Google Cloud Whitepaper
October 2021

Google Cloud & Australian Privacy Principles

Table of Contents

Disclaimer

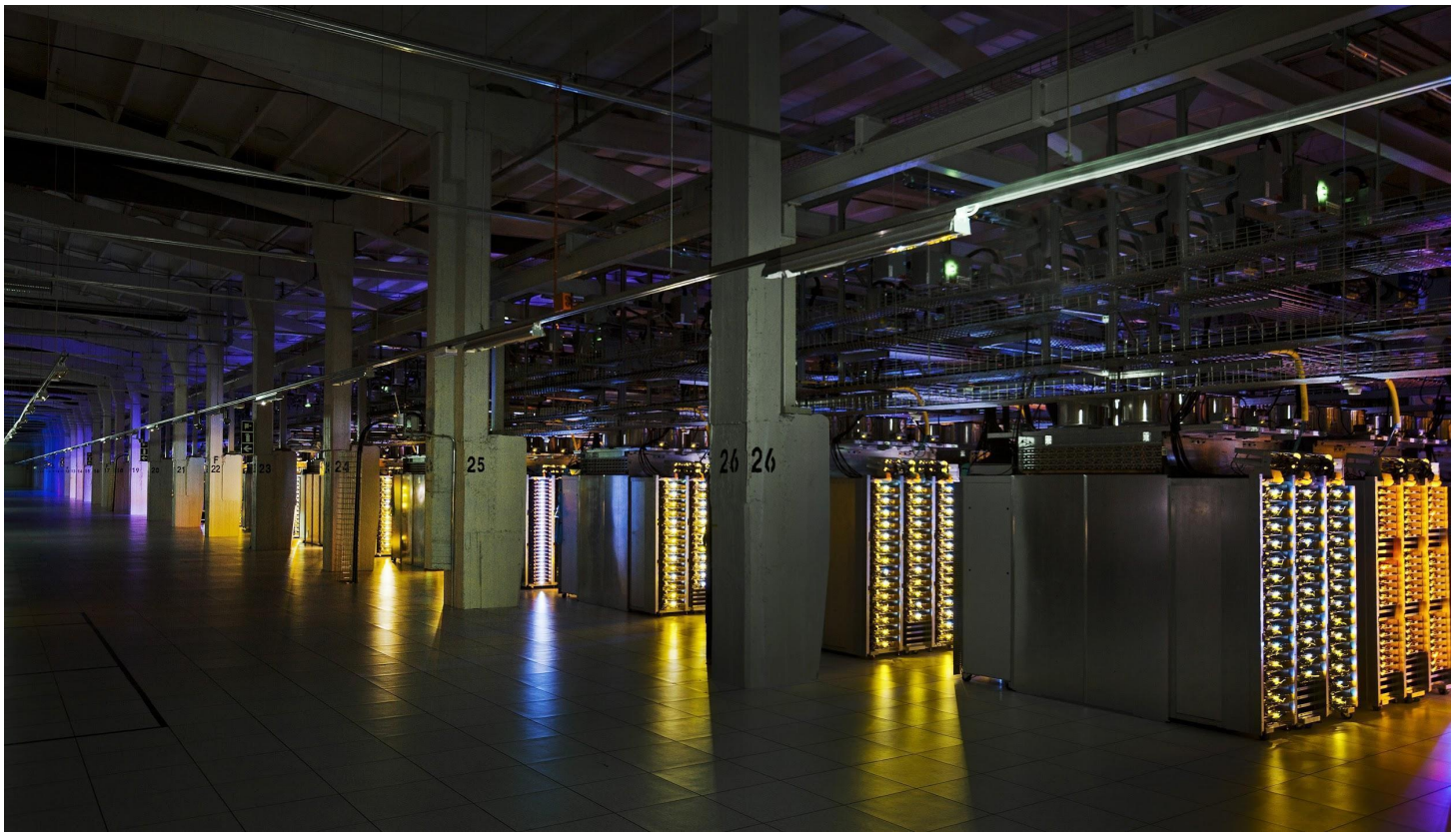
This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of October 2021 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

This paper is intended to help customers of Google Cloud understand Google's security and privacy features and provide insight into how Google Cloud Platform and Google Workspace service offerings may help organizations achieve compliance with the requirements under the Australian Privacy Act 1988 (Cth) (the "**Privacy Act**") and by the Australian Privacy Principles while running their workloads on Google's infrastructure. Specifically, this paper explains how information is stored, processed, secured, accessed, and maintained in Google Cloud.

This paper has six sections:

Section 1: The Privacy Act and the Australian Privacy Principles
Section 2: Security and Trusted Infrastructure
Section 3: Data Protection and Privacy
Section 4: Australian Privacy Principles mapping to Google controls
Section 5: Notifiable data breaches
Section 6: Conclusion



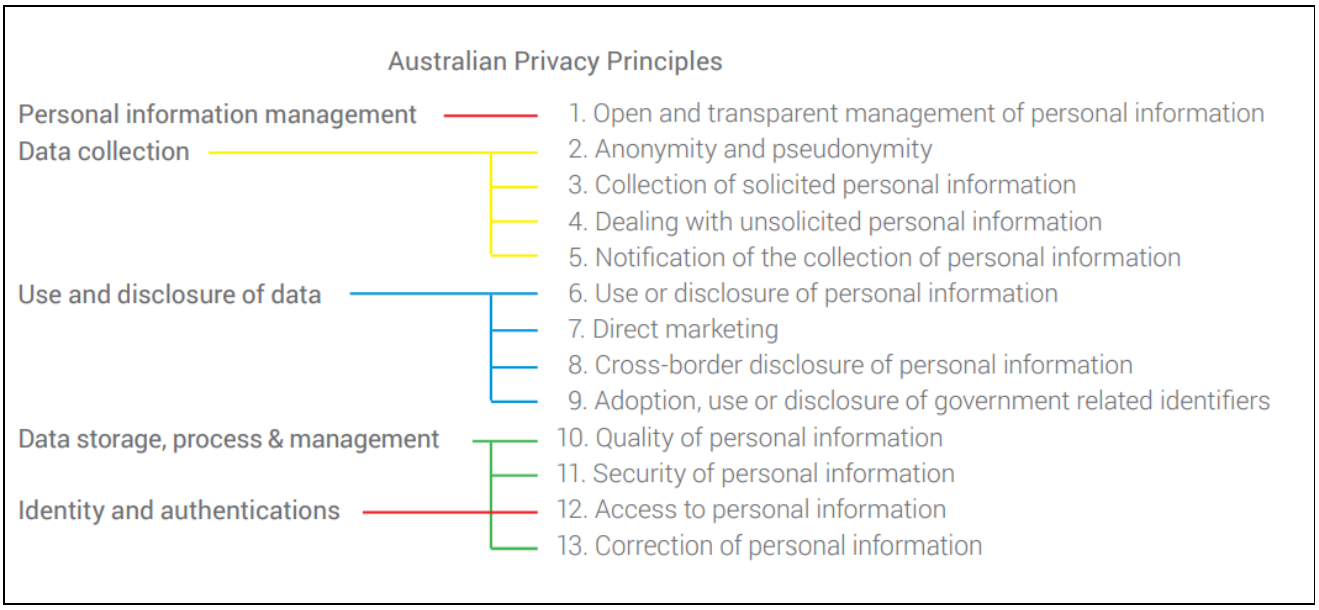
Section 1: The Privacy Act and the Australian Privacy Principles

What is the Privacy Act?

The Privacy Act 1988 (Cth) (Privacy Act), which includes the Australian Privacy Principles (APP), regulates how organisations and government agencies handle the personal information as well as the sensitive information of individuals. There are 13 Australian Privacy Principles.

These principles give individuals the right to:

- Know why their personal information is being collected,
- Know how such information will be used,
- Know whom their personal information will be disclosed to,
- Have the ability to ask for access to their personal information, and
- Ask for correction of their personal information.



More details on the Privacy Act can be found on the Australian Information Commissioner's website. Customers of cloud computing providers are responsible for ensuring they comply with their obligations under the Privacy Act, including the Australian Privacy Principles.

The Australian Privacy Principles and Google Cloud

Google undergoes independent third-party audits on a regular basis. These audits verify the security, privacy and compliance controls present in Google data centres, its infrastructure and its operations.

Google Cloud Platform is an IaaS/PaaS/SaaS public cloud-based offering from Google. Google Cloud Platform has annual audits for the following standards:

- **SSAE 16 / ISAE 3402 Type II**:
  - SOC 1
  - SOC 2
  - SOC 3
- **ISO 27001** is one of the most widely recognized, internationally accepted independent security standards. Google has earned ISO 27001 certification for the systems, applications, people, technology, processes and data centres serving Google Cloud Platform. View Google Cloud Platform ISO 27001 Certificate. Google has also earned the ISO 27001 certification for Google's shared Common Infrastructure. View the Common Infrastructure ISO 27001 Certificate.
- **ISO 27017**, Cloud Security, is an international standard of practice for information security controls based on ISO/IEC 27002 specifically for cloud services. View the Google Cloud Platform ISO 27017 Certificate.
- **ISO 27018**, Cloud Privacy, is an international standard of practice for protection of personally identifiable information (PII) in public cloud services. View the Google Cloud Platform ISO 27018 Certificate.
- **ISO 27701** is an international data privacy standard that is an extension of the ISO 27001 standard, with an emphasis on the creation of a Privacy Information Management System (PIMS). Google Cloud Platform and Google Workspace have received an accredited ISO/IEC 27701 certification as PII processors.

Google Workspace is a SaaS public cloud-based offering from Google. Google Workspace is a set of intelligent apps including Gmail, Docs, Drive, Calendar, Sites and Hangouts. Google designed Google Workspace to meet stringent privacy and security standards based on industry best practices. Google Workspace has annual audits for the following standards:

- **SSAE 16 / ISAE 3402 Type II**:
  - SOC 1
  - SOC 2
  - SOC 3
- **ISO 27001** is one of the most widely recognized, internationally accepted independent security standards. Google has earned ISO 27001 certification for the systems, technology, processes and data centres that run Google Workspace. View the Google Workspace ISO 27001 Certificate.
- **ISO 27017**, Cloud Security, is an international standard of practice for information security controls based on ISO/IEC 27002 specifically for cloud services. View the Google Workspace ISO 27017 Certificate.
- **ISO 27018**, Cloud privacy, is an international standard of practice for protection of personally identifiable information (PII) in public cloud services. View the Google Workspace ISO 27018 Certificate.

- **ISO 27701**, Cloud privacy, is an international standard of practice focused on the collection and processing of personally identifiable information (PII). Request the Google Workspace ISO 27701 Certificate.

For more information on Google certifications, audits, and assessments, see the Google Cloud Platform and Google Workspace security web pages.

Security as a Shared responsibility model

As Security and Compliance is a shared responsibility between Google and the customer, it's critical to understand the shared responsibility model and which Security and Compliance tasks are handled by Google and which tasks are handled by the customer. The workload responsibilities vary depending on whether the workload is hosted on Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or in an on-premises datacenter

Section 2: Security and Trusted Infrastructure

Google maintains geographically distributed data centres. Google stores all production data in physically secure data centres.

Google data center infrastructure redundancy

Google Cloud Platform services are available in locations across the Americas, Europe, Australia and Asia. These locations are divided into regions and zones. A full list of Google Cloud Platform regions can be found on Cloud Locations Map.

Google Workspace services are available in locations across North America, Europe, South America and Asia. Customers can choose to store their data in the United States, Europe or configure global storage. Additionally, data regions offer the flexibility to choose one data region for some of your users, or different data regions for specific departments or teams. Please check this page for more information. A full list of Google Workspace datacenter locations can be found at Cloud Workspace datacenter locations.

Certain Cloud Platform resources are hosted in multiple regions globally, while other resources, including (but not limited to) Google Compute Engine virtual machine instances, Persistent Disks, Cloud Storage buckets, App Engine applications, Cloud Bigtable, Dataproc, BigQuery datasets and Cloud VPN can be created and deployed within specific geographic regions.

Customers can take advantage of Google Cloud infrastructure by replicating data within selected geographic regions for redundancy and availability or by choosing a specific geographic region based on latency considerations. For more information on data locality for Google Cloud Platform services, see Geographic management of data and Google Cloud Platform Service Level Agreements.

Additionally, service-interrupting events can happen at any time. Google Cloud Platform provides many of the facilities customers need to implement a robust, targeted and well-tested disaster recovery plan, such as redundancy, scalability, compliance and security. The Disaster Recovery Cookbook provides some scenarios to show how Google Cloud Platform can help. In Google Workspace, Google has designed the platform components to be highly redundant. This redundancy applies to Google server design, how Google stores data, network and Internet connectivity and the software services themselves. This ‘redundancy of everything’ model includes the handling of errors by design and creates a solution that is not dependent on a single server, data centre or network connection. Google’s data centres are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software or network failure, data is automatically shifted from one facility to another ensuring that Google Workspace customers can continue working in most cases without interruption. Customers with global workforces can collaborate on documents, video conferencing and more without additional configuration or expense. Global teams share a high performance and low latency experience as they work together on a single global network.

Google data centre security

Google's data centres employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas.

Google's data centres maintain an on-site security operation responsible for all physical data centre security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor closed-circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data centre regularly.

Google maintains formal procedures for allowing physical access to the data centres. The data centres are housed in facilities that require electronic card key access, with alarms that are linked to the on-site Security Operations. All entrants to the data centre are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centres. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Access to a Google data centre's secure floor, where Google's production servers are housed, is controlled via a security corridor that implements multi-factor access control using security badges and biometrics. Only approved individuals with specific roles may enter. More information on Google data centre access and site controls can be found on the Google Cloud Platform Data Processing and Security Terms, Appendix 2: Security Measures and Google Workspace Data Processing Amendment, Appendix 2: Security Measures.

For more information on Google's data centres, visit our keyword and data center homepage for more information.

Data in transit

Google supports various encryption protocols and ciphers to protect data in transit between the customer and Google. It is the customer's responsibility to use a secure browser that supports the latest encryption and security updates. This ensures that machines connecting to Google Cloud are configured to use appropriate encryption for Google-to-customer communications.

Data in transit includes data traveling between the customer and Google, and within Google's infrastructure. The sections below provide more details on Google's network protection and encryption measures for each kind of data in transit.

Between a customer and Google

When a user sends a request to Google, Google secures the data in transit with authentication, integrity and encryption by using the HTTPS protocol with a certificate from a public certificate authority. Since 2011, Google has been using forward secrecy in its transport layer security (TLS) implementation. Forward secrecy makes sure the key that protects a connection is not persisted, so an attacker who intercepts and reads one message cannot read previous messages.

When a Google Workspace customer transfers data to Google data centers, we encrypt traffic between your browser and our data centers. Google websites and properties use robust public key technologies: 2048-bit RSA or P-256 ECDSA TLS certificates issued by a trusted authority. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA forward secrecy methods by default. This helps ensure that information encrypted today is less vulnerable to new methods of breaking encryption in the future and prevents a connection's private keys from being kept in persistent storage. Keys are rotated at least every other day limiting the impact of a compromised encryption key.

The list of Google-supported encryption protocols and ciphers may change from time to time. For more information on the cryptographic library, see the BoringSSL library that Google maintains.

Within Google data centres

Remote Procedure Calls (RPC) within Google data centres are cryptographically authenticated. Jobs in Google's data centres authenticate RPCs to each other, and furthermore the infrastructure automatically encrypts all infrastructure RPC traffic which goes over the WAN between data centres, without requiring any explicit configuration from the service.

Between a customer and non-Google users

Customer data is encrypted when on Google's internal networks, in transport and at rest. Google uses encryption when customer data traverses public networks. Encryption may be open-source based or proprietary. In addition, Google forces Transport Layer Security (TLS) for all authentication traffic.

In Google Workspace, when customers send email from Google to a non-Google server that supports TLS, the traffic will be encrypted, preventing passive eavesdropping. Google has improved email security in transit by developing and supporting the MTA-STS standard allowing receiving domains to require transport confidentiality and integrity protection for emails. Google Workspace customers also have the extra ability to only permit email to be transmitted to specific domains and email addresses if those domains and addresses are covered by TLS.

Data at rest

Google Cloud encrypts customer content stored at rest, without any action required from the customer, using one or more encryption mechanisms. All data stored in Google Cloud is encrypted at the storage level using AES256, with the exception of a small number of Persistent Disks created before 2015 that use AES128. Google uses a common cryptographic library, Tink, which incorporates our FIPS 140-2 validated module, BoringCrypto, to implement encryption consistently across almost all Google Cloud products.

In Google Cloud Platform, customers can choose one of the following key management solutions to manage the encryption keys that protect the data encryption keys that protect their data:

- Default Google encryption: Key encryption keys are stored in Google's internal Key Management Service.
- Customer-managed encryption keys (CMEK) using Cloud Key Management Service (KMS): Key encryption keys are stored in Cloud KMS.
- Customer-supplied encryption keys (CSEK), available in Google Compute Engine and Google Cloud Storage services: Key encryption keys are provided by the customer as part of every API call.

In addition, customers can encrypt the data themselves before importing it into Google Cloud Platform services.

In Google's data centers, data belonging to Google Workspace customers is stored at rest in two types of systems, disks and backup media. Disks are used to write new data as well as store and retrieve data in multiple replicated copies. Google also stores data on offline backup media to help ensure recovery from any catastrophic error or natural disaster at one of our data centers. Data stored at rest is encrypted on both disks and backup media.

For more information on encryption and key management, see the Google Workspace Encryption Whitepaper, the Google Cloud Platform Encryption in Transit Whitepaper and Google Cloud Platform Encryption at Rest Whitepaper.

Section 3: Data Protection and Privacy

Both GCP and Google Workspace offer our customers the ability to control the access to data and services, to help ensure that customer data is protected in accordance with the organization's desired configuration. Our Google Cloud Trust Principles summarize our commitment to protecting the privacy of data stored by customers in Google Cloud.

Data Privacy on GCP and Google Workspace

The customer data stored and managed on GCP and Google Workspace is only used to provide that customer with services in accordance with their contract and for no other purpose. Not for advertising, not for anything else.

For further information around how Google helps our customer's secure and protect their data on the cloud, refer to our Privacy Resource Center and our GCP Trust whitepaper.

If Google receives a government request for cloud customer data, it is Google's policy to direct the government to request such data directly from the cloud customer. We have a team that reviews and evaluates each and every one of the requests we receive based on international human rights standards, our own policies, and the law. Google does not provide any government entity with "backdoor" access. Detailed information is available in our Transparency Report and Google Cloud Government Requests White Paper. We provide an overview of the implications of encryption for government data requests in our white paper: **Government requests for customer data: controlling access to your data in Google Cloud** (available under NDA).

Google Workspace offers audit logs to help security teams maintain audit trails in Google Workspace and view detailed information about Admin activity, data access, and system events. Google Workspace users can use the Admin Console to access the logs and customize and export logs as required. Customers can use app access control, to see which third-party apps users have approved to access their Google Workspace data and can then limit access to trusted apps. We also help our customers manage risk with app verification, which ensures that apps accessing Gmail data meet security and privacy standards. For more information on data protection and privacy features available in Google Workspace, please refer to the Google Workspace Trust whitepaper.

Google offers its customers a detailed Google Workspace Data Processing Amendment and Google Cloud Platform Data Processing and Security Terms that describe its commitment to protecting customer data.

Identity and authentication

Google Cloud Platform and Google Workspace use Google Accounts for authentication and access management. Google recommends using fully managed corporate Google accounts for increased visibility, auditing and control over access to Cloud resources.

Cloud Identity provides free, managed Google Accounts you can use with Google services including Cloud Platform. Using Cloud Identity accounts for each of your users, you can manage all users across your entire domain from the Google Admin console.

If you're a Google Workspace administrator, you can manage all of your users and settings through the Google Workspace Admin Console. By default, all new users are assigned a Google Workspace license. If you have a subset of developers who don't require Google Workspace licenses, you can add Cloud Identity accounts instead. For more information, see Get started with Cloud Identity.

The customer is responsible for managing all aspects of access control (authentications) for the customer's users of Google Cloud, and can take advantage of rich authentication features including single-sign-on (SSO), OAuth and two-factor verification to protect their Google Accounts.

Single sign-on : Google supports SAML 2.0-based SSO, which provides seamless SSO against Cloud Platform Console, web- and command-line-based SSH, and OAuth authorization prompts. Cloud Platform's command-line interface tools, such as gcloud, gsutil, and bq, use SAML 2.0-based SSO for browser-based authentication as well. For information about setting up Google SSO, see Set up Single Sign-On for Google Workspace accounts. This guide applies to both Cloud Platform and Google Workspace, because both products share a common directory, authentication and SSO infrastructure.

OAuth : Google APIs use OAuth 2.0 protocol for authentication and authorization to determine the identity of a user and what permissions an authenticated user has on a set of specific resources. Google supports common OAuth 2.0 scenarios such as those for web server, installed and client-side applications. For information about setting up OAuth 2.0, see using OAuth 2.0 to Access Google APIs.

2-Step Verification : A combination of a Google password and a credential using Google 2-Step Verification adds an extra layer of security to a customer account by requiring the user to enter a verification code or using a physical security key in addition to their username and password when signing into their account. Google provides three simple ways to implement 2-step Verification.

Verification Method	Software or Hardware	Requirements
Text message	Software	Cellular service and a powered mobile device
Google Authenticator	Software	Powered mobile device
Security Keys	Hardware	Google Chrome desktop browser (version 40+), iOS, Android

More information on how to set up the security keys on a Google Cloud Platform account can be found on Securing your Cloud Platform Account with Security Keys.

In addition, on Google Cloud Platform, Cloud Identity and Access Management (IAM) can help customers to manage individual access permissions for certain Google Cloud Platform resources. Customers can assign individuals to a group and role membership by configuring their application via Google Cloud Identity and Access Management (IAM) policies or Access Control Lists (ACLs). These

access management capabilities can help customers to address the privacy of data and ensure that each individual only has access to their own data.

Google Workspace offers a set of configurable role-based access controls, security keys and 2-Step Verification and the Advanced Protection Program for organizations, to help mitigate risks such as the misconfiguration of employee access controls or attackers taking advantage of compromised accounts and enforce a curated set of strong account security policies for enrolled users.

To facilitate easier user access, while at the same time protecting the security of data, Google has developed context-aware access. This provides granular controls for Google Workspace apps, based on a user's identity and context. Based on the BeyondCorp security model developed by Google, users can access web applications and infrastructure resources from virtually any device, anywhere, without utilising remote-access VPN gateways while administrators can establish controls over the device.

Google also provides a rich set of logging and monitoring tools, such as Google Workspace Admin Console Report, Cloud Logging, Cloud Monitoring, and Cloud audit logs, that make it possible to collect and analyze request logs and monitor user activities.

Section 4: Australian Privacy Principles with Google Cloud

Summary of what the APP is/means Framework reference	Customer obligations	Google Cloud commentary
APP 1 - Open and transparent management of personal information	The customer is required to manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy. Customer to create a data inventory that describes how your business collects, uses, and shares personal information.	1. Google supports customer compliance by committing not to use customer data except for providing the service. This is addressed in the Data Processing and Security Terms for GCP and Data Processing Amendment to Google Workspace where Google makes commitments to protect your data. 2. Details on Google compliance collateral can be found at the compliance resource center. 3. Google has tools such as the Data Catalog that can help identify and classify data. 4. Create a data inventory that describes how your business collects, uses, and shares personal information. You can use some of our tools, such as Cloud Data Loss Prevention, to help identify and classify data
APP 2 - Anonymity and pseudonymity	Where practicable to do so, customers are required to give individuals the option of not identifying themselves, or of using a pseudonym.	
APP 3 - Collection of solicited personal information	Outlines how a customer can collect personal information that is solicited. It applies higher standards to the collection of sensitive information.	
APP 4 - Dealing with unsolicited personal information	Outlines the steps a customer must take if it receives unsolicited personal information.	
APP 5 - Notification of the collection of personal information	Outlines how a customer that collects personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters	
APP 6 - Use or disclosure of personal information	Outlines the circumstances when a customer may use or disclose personal information	

	that it holds.	
APP 7 - Direct marketing	A customer may only use or disclose personal information for direct marketing purposes if certain conditions are met.	This is a customer consideration.
APP 8 - Cross-border disclosure of personal information	Customers must take reasonable steps to ensure an overseas recipient does not breach the APPs before disclosing personal information to that overseas recipient.	A customer's obligation to comply with APP 8 arises where there is a "disclosure" of personal information to an overseas recipient. Guidance from the Office of the Australian Information Commissioner (OAIC) is such that where the customer does not release the handling of personal information from its effective control, this may be considered a "use" rather than a "disclosure" under the Privacy Act. As such, a customer's use of Google Workspace and Google Cloud Platform does not constitute a "disclosure" of personal information given the customer retains effective control over any personal information that may be uploaded and Google acts as a data processor in accordance with the customer's directions.
APP 9 - Adoption, use or disclosure of government related identifiers	Outlines the limited circumstances when a customer may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.	1. Google supports customer compliance by, committing not to use customer data except for providing the service this is addressed in the Data Processing and Security Terms for GCP and Data Processing Amendment to Google Workspace where Google makes commitments to protect your data. 2. Details on Google compliance collateral can be found at the compliance resource center
APP 10 - Quality of personal information	A customer must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. A customer must also take reasonable steps to ensure the personal information it uses or discloses is accurate,	

	up to date, complete and relevant, having regard to the purpose of the use or disclosure.	3. Google has tools such as the Data Catalog that can help identify and classify data. 4. Create a data inventory that describes how your business collects, uses, and shares personal information. You can use some of our tools, such as Cloud Data Loss Prevention, to help identify and classify data 5. For organizations that want more geo-control, the data regions feature for Google Workspace gives you the choice to pick where covered data for select Google Workspace apps is stored at rest — whether globally distributed, in the US, or across Europe.
APP 11 - Security of personal information	A customer must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. A customer has obligations to destroy or de-identify personal information in certain circumstances.	
APP 12 - Access to personal information	Outlines the customer obligations when an individual requests to be given access to personal information held about them by the customer. This includes a requirement to provide access unless a specific exception applies.	
APP 13 - Correction of personal information	Outlines a customer's obligations in relation to correcting the personal information it holds about individuals.	This is a customer consideration, however, Google has relevant products & services to assist including; Cloud Audit Logs - Track "Who did what, where, when" by maintaining three audit logs (Admin Activity, Data Access, System Event) for each GCP project, folder, and organization. Identity-Aware Proxy (IAP) - Control access to your cloud applications and VMs running on GCP by verifying user identity and the context of the request. Cloud Data Loss Prevention - Provides fast, scalable classification and redaction for sensitive data elements like names, credit card numbers,

		Google Cloud credentials, and more. Data Loss Prevention - Google Workspace - Scan files for sensitive content and prevent users from sharing sensitive content in Google Drive or shared drive with people outside your organization. Access Transparency - Google Workspace - Review logs of actions taken by Google staff when accessing user-generated text entered into Gmail, Docs, Sheets, Slides, and other apps. Vault - Google Workspace - Retain, search, and export your organization's data from select apps with Vault for Google Workspace Business and Enterprise editions.

Section 5: Notifiable data breach obligations

To support customers, incident response is a key aspect of Google's overall security and privacy program. We have a rigorous process for managing data incidents. This process specifies actions, escalations mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data.

In accordance with Section 7.2 ("Data Incidents") of the Data Processing and Security Terms and Data Processing Amendment, Google contractually commits to notifying customers promptly and without undue delay after becoming aware of a breach of Google's security that has led to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, customer data on Google Workspace or Google Cloud Platform. For more information, a paper on our data incident response process is available here: https://cloud.google.com/security/incident-response

Importantly, customers maintain control over their customer data stored in the Google Workspace and Google Cloud Platform. Google is not in a position to assess whether customer data uploaded in Google Workspace or Google Cloud Platform includes personal information, such that if a notifiable data breach did occur, the obligation to notify is not something that can apply to Google.

As such, it is the responsibility of customers to monitor for and take remedial action to prevent security incidents related to their use of Google Workspace and Google Cloud Platform, including

- in the case of a data breach that is likely to result in serious harm, providing notification to affected individuals and OAIC as required; and
- in the case where there are reasonable grounds to suspect a data breach has occured, undertaking an assessment to determine if notification to OAIC and affected individuals is required, in accordance with the Privacy Act.

Section 6: Conclusion

This document describes how customer information can be stored, processed, maintained, secured and accessed in Google Cloud using Google Cloud Platform and Google Workspace products, to enable customers to build a cloud infrastructure that is compliant with the Australian Privacy Principles.

Globally, public and private organizations are increasingly migrating to the cloud and unlocking the financial, security and operational benefits of operating from the cloud. GCP and Google Workspace provide public and private organizations with the scale, computing power, tools and services that they will need to set up secure, compliant, highly available, resilient infrastructure to both migrate and build their customer data and business applications.

To assist Google's customers in their cloud compliance journey, GCP and Google Workspace technologies and services are designed keeping compliance in mind, while enabling customers to keep pace with changes in their highly competitive and regulated business environments. By using GCP and Google Workspace products and service offerings, organizations can avail the transparency that Google provides to its customers with respect to how their information is handled and protected by Google Cloud.

To learn more about GCP and Google Workspace products and service offerings, or to contact us, please visit https://cloud.google.com/.

Google Cloud security
For general information on Google security and encryption of data at rest, see the Google Cloud whitepapers website.

Google Cloud Platform compliance
For information on Google Cloud Platform compliance and compliance certifications, see the Compliance section of the Google Cloud Platform website.

Google Workspace compliance
For information on Google Workspace compliance and compliance certifications, see the Compliance section of the Google Workspace websites.

Google Cloud Privacy Notice
For information on how Google Cloud handles Service Data
Google Cloud Privacy Notice