Google Cloud Whitepaper
March 2023

Indonesia Personal Data Protection Law

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of March 2023 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

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 Indonesia Personal Data Protection Law 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 Indonesia Personal Data Protection Law 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 Indonesia Personal Data Protection Law

The Indonesia Personal Data Protection Law ("PDP Law"), enacted on October 17, 2022, regulates the collection, use, disclosure, and other processing of personal data by international organizations and governmental and private entities.

Similar to other data protection laws, the PDP Law places different obligations on "Personal Data Controllers" ("Controllers") and "Personal Data Processors" ("Processors"). A Controller is a person, public agency, or international organization that acts individually or jointly in determining the purposes of and exercising control over the processing of personal data. A Processor is a person, public agency, or international organization that acts individually or jointly in processing personal data on behalf of a Controller. The law imposes particular obligations on the processing of "Specific Personal Data" – which includes more sensitive categories of data such as health data, biometric information, and children's data – such as by requiring data protection impact assessments where a Controller processes Specific Personal Data.

The PDP Law sets forth responsibilities for organizations and privacy rights for individuals. It shares several concepts with other data protection laws, such as a requirement to process personal data only pursuant to a legal basis and an obligation to adopt policies and procedures to be accountable for compliance. Additionally, the PDP Law requires Controllers to process personal data according to an

[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).

enumerated set of processing principles, including that organizations must notify data subjects of the purposes for which they process personal data, must process personal data in a limited, specific, transparent, and lawful manner, and must protect the security of personal data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and loss.

The PDP Law applies to both organizations located within Indonesia and those located outside Indonesia, if the organization's data processing activities have legal consequences within Indonesia or affect Indonesian citizens outside of Indonesia. In this respect, the PDP Law has a broader scope of applicability than most other data protection laws, many of which only apply to activity within the country or directed to country residents.

Enforcement of the law begins in October 2024, two years after it was enacted. There are a variety of enforcement mechanisms under the PDP Law, including a private right of action for violations of the law, administrative fines, confiscation of profits or assets, and criminal penalties. The PDP Law provides for a Data Protection Authority to be established in order to administer the law and issue implementing regulations in the future.

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 PDP Law. 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 PDP Law. 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 Cloud Data Processing Addendum, 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 and Encryption at Rest pages.

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 data. To learn more about our security technologies, refer to our security products & capabilities page.

Additional Security Resources

(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 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 - Put an extra barrier between customer's business and cybercriminals who try to steal usernames and passwords to access business data.
- Identity and Access Management (IAM) - Assign roles and permissions to administrative groups, incorporating principles of least privilege and separation of duties.
- VPC Service Controls - Tightly control what entities can access what services in order to reduce both intentional and unintentional data losses.

Access Log

- Cloud Logging - Store, search, analyze, monitor, and alert on logging data and events from Google Cloud and Amazon Web Services.

- 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 - 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 - Detect threats through hypervisor-level instrumentation.

Monitoring

- Google Cloud Status Dashboard - Provide status information on the services.
- Google Workspace Status Dashboard - Provide status information on the services.
- Google Cloud Operations - Gain insight into your applications that run on Google Cloud, including availability and uptime of the services.
- Admin Console Reports - Examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more.

(3) Security resources

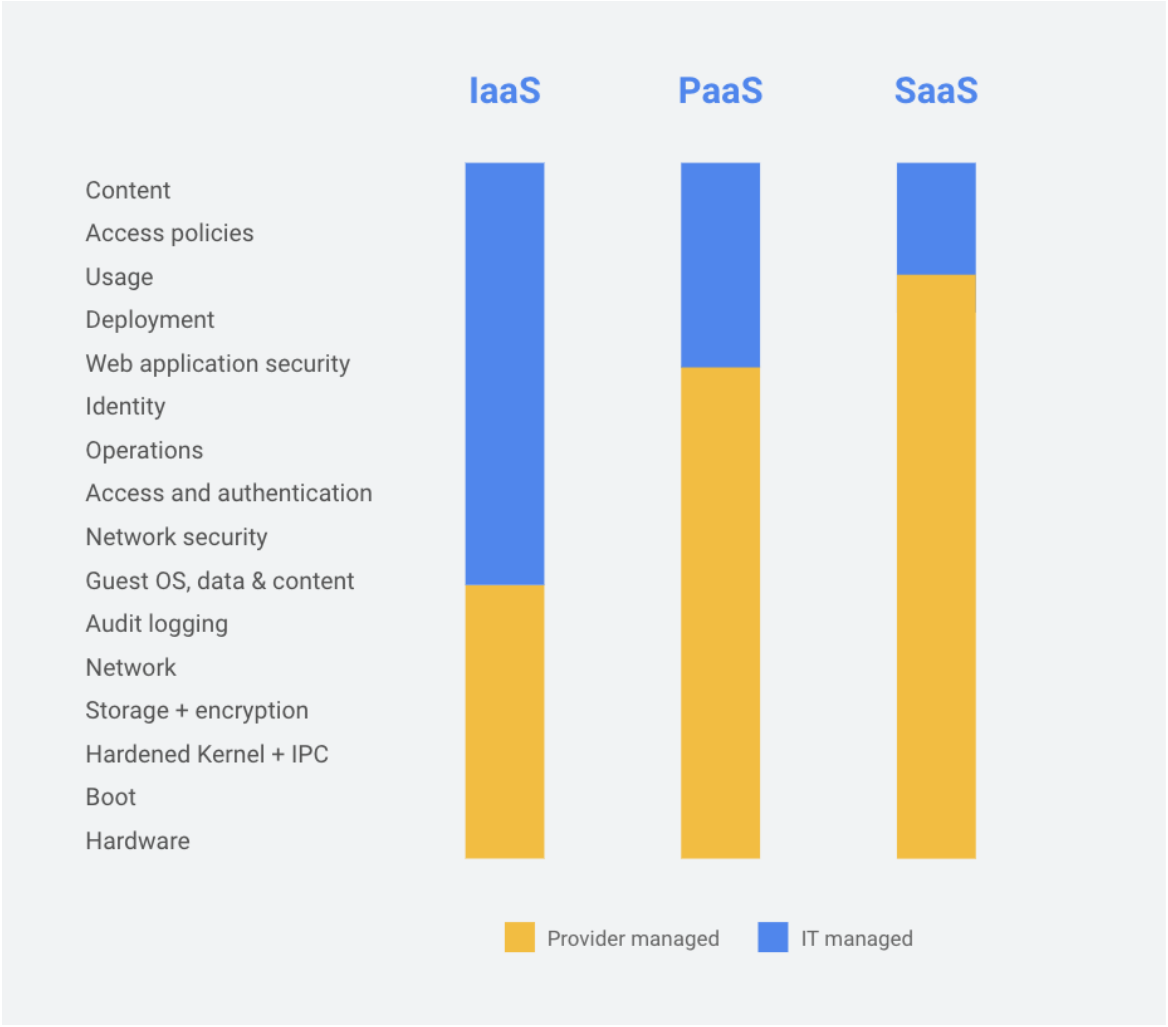
Google also publishes guidance on:

- Security best practices
- Security use cases
- Security blueprints

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 Personal Data Protection Law

Data Protection Obligations	How Google Supports PDP Law Requirements
Collection, Use, and Disclosure of Personal Data	
Notice of Collection • Organizations processing personal data shall notify data subjects of the purpose for processing and provide information regarding processing activities. • Under the PDP Law, a Controller must provide certain information to individuals when obtaining consent. This information includes confirmation that the personal data processing shall be carried out for lawful purposes; the purpose of the personal data processing; the type and relevance of the personal data to be processed; the retention period for documents containing personal data; details regarding the information collected; how long the processing of the personal data will be carried out; and rights of the personal data subject. • Controllers must also notify data subjects in the event the Controller undergoes a merger, spin-off, acquisition, consolidation, or dissolution.	Customer Responsibility: • Ensure the personal data is collected in a lawful manner. • Customers must also make disclosures about how they collect and process personal data. 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 • Controllers must process Personal Data in a limited and specific manner, lawfully and transparently.	Customer Responsibility: • To ensure collection, use, or disclosure of personal data is limited to the lawful purposes specified. Google Cloud Commentary: • You 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.
Personal Data Use ● Under the PDP Law, Controllers have an obligation to protect personal data from unauthorized processing. ● Organizations are prohibited from unlawfully obtaining or collecting personal data that do not belong to them with the intention to benefit themselves or other persons if that may result in loss to a data subject. Organizations are further prohibited from unlawfully disclosing personal data that does not belong to them.	Customer Responsibility: ● To ensure collection, use, or disclosure of personal data is lawful. Google Cloud Commentary: ● You 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 Data Disclosure ● Under the PDP Law, Controllers have an obligation to maintain the confidentiality of personal data, unless an exception applies. ● Organizations are prohibited from unlawfully disclosing personal data that does not belong to them. ● Under the law, if a Controller engages a Processor to process personal data, then the Processor must carry out personal data processing in accordance with the instructions of the Controller. ○ The law further states that Processors may involve another Processor to process personal data if the Controller has given prior written approval. ● Controllers have a duty under the law to supervise parties involved with processing personal data under the control of the Controller.	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 ● When transferring personal data, the law requires that Controllers ensure that the Controller's country of domicile and/or the domicile country of the Processor that receives the transfer of personal data protects personal data in a way that is at least as protective as the PDP Law. ○ Alternatively, it is the Controller's responsibility to ensure adequate and binding data protection measures apply to the transferred personal data, or to obtain consent to the transfer from a data subject.	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. ● Google Workspace and Google Cloud services undergo several independent third-party audits on a regular basis to verify security, privacy, and compliance controls. See Cloud's compliance reports.
Accountability	
Privacy impact assessments ● If certain personal data processing has a potential to cause a high risk for data subjects, Controllers must conduct an assessment the impact on the processing on those data subjects. Circumstances presumptively considered high-risk include, but are not limited to, automatic decision making that has legal consequences or significant impact on a data subject or the processing of Specific Personal Data (like health data, biometric information, or children's data), processing of personal data on a large scale, processing of personal data for the purpose of systematically evaluating or monitoring a data subject, and processing of personal data for the purpose of matching or combining groups of data .	Customer Responsibility: ● Customers should conduct a privacy impact assessment, if required. 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 See Cloud's compliance reports.
Requests to access or correct personal data ● The law requires Controllers to provide data subjects with access to personal data that is processed about them, as well as how it was processed and the relevant retention periods that attach to the personal data.	Customer Responsibility: ● To develop procedures and capabilities to allow individuals to access and correct their personal data. Google Cloud Commentary: ● Customers may access their data on

○ Access must be provided no later than 72 hours from the time that the controller receives a data subject request, unless an exception applies. ● Additionally, the PDP Law requires Controllers to update or correct errors or inaccuracies in personal data. This right is subject to certain exceptions. ○ Correction must be addressed no later than 72 hours from the time that the Controller receives a data subject request. ○ The law requires Controllers to notify the personal data subject of the results of the correction request.	Google Cloud services at any time. ● 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. ● 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 data; Requests to delete personal data ● If a Controller relies on consent to process personal data, the Controller must cease the processing if a data subject withdraws consent, unless an exception applies. ○ Such processing must cease no later than 72 hours from the time that the Controller receives a data subject request. ● Subject to some exceptions, Controllers must also delete or destroy personal data upon a request from the data subject. ○ A Controller must notify data subjects when it has deleted or destroyed the personal data. ● Subject to some exceptions, data subjects have the right under the PDP Law to delay or limit personal data processing proportionally with the purpose of personal data processing. ○ Such processing must cease no later than 72 hours from the time that the controller receives a data subject request and must notify the data subject that delay and restriction on processing have been implemented. ● Individuals also have a right under the	Customer Responsibility: ● If you wish to stop using our services, you can do so at any time. ● Where required, delete personal data in response to requests from data subjects or as otherwise required by law. 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

PDP Law to object to object to processing that is based solely on automated decision-making, including profiling, subject to some exceptions. ● Organizations processing Personal Data must destroy and/or delete it after a retention period expires or at the request of a data subject, unless otherwise stipulated by laws and regulations.	programming interfaces which provide access to Google Cloud.
Requests for portability of personal data ● The PDP Law grants data subjects a right to data portability. Some limited exceptions apply to this right. ○ Individuals have the right obtain information from data Controllers in a form that is in a commonly used structure or format or is readable by an electronic system.	Customer Responsibility: ● Enable data subjects to obtain a copy of their personal data in a commonly used format. Google Cloud Commentary: ● Google enables customers to access and 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.
Records of Processing ● The PDP Law requires that Controllers record all personal data processing activities, unless an exception applies.	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 contract.
Care of Personal Data	
Data Breach Notification • In the event of a data breach, the PDP Law states that a controller must notify both the affected data subject(s) and the Indonesian data protection authority with 72 hours, unless an exception applies.	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 PDP Law obligates Controllers to cease processing personal data in the event that the retention period has been reached; the purpose of the processing has been achieved; or a data subject	Customer Responsibility: • Customers should delete the personal data it holds once its purpose has expired. Google Cloud Commentary:

requests that the Controller cease processing, unless an exception applies. • Subject to certain exceptions, Controllers must also delete personal data in the event that it is no longer necessary to achieve the purposes of processing; a personal data subject has withdrawn their consent; there is a request from a personal data subject to delete it; or personal data is obtained and/or processed in an unlawful manner. • Furthermore, the PDP Law requires controllers to destroy personal data in the event that: the retention period has expired; a data subject requests destruction; the personal data is not related to the settlement of the legal process of a case; and/or personal data is obtained and/or processed in an unlawful manner.	• 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 • Entities processing personal data have an obligation to protect the security of personal data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or loss. • Controllers must prepare and implement operational technical measures to protect personal data processing. The PDP Law dictates that Controllers shall determine the level of security required by taking into account the nature and risks of personal data. • Controllers must prevent personal data from being accessed illegally. Under the law, this can be accomplished through the use of a security system and/or by processing personal data using an electronic system in a reliable, secure, and responsible manner.	Customer Responsibility: • Customers should implement sufficient security controls to protect the personal data 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 Indonesia Personal Data Protection Law.