Google Cloud Whitepaper
May 2022

New Zealand's Privacy 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 May 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 safeguard your customer data and provide you with tools and features to control it on your terms.

This whitepaper provides information to our customers about New Zealand's Privacy Act 2020 ("the Privacy Act") and how Google Cloud leverages Google's industry-leading data privacy and security capabilities to store, process, maintain, and secure customer data. We are committed to partnering with our customers so they can deploy workloads using Google Cloud services and Google Workspace for their productivity needs in a manner that aligns with the PIPA's requirements. We explain our data protection features and highlight how they map to the PIPA's requirements. However, please note that, as a provider of cloud services, we are not in a position to provide you with legal advice - this is something only your legal counsel can provide.

Overview of the New Zealand Privacy Act

The Privacy Act 2020 (the Privacy Act) came into effect on December 1, 2020, repealing and replacing the Privacy Act 1993. The updated law covers many of the same concepts as the 1993 law, but adds provisions covering extraterritorial application, mandatory breach notification, access requests, Privacy Commissioner enforcement powers, and certain criminal offenses and penalties. Key to the Privacy Act 2020 are its thirteen Information Privacy Principles that govern how organisations should collect, handle and use personal information.

The purpose of the Privacy Act is to promote and protect individual privacy by providing a framework for protecting an individual's right to privacy of personal information while recognising that other rights and interests may at times also need to be taken into account. The Privacy Act gives effect to internationally recognised privacy obligations and standards in relation to the privacy of personal information, including the OECD Privacy Guidelines and the International Covenant on Civil and Political Rights.

The Principles regulate how agencies should conduct data processing activities. The first four principles govern how agencies can collect personal information (including the purpose, source, and manner of collection, along with transparency requirements); the next three govern storage of personal information (including storage and security and individuals' rights to access and correction); and the

[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.
In this whitepaper "customer data" and "your data" refers to the customer data we process according to your Google Cloud agreement(s).

final six (accuracy, retention, use, disclosure, cross-border transfer, and use of unique identifiers) govern agencies' use and sharing of personal information.

Unlike many other global privacy laws, the Privacy Act does not use the terms "controller" or "processor." The Privacy Act instead applies primarily to "agencies" that process personal information on their own behalf (analogous to a controller), and imposes liability on "agents of a 'principal agent'" (analogous to a processor) only where there have been certain privacy breaches. If an agency (A) holds information as an agent for another agency (B) (e.g., a processor or service provider relationship), then the personal information is to be treated as being held by B, and not A. However, the personal information is to be treated as being held by both A and B if A also uses or discloses the information for its own purposes.

The term "agency" includes an "overseas agency," and the Privacy Act applies to data processing activities by overseas agencies undertaken in the course of carrying on business in New Zealand. Factors organisations should assess when determining whether they are "carrying on business" in New Zealand are explained in the Disclosing personal information outside New Zealand guidance. An agency may be treated as "carrying on business" in New Zealand without necessarily being a commercial operation, having a place of business in New Zealand, receiving any monetary payment for the supply of goods or services, or intending to make a profit from its business in New Zealand.

The New Zealand Privacy Commissioner has released a series of guidance documents relating to the Privacy Act, including information sheets on issues like breach notifications and the updated Privacy Principles. The Privacy Commissioner has also released guidance on disclosing personal information outside New Zealand and guidance material for small to medium sized businesses, to help them protect personal information when using cloud computing.

The Privacy Commissioner can also issue "Codes of Practice" which may provide guidance or alter the law. These codes modify the operation of the Privacy Act and set rules for specific industries, organisations, or types of personal information. There are currently six codes covering areas such as telecommunications information, credit reporting, and health information.

Google Cloud data protection overview & the Shared Responsibility Model

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

Topics

Google Cloud's approach to data protection and privacy
- Data privacy trust principles
- Dedicated privacy team
- Data access and customer control
- Restricted access to customer data
- Law enforcement data requests

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

Google Cloud's approach to data protection and privacy

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

Data protection and privacy trust principles

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

Our commitments to you about your data

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

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

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

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

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

Dedicated privacy team

The Google privacy team operates separately from product development and security organisations, but participates in every Google product launch by reviewing design documentation and performing code reviews to ensure that privacy requirements are followed. They help release products that reflect strong privacy practices: transparent collection of user data, providing users and administrators with meaningful privacy configuration options, and continuing to be good stewards of any information stored on our platform. To learn more about our privacy team, refer to the privacy team section of the Google security whitepaper for Google Cloud and the Google Workspace Security whitepaper.

Data access and customer control

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

Restricted access to customer data

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

Google Cloud's approach to data security

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

Strong security culture

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

To learn more about our security culture, refer to the security culture sections in our Google security whitepaper and our Google Workspace Security whitepaper.

Security team

Google employs more than 850 security professionals, including some of the world's foremost experts. This team maintains the company's defense systems, develops security review processes, builds security infrastructure, implements Google's security policies, and actively scans for security threats. Our team also takes part in research and outreach activities to protect the wider community of Internet

users, beyond just those who choose Google solutions. Our research papers are available to the public. As part of our outreach efforts, we have a team known as Project Zero that aims to prevent targeted attacks by reporting bugs to software vendors.

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

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

Trusted infrastructure

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

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

Infrastructure redundancy

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

State-of-the-art data center security

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

Data encryption

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

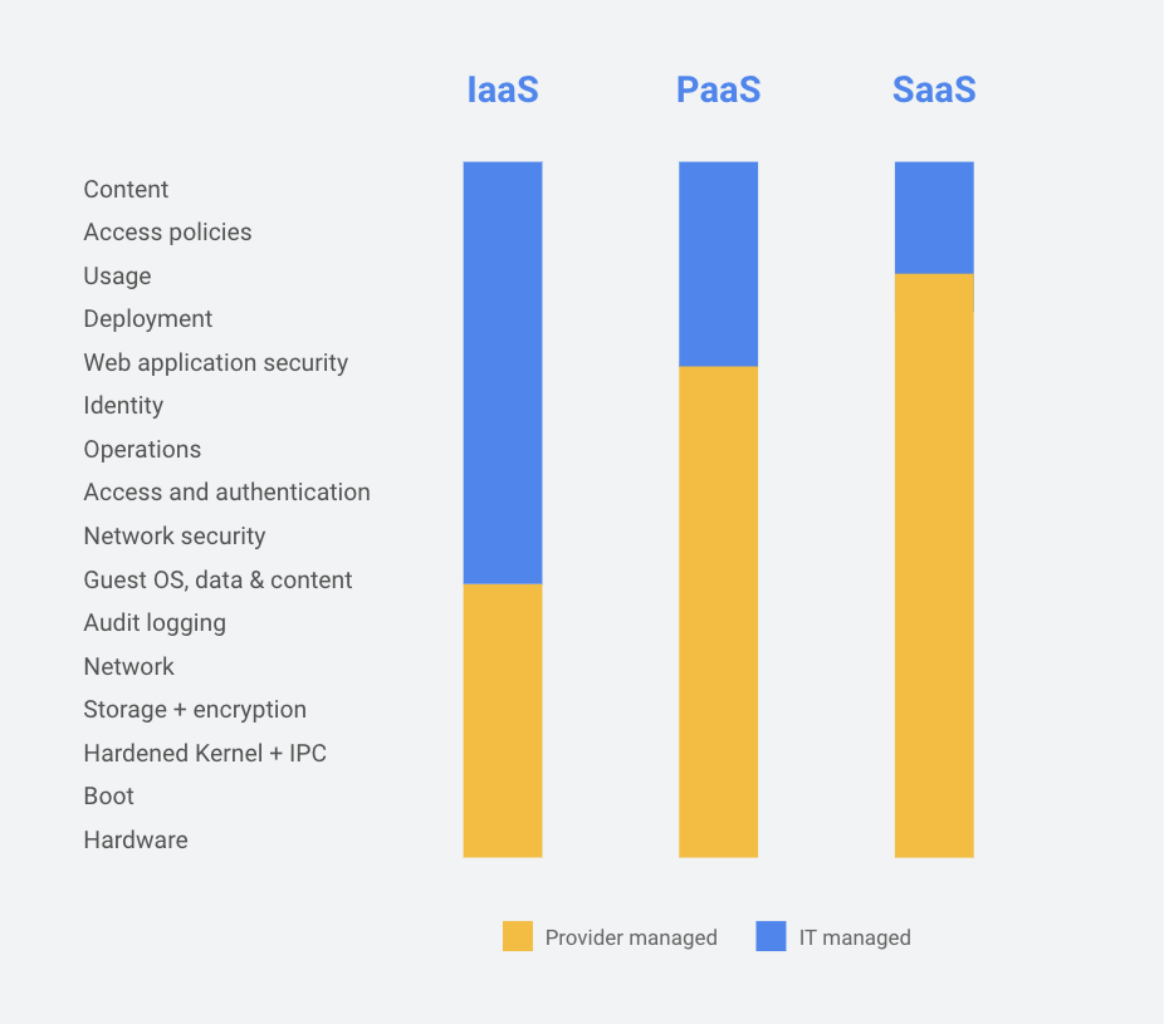
Cloud-native technology

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

The Shared Responsibility Model

Under our Shared Responsibility Model, the cloud customer and its CSP share the responsibilities of managing the IT environment, including those related to security and compliance. As a trusted partner, Google Cloud's role in this model includes providing services on a highly secure and controlled platform and offering a wide array of security features from which customers can benefit. Shared responsibility enables our customers to allocate resources more effectively to their core competencies and concentrate on what they do best. The shared responsibility model does not remove the accountability and risk from customers using Google Cloud services, but it does help relieve the burden as we manage and control system components and physical control of facilities. It also shifts a portion of the cost of security and compliance onto Google Cloud services 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 New Zealand's Privacy Act

Data Protection Obligations	Who Has the Responsibility
Collection, Use, and Disclosure of Personal Information	
Notice of Collection • Under Principle 3, agencies must take reasonable steps to make sure that the person knows, either before the point of collection or as soon as practicable after it is collected: why it's being collected; who will receive it; whether giving it is compulsory or voluntary; what will happen if they don't disclose the information; and their rights to access and correction of the information. • There are certain exceptions to this obligation (e.g., if providing notice would undermine the purpose of the collection or if it's not practicable to inform the individual). • See here for additional guidance on Principle 3 and privacy statements.	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 • Principle 1 states that organisations must only collect personal information if it is for a lawful purpose connected with their functions or activities, and the information is necessary for that purpose. • See here for additional guidance on Principle 1 and purpose limitation obligations.	Customer Responsibility: • To ensure collection, use, or disclosure of personal information 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 it for any other products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.
Source	Customer Responsibility:

• Principle 2 states that personal information should be collected directly from the person it is about. • However, organisations can collect personal information from other people other than the person in certain circumstances (e.g., if the person concerned authorizes collection from someone else or if it's necessary to uphold or enforce the law). • See here for additional guidance on Principle 2.	• Customers should make all efforts to collect information directly from the individual, unless certain circumstances apply. Google Cloud Commentary: • You decide which Services to use, how to use them, and what information to collect.
Manner of Collection • Principle 4 states that personal information must not be collected by unlawful, unfair or unreasonably intrusive means. When an organisation collects information about a person, it has to do so in a way that is fair and legal. • What is reasonable under the law depends on the circumstances, such as the purpose for collection, the degree to which the collection intrudes on privacy, and the time and place it was collected. • See here for additional guidance on Principle 4.	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.
Personal Information Use • In general, under Principle 10, an agency can only use personal information for the purpose it was collected. • Agencies may use personal information for additional purposes set forth in the law (e.g., for a purpose that is directly related to the purpose in connection with which the information was obtained or for a purpose authorized by the individual). • See here for additional guidance on Principle 10 and personal information use.	Customer Responsibility: • To ensure the use of personal information is limited to the purposes for which it was collected. 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 it for any other products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.
Personal Information Disclosure • Principle 11 states that an organisation may only disclose personal information in limited circumstances. • For example, the agency that holds the	Customer Responsibility: • To ensure personal information is disclosed in connection with a permitted purpose.

personal information may disclose it if the disclosure is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained. An agency may also disclose information if the individual concerned has consented to such disclosure. • Disclosure is also permitted under the law if it is necessary to enable an intelligence and security agency to perform any of its functions. • See here for additional guidance on Principle 11 and personal information disclosure.	Google Cloud Commentary: • Google commits to only access, use or disclose your data to provide the services ordered by you and in accordance with the contract terms. If Google Cloud receives a government request for information, we will attempt to redirect the request to the customer and only disclose if strictly necessary to comply with legal process. (See our Government Requests for Cloud Customer Data whitepaper).
Cross-Border Data Disclosure • Principle 12 sets rules around sending personal information to organisations or people outside New Zealand. • An agency may only disclose personal information to another organisation outside New Zealand if the receiving organisation: is subject to the Privacy Act because they do business in New Zealand; is subject to privacy laws that provide comparable safeguards to the Privacy Act; agrees to adequately protect the information (e.g. by using model contract clauses); or is covered by a binding scheme or is subject to the privacy laws of a country prescribed by the New Zealand Government. • If none of the above criteria apply, an agency may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act. • The Privacy Commissioner has released guidance on cross-border disclosures and model privacy clauses. This guidance makes clear that sending information to another organisation to hold or process on your behalf (as your agent), will not be treated as a disclosure under the Privacy Act 2020. This could be, for example,	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.

when an agency is providing cloud storage services on behalf of the NZ based client. Under such circumstances, the principal organisation will be responsible for ensuring that the agent handles the personal information in accordance with the New Zealand Privacy Act. • Similarly, organisations generally do not need to enter into an agreement with a cloud service provider which incorporates the model clauses because, for the purposes of the Privacy Act, the organisation will (in most circumstances) remain responsible for the personal information that it puts in the cloud. • See here for additional guidance on Principle 12 and cross-border disclosure.	
Accountability	
Requests for access to personal information • Principle 6 states that people have a right to ask for confirmation of whether an agency holds any personal information about them and to ask for access to their own personal information. • See here for additional guidance on Principle 6.	Customer Responsibility: • To develop procedures and capabilities to allow individuals to access their personal information. Google Cloud Commentary: • Customers may access customer 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 provide functionality to access customer data that you or your users put into our systems.
Requests for correction of personal information • Under Principle 7, an individual has a right to ask an organisation or business to correct information about them if they think it is wrong. • See here for additional guidance on Principle 7.	Customer Responsibility: • To develop procedures and capabilities to allow individuals to rectify 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 the correction of 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 rectify any data that you or your users put into our systems.
Care of Personal Information	
Accuracy • Under Principle 8, an agency that holds personal information must not use or disclose that information without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant, and not misleading. • Individuals that have suffered harm as a result of the use of inaccurate information may file a complaint with the Privacy Commissioner. • See here for additional guidance on Principle 8 and the accuracy of information.	Customer Responsibility: • 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, 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 • The Privacy Act introduces mandatory privacy breach notification requirements for organisations when a notifiable privacy breach has occurred having affected individuals. This includes notification to the Privacy Commissioner and to affected individuals as soon as practicable after becoming aware that a notifiable privacy breach has occurred. • Agencies must consider several elements when assessing whether a privacy breach is likely to cause serious harm (i.e., to determine whether the breach is "notifiable"), such as any action it took to reduce the risk of harm following the breach or whether the personal	Customer Responsibility: • Customers should develop policies and procedures for effectively addressing data breaches, including early warning systems, effective communication protocols, and robust remediation procedures. Google Cloud Commentary: • Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. • Google Cloud has dedicated teams and processes in place to enable us to promptly resolve and notify you of data incidents.

information is sensitive. ● Agencies can use the Privacy Commissioner's "NotifyUs" tool to report a breach. This tool allows agencies to undertake a privacy breach self-assessment, report a notifiable privacy breach, and update a report as necessary.	● More information on Google's data incident response process is available in our Data incident response whitepaper.
Retention ● Privacy Principle 9 states that an agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used. ● See here for additional guidance on Principle 9.	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 ● Under Principle 5, organisations must ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information. This includes making sure personal information is protected from loss, accidental or unauthorised disclosure, access, use or modification or any other misuse. ● See here for additional guidance on Principle 5 and security obligations.	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
Unique Identifiers • Principle 13 prescribes rules for assigning and handling personal identifiers such as a driver's licence number, a passport number, a student ID number, or an IRD number. • It states that an agency can only use unique identifiers when it is necessary and cannot assign a unique identifier to a person if that unique identifier has already been given to that person by another agency. • Agencies must also take reasonable steps to protect unique identifiers from misuse. • See here for additional guidance on Principle 13 and unique identifiers.	Customer Responsibility: • Customers should assign unique identifiers only if necessary and implement procedures for the management and protection of personal identifiers. Google Cloud Commentary: • Google commits to process and protect your data in accordance with the contract terms. For more information on how Google protects customer data, see above.

Conclusion

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

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

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