal data. To learn more about our security technologies, refer to our security products & capabilities page.

The Shared Responsibility Model

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

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


IaaS
PaaS
SaaS
Content
Access policies
Usage
Deployment
Web application security
Identity
Operations
Access and authentication
Network security
Guest OS, data & content
Audit logging
Network
Storage + encryption
Hardened Kernel + IPC
Boot
Hardware
Provider managed
IT managed

How Google Cloud helps customers meet the requirements of the Thailand Personal Data Protection Act

Data Protection Obligations	How Google Supports PDPA Requirements
Collection, use, and disclosure of personal information	
Notice of Collection ● Data controllers are responsible for informing data subjects, prior to or at the time of such collection, of certain details regarding how the data controller collects and processes personal data, as well as the data subjects' rights. This information must include the following: ○ purpose of the processing personal data; ○ the legal basis for processing; ○ whether an individual must provide personal data and the possible consequences of failure to do so; ○ the retention period for stored personal data; ○ the categories of third parties to which personal data may be disclosed; ○ the identity and contact details of the data controller or the data controller's representative or data protection officer where applicable; and ○ the rights of the data subject.	Customer Responsibility: ● Ensure the personal information is collected in a lawful manner. ● Customers must also make disclosures about how they collect and process personal information. Google Cloud Commentary: ● Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms.
Purpose Limitation ● The PDPA requires that data controllers collect, use, or disclose personal data according to the purpose about which data subjects were notified prior to or at the point of collection.	Customer Responsibility: ● To ensure collection, use, or disclosure of personal information is limited to the lawful purposes specified. Google Cloud Commentary: ● Google gives you control to decide what information to put into the services and which services to use, how to use them, and for what purpose.

	• Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms. Google will not use your data for any other products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.
Source • Under the PDPA, the data controller may not collect personal data from any other source, apart from the data subject directly, except where: (1) the data controller has informed the data subject of the collection of personal data from another source without delay, but not more than 30 days after the date of collection, and obtained consent from the data subject; or (2) there is a legal basis to collect the personal data.	Customer Responsibility: • Customers should make all efforts to collect information directly from the individual, unless certain circumstances apply. Google Cloud Commentary: • Google gives you control to decide which Services to use, how to use them, and what information to collect.
Manner of Collection • Data controllers may only collect personal data if the data subject consents or pursuant to a legal basis under the PDPA.	Customer Responsibility: • To ensure the collection of personal information is conducted through lawful, fair, and not unreasonably intrusive means. • Such information collection should at all times be fair, lawful, and be directly related to the provisioning of services. Google Cloud Commentary: • Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms.
Anonymization • Data subjects have a right to request that the data controller erase or destroy the personal data, or anonymize it such that the data subject cannot be re-identified.	Customer Responsibility: • Prior to collecting personal information, Customers should consider whether their processing purposes can be fulfilled without individuals identifying themselves, or using a pseudonym. • If personal information is collected, customers should consider implementing anonymisation or pseudonymisation processes before further processing. Google Cloud Commentary: • Google Cloud offers Data Loss Prevention, a service designed to help

	with discovery, classification, and anonymization of sensitive personal data via an API that can be used by most applications / services.
Personal Information/Data Use ● The PDPA requires that data controllers collect, use, or disclose personal data according to the purpose about which data subjects were notified prior to or at the point of collection. ● Data controllers may not collect, use, or disclose personal data in a different manner unless the data subject consents or the collection, use, or disclosure is otherwise in accordance with the PDPA or other laws.	Customer Responsibility: ● To ensure collection, use, or disclosure of personal information is lawful. Google Cloud Commentary: ● Google gives you control to decide what information/data to put into the services and which services to use, how to use them, and for what purpose. ● Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms. Google will not use it for any other products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.
Personal Information/Data Disclosure ● When disclosing personal data, it is the responsibility of the data controller to take action to prevent recipients from using or disclosing personal data unlawfully or without authorization.	Customer Responsibility: ● To develop a disclosure handling process. Google Cloud Commentary: ● Google Cloud makes robust confidentiality, data protection, and security commitments in our contracts. ● Google commits to processing your data to provide the services ordered by you and in accordance with the contract terms. Google will not use it for any other products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.
Cross-Border Data Disclosure ● In the event a data controller sends or transfers the personal data to a foreign country, the transfer must be carried out in accordance with rules prescribed by the Committee. ● The transfer must also be to a jurisdiction or international organization that has an adequate data protection standard or where an exception applies. ○ These exceptions include transfers for purposes of complying with laws, where the	Customer Responsibility: ● Customers should ensure proper consent and justification (in the event consent is not required) for cross-border transfers are in place. Google Cloud Commentary: ● Google applies the same robust security measures to customer data wherever it is located. Our data processing agreements for Google Workspace and Google Cloud services clearly articulate our privacy and security commitment to customers.

consent of the data subject has been obtained, where the transfer is for compliance with a contract, and others. ● The PDPA also allows international transfers of personal data where the transfer is between affiliates with binding corporate rules that are approved by the Committee or with additional mechanisms in place pending Committee approval.	● Google Workspace and Google Cloud services undergo several independent third-party audits on a regular basis to verify security, privacy, and compliance controls. See Google Cloud's compliance reports.
Accountability	
Privacy impact assessments ● The PDPA does not require privacy impact assessments. However, data controllers have a duty to establish appropriate security measures and review them as necessary or when the technology has changed in order to effectively maintain appropriate security and safety standards.	Customer Responsibility: ● Establish and periodically review security measures, Google Cloud Commentary: ● Google Cloud recognizes that you need certain information in order to conduct a privacy impact assessment. Our data processing agreements for Google Workspace and Google Cloud services clearly articulate our privacy and security commitment to customers. ● In addition, you can review Google's current certifications and audit reports via Google Cloud's compliance reports.
Requests to access or correct personal information ● The PDPA grants data subjects the right to request access to and obtain a copy of their personal data which is under the responsibility of the data controller. ○ Data controllers have 30 days to fulfill such a request, unless an exception applies. ○ Note that the Committee may prescribe rules for the access to and request to obtain a copy of personal data. ● Data controllers must also ensure that the personal data remains accurate, up-to-date, complete, and not misleading. ○ Data subjects may request that data controllers maintain personal data in accordance with this requirement.	Customer Responsibility: ● To develop procedures and capabilities to allow individuals to access and correct their personal information. Google Cloud Commentary: ● Customers may access their data on Google Cloud services at any time. ● If Google receives a request from an individual relating to their personal information, our privacy team will advise the requester to submit the request to you, the Google Cloud customer. Google Cloud customers can then take control for responding to these requests as per their internal procedures and requirements. ● Google Cloud's administrative consoles and services possess the functionality to access any data that you or your users put into our systems.

Requests to restrict processing of personal information; Requests to delete personal information ● Data subjects has the right to object to the collection, use, or disclosure of their personal data under certain circumstances. ○ In the event that the data subject exercises their right to object a data controller may no longer collect, use, or disclose such personal data and must distinguish the data immediately when the data subject gives notice of an objection. ● Furthermore, data subjects have the right to request that the data controller restrict the use of personal data under certain circumstances. ○ The Committee may prescribe and announce rules regarding the suspension of use of personal data. ● Data subjects also have a right to request that the data controller erase or destroy their personal data, or anonymize it such that it cannot identify the data subject, under certain circumstances. ○ Where the data controller has disclosed personal data and the data subject requests deletion or anonymization, the data controller is responsible for fulfilling the request (if appropriate), including associated technology implementation and associated costs, and informing other data controllers in order to obtain their responses to fulfill the deletion request.	Customer Responsibility: ● If you wish to stop using our services, you can do so at any time. ● Where required, delete personal information in response to requests from data subjects. Google Cloud Commentary: ● Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data. You can use the following functionality of Google Cloud services: ○ Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources. ○ Admin Console: A web-based graphical user interface that customers can use to manage their Google Workspace resources. ○ gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. ○ Google APIs: Application programming interfaces which provide access to Google Cloud.
Requests for portability of personal information ● Data subjects have the right under the PDPA to receive their personal data from the data controller. The data controller is obligated to arrange personal data in a format which is readable or commonly used by means of automatic tools or	Customer Responsibility: ● Enable data subjects to obtain a copy of their personal information in a commonly used format. Google Cloud Commentary: ● Google enables customers to access and

equipment, and can be used or disclosed by automated means, unless an exception applies.	export their data throughout the duration of their contract and during the post-termination transition term. ● You can export your data from a number of Google Cloud services in a number of industry standard formats: For example: ○ Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. ○ Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. ○ You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here. ○ In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our services.
Registration ● The PDPA does not contain a general registration requirement. However, any data controller, data processor or local representative that either (a) collects, processes or discloses a large volume of personal data; or (b) whose core activity is the collection, processing or disclosure of sensitive personal data, must appoint a Data Protection Officer (DPO) and notify the Commission of the DPO's contact information.	Customer Responsibility: ● Customers are responsible for their registration obligations. Google Cloud Commentary: ● 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 certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.
Records of Processing ● Data controllers must maintain records of processing, which may be accessed by data subjects or the Committee. Note that this requirement does not apply to small organizations. ● Such records must include: the personal	Google Cloud Commentary: ● Google maintains electronic records related to its processing of customer data. ● The rights, responsibilities, roles, obligations, and duties of Google and customers are set out in the Google Cloud

data collected; the purpose of the collection for each category of personal data; details of the data controller; the retention period; data subject rights and methods for access to personal data; the use or disclosure of personal data collected under a legal basis besides consent; records of rejections of data subject requests; and an explanation of the security measures in place to protect personal data. ● The request for consent must be through written statement or electronic means.	contract.
Privacy & Security Program ● The PDPA requires that data controllers provide appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of personal data ● Data controllers must review the security measures they put in place as necessary or when technology has changed.	Customer Responsibility: ● Customers should implement sufficient security controls to protect the personal information including proper configuration of features in the cloud under customer management. Google Commentary: (1) Security of Google's infrastructure Google manages the security of our infrastructure (ie., the hardware, software, networking and facilities that support the services). Google provides detailed information to customers about our security practices at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page ● Our Cloud compliance page (2) Security of your data and applications in the cloud (a) Security by default ● Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from

	you. More information is available on the Google Cloud Encryption at rest page. ● Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products Information on Google's security products is available on our Cloud Security Products page. The below illustrative list of Google Cloud and Google Workspace services may be used to help with your storage and security requirements: **Access control** 2-Step Verification ● 2-Step Verification puts an extra barrier between customer's business and cybercriminals who try to steal usernames and passwords to access business data. With 2-Step Verification, customer's users sign in to their account in two steps with something they know (their password) and something they have (their mobile phone with Google OTP installed) Identity and Access Management (IAM) ● Identity and Access Management (IAM) can be used to assign roles and permissions to administrative groups, incorporating principles of least privilege and separation of duties. VPC Service Controls ● VPC Service Controls allow customers to address threats such as data theft, accidental data loss, and excessive access to data stored in Google Cloud multi-tenant services. It enables clients to

	tightly control what entities can access what services in order to reduce both intentional and unintentional losses. ● VPC Service Controls delivers zero-trust style access to multi-tenant services. Clients can restrict access to authorized IPs, client context, and device parameters while connecting to multi-tenant services from the internet and other services. Examples include GKE, BigQuery, etc. It enables clients to keep their entire data processing pipeline private. **Access Log** Cloud Logging ● Cloud Logging is a fully managed service that allows you to store, search, analyze, monitor, and alert on logging data and events from Google Cloud and Amazon Web Services. You can collect logging data from over 150 common application components, on-premises systems, and hybrid cloud systems. Access Transparency ● Access Transparency Maintain visibility of insider access to your data through near real-time logs from Access Transparency. **Protection from External Threats** Cloud Security Command Center ● Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security posture by evaluating your security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities, and threats; and helping you mitigate and remediate risks. Virtual Machine Threat Detection

	• Virtual Machine Threat Detection, a built-in service of Security Command Center Premium, provides threat detection through hypervisor-level instrumentation. **Monitoring** • The Google Cloud Status Dashboard provides status information on the services. • The Google Workspace Status Dashboard provides status information on the services. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. • Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints
Accountability	
Assistance with Investigations • The Committee is authorized to carry out investigations for allegations of noncompliance with the PDPA. Failure of any person to cooperate in an investigation may result in an administrative fine of up to THB 500,000 (approx. USD 13,900).	Google Cloud Commentary • Google is committed to supporting regulated entities with audits of our services. As this support is not included in our usual publicly listed service fees, Google may charge an additional fee in connection with an audit. • Google will provide further details of any fee in advance of the activity when the scope of the activity is known.
Care of Personal Information	
Accuracy	Customer Responsibility:

• Data controllers must also ensure that the personal data remains accurate, up-to-date, complete, and not misleading.	• Customers must take reasonable steps to ensure the personal information it collects, uses or discloses is accurate, up to date, and complete, having regard to the purpose of the use or disclosure. Google Cloud Commentary: • Google Cloud is not involved in maintaining the accuracy of personal information collected by customers. • Google Cloud does, however, help ensure the integrity of data placed in our services. • Customers may also use the administrative consoles to maintain the accuracy of their data.
Data Breach Notification • Data controllers must notify the Committee of any personal data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such personal data breach is unlikely to result in a risk to the rights and freedoms of individuals. • If the breach is likely to result in a high risk to the rights and freedoms of individuals, the PDPA requires that the data controller also notify the data subject regarding the breach and remedial steps taken without delay. • The notification and the exemption to the notification must be made in accordance with rules and procedures set forth by the Committee.	Customer Responsibility: • Customers should develop policies and procedures for effectively addressing and responding to data breaches. Google Cloud Commentary: • Google recognizes that to effectively manage your use of the services, including handling potential data breaches, you need sufficient information about the services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the services on an ongoing basis. • Google will make information about developments that materially impact Google's ability to perform the services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard for Google Cloud and the Status Dashboard for Google Workspace. • Google will also notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper. • Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. Refer to

	our Data incident response whitepaper for more information.
Retention ● The PDPA obligates data controllers to put in place a system to monitor erasure or destruction of personal data when the retention period ends; or when the personal data is no longer relevant or beyond the purpose necessary for which it has been collected; or when the data subject has request to do so; or when the data subject withdraws consent, except where the retention is necessary for certain purposes.	Customer Responsibility: ● Customers should delete the personal information it holds once its purpose has expired. Google Cloud Commentary: ● Google will retain, return, destroy, or delete customer data in accordance with the contract. ● Google Cloud and Google Workspace administrative consoles and services provide functionality to delete customer data put into our systems. If customers delete their data, we commit to deleting it from our systems within 180 days. To learn more about data deletion at Google, refer to our Data deletion on Google Cloud whitepaper. ● We also provide tools that make it easy for customers to take their data with them if they choose to stop using our services, without additional cost.
Storage and Security ● The PDPA requires that data controllers provide appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of personal data ● Data controllers must review the security measures they put in place as necessary or when technology has changed.	Customer Responsibility: ● Customers should implement sufficient security controls to protect the personal information including proper configuration of features in the cloud under customer management. Google Commentary: (1) Security of Google's infrastructure Google manages the security of our infrastructure (ie., the hardware, software, networking, and facilities that support the services). Google provides detailed information to customers about our security practices at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper

	• Our infrastructure security design overview page • Our security resources page • Our Cloud compliance page (2) Security of your data and applications in the cloud (a) Security by default • Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. • Encryption in transit. Google encrypts and authenticates 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. VPC Service Controls enable clients to keep their entire data processing pipeline private. **Access Log** Cloud Logging • Cloud Logging is a fully managed service that allows you to store, search, analyze, monitor, and alert on logging data and events from Google Cloud and Amazon Web Services. You can collect logging data from over 150 common application components, on-premises systems, and hybrid cloud systems. Access Transparency • Access Transparency can maintain visibility of insider access to your data through near real-time logs from Access Transparency. **Protection from External Threats**

	Cloud Security Command Center • Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security posture by evaluating your security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities, and threats; and helping you mitigate and remediate risks. Virtual Machine Threat Detection • Virtual Machine Threat Detection, a built-in service of Security Command Center Premium, can provide threat detection through hypervisor-level instrumentation. **Monitoring** • The Google Cloud Status Dashboard provides status information on the services. • 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 can free you to focus on your business and innovation.

Data protection and privacy is more than just security. Google's strong contractual commitments help make sure you maintain control over your data and how it is processed, including the assurance that your data is not used for advertising or any purpose other than to deliver Google Cloud services.

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