Google Cloud Whitepaper

June 2021

Act on the Protection of Personal Information (Japan)

Google Cloud

Google Cloud

Introduction

Personal identifiable information (PII) is critical to today's information systems. PII is sensitive both in terms of privacy and security, and violations of either could cause harm to both individuals and society. It is for these reasons that organizations have an obligation to protect PII, and governments have increased legislation and regulation around it. In Japan, the Act on the Protection of Personal Information (APPI) is one such regulation put in place to protect PII. This whitepaper will examine APPI from the perspective of adopting Google Cloud services. It will clarify the roles & responsibilities of cloud providers and cloud customers. It will also highlight Google cloud services that can assist customers with different aspects of APPI compliance as well as PII protection in general.

Scope

Personal Identifiable Information

This whitepaper will reference Personal Identifiable Information (PII), specifically PII that a customer places in Google Cloud Platform or Google Workspace. We will not speak to PII that customers provide directly to Google Cloud as a service provider. For more information on that topic please see our privacy notice.

Services

The principles in this paper apply to both Google Workspace as well as Google Cloud Platform which we will refer to collectively as Google Cloud for the sake of simplicity. This paper is intended to be for informational purposes only. Nothing in this whitepaper is intended to provide you with or should be used as a substitute for legal advice.

APPI Regulation

The APPI was first passed in 2003, and has since been ratified multiple times. The last update at the time of writing was June 2020, and that will become enforceable by June 2022. The Japanese government established the Personal Information Protection Commission (PPC) in 2016 as the primary regulator for APPI. It has the following scope:

- To audit and request reports from PII handlers (Article 40)
- To provide advice to PII handlers and issue directives (Article 41)
- To order a PII handler to cease APPI violations or take corrective action (Article 42, 43)

While the PPC does not have the authority to impose penalties, they can refer a case to law enforcement. In these circumstances, penalties can include both fines and even imprisonment for particularly egregious cases. In addition, false reports to the PPC or failure to comply with PPC orders may also be subject to fines. Furthemore, civil liabilities to those whose PII has been abused may also be possible.

The PPC is not the only regulator with regards to APPI. Some industry sectors also have sector specific guidance from their regulators. For example, the Ministry of Internal Affairs & Communication (MIC) and the Financial Services Agency (FSA) have published guidelines for their sectors as well. The PPC website is an excellent source of information on the Act and includes most relevant guidelines to its interpretation.

Key obligations

APPI lays out the key obligations that PII handlers have towards the individuals whose PII they handle. Below is a summary of the key obligations that PII handlers have towards an individual under APPI.

[1] Purpose (Articles 15 and 18)

A PII handler must notify the individual of the purpose for collecting their PII.

[2] Restrictions on Use (Article 16)

A PII handler may not process PII beyond the scope of the purpose, without the explicit consent of the individual.

[3] Consent (Article 17)

A PII handler must obtain the consent of an individual in order to collect PII that contains sensitive information. This includes race, beliefs, social status, religion, physical or mental disabilities, medical records, criminal history and facts related to being the victim of a crime.

[4] Accuracy (Article 19)

A PII handler must seek to keep an individual's PII accurate and up to date.

[5] Deletion (Article 19)

A PII handler must delete an individual's PII once the purpose of use has expired.

[6] Security Controls (Article 20)

A PII handler must implement security controls to protect the PII they handle.

[7] Supervision (Articles 21 and 22)

A PII Handler must implement sufficient supervision over employees and entrusted parties who handle the PII.

[8] 3rd Party Transfer (Article 23)

A PII handler must obtain additional specific consent from an Individual in order to transfer their PII to a 3rd party.

[9] Overseas Transfer to 3rd party (Article 24)

A PII handler must obtain additional specific consent from an individual in order to transfer their PII to a 3rd party in a foreign country except those countries specified by the PPC as having PII protection on par with Japan's.

[10] Disclosure (Article 28)

A PII handler must disclose to an individual the details of that individual's PII upon request.

Shared Responsibility Model

Google Cloud is responsible for the security of the cloud while our customers are responsible for the security of what they place in the cloud.

Google Cloud has a relationship with its customers but not with the individuals whose PII they collect. Google Cloud is not aware of PII our customers place in GCP or Google Workspace, nor do we act as handlers of that PII. The only interaction Google Cloud has with any customer data in our systems is to execute the services our customers select.

To further clarify we examine each of the ten key APPI requirements in terms of customer responsibility versus Google Cloud's responsibility.

[1] Purpose

A PII handler must notify the individual of the purpose for collecting their PII.

Customer Responsibility	Google Cloud Responsibility
Handle relationships with individuals and ensure the PII is collected in a lawful manner by clearly stating its purpose of use.	Google Cloud has no relationship with individuals a customer collects PII from and is not involved in stating the purpose of use nor deriving consent for it.

[2] Restrictions on Use

A PII handler may not process PII beyond the scope of the purpose, without the explicit consent of the individual.

Customer Responsibility	Google Cloud Responsibility
Handle relationships with individuals and ensure the PII is processed in a lawful manner by maintaining its stated purpose of use.	Google Cloud provides cloud services that a customer may select to use for PII.

[3] Consent

A PII handler must obtain the consent of an individual in order to collect sensitive PII.

Customer Responsibility	Google Cloud Responsibility
Ensure the necessary consent is collected.	Google Cloud has no relationship with individuals a customer collects PII from and is not involved in deriving consent from them.

[4] Accuracy

A PII handler must seek to keep an individual's PII accurate and up to date.

Customer Responsibility	Google Cloud Responsibility
Ensure the accuracy of PII.	Google Cloud provides cloud services that a customer may select to use for PII. Google Cloud is not involved in maintaining the accuracy of customer PII. Google Cloud does however ensure the integrity of data placed in our services.

[5] Deletion

A PII handler must delete an individual's PII once the purpose of use has expired.

Customer Responsibility	Google Cloud Responsibility
Delete PII once its purpose has expired or an Individual has requested it.	Google Cloud provides cloud services that a customer may select to use for PII. Customers can select to delete their data in Google Cloud at any time.

[6] Security Controls

A PII handler must implement security controls to protect the PII they handle.

Customer Responsibility	Google Cloud Responsibility
Implement sufficient security controls to protect the PII including proper configuration of features in the cloud under customer management.	Provide cloud services that have sufficient security controls for customers to safely build upon.

[7] Supervision

A PII handler must implement sufficient supervision over employees and entrusted parties who handle the PII.

Customer Responsibility	Google Cloud Responsibility
Put in sufficient controls to supervise handling of PII.	Google Cloud does not supervise our customer's use of the data they put in Google Cloud.

[8] 3rd Party Transfer

A PII handler must obtain additional specific consent from an Individual in order to transfer their PII to a 3rd party PII handler.

Customer Responsibility	Google Cloud Responsibility
The Personal Information Protection Commission (PPC) has stated that transfer of PII to a cloud provider who does not handle the PII does not constitute transfer to a 3rd party PII handler and therefore additional specific consent is not required. **Reference**: PPC Q&A Q5-33	Google Cloud has no relationship with individuals a customer collects PII from and is not involved in deriving consent for it, nor do we act as a PII handler on it.

[9] Overseas Transfer to 3rd party

A PII handler must obtain additional specific consent from an individual in order to transfer their PII to a 3rd party in a foreign country except those countries specified by the PPC as having PII protection on par with Japan's.

Customer Responsibility	Google Cloud Responsibility
Customers should obtain consent for cases where they transfer PII to an overseas 3rd party PII handler. **Reference**: PPC Q&A Q5-33, Q9-6	Google Cloud provides clear guidance on which of our services are located in Japan vs overseas.

[10] Disclosure

A PII handler must disclose to an Individual the details of that individual's PII upon request.

Customer Responsibility	Google Cloud Responsibility
Have a PII disclosure handling process.	Google Cloud has no relationship with individuals a customer collects PII from and can not handle disclosure requests.

Google Cloud

Frequently Asked Questions

[1] Does APPI allow data handlers to place PII in cloud services like Google Cloud?

Yes. APPI has no restrictions on the use of cloud services.

[2] Does placing PII in Google Cloud constitute a transfer to a 3rd party handler requiring additional specific consent?

The Personal Information Protection Commission (PPC) has stated that transfer of PII to a cloud provider who does not handle the PII does not constitute transfer to a 3rd party PII handler and therefore additional specific consent is not required.

Reference: PPC Q&A Q5-33

[3] Where can I find more information about the interpretation of the Act with respect to specific technologies and how that might affect consent requirements?

The PPC website is an excellent source of information on the Act and includes most relevant guidelines to its interpretation.

[4] APPI requires additional specific consent if the PII is stored overseas. So where is my data when I place it in Google Cloud?

The geographic scope of our services is on our website. Services that are marked as in the Tokyo or Osaka regions store data in Japan. Other services may store data overseas.

Google applies security measures consistently to its services regardless of their location so customers can rest assured that PII will benefit from that secure foundation regardless of if it's in Japan or Jakarta.

[5] How can I be sure that Google Cloud has adequate security around its services?

Google Cloud implements industry-leading security measures. We speak to these in our whitepapers including this one. We commit to them in our contract terms. We also have 3rd

party auditors check them against multiple international standards so as to provide assurance. We can provide audit reports and copies of certificates to meet your own audit assurance needs.

[6] How does Google Cloud handle government requests for data?

Google has to comply with the law in the countries we operate in including Japan. Our experience is that law enforcement agencies typically issue requests for data to the target of their investigation. It is rare to issue to the cloud provider of a company that handles the PII of the target of their investigation.

Google handles government requests by carefully vetting them to ensure they are legal, enforceable and scoped correctly. Invalid requests are refused. We notify and work with our customers where legally permissible. There is more on this in our Government Requests for Customer Data Whitepaper. In addition we publish a transparency report where customers can understand the nature of the requests we've received.

[7] How will Google Cloud monitor and respond to changes in regulations?

We employ an extensive team of lawyers, regulatory compliance experts, and public policy specialists who oversee privacy and security compliance. These teams engage with customers, industry stakeholders, and supervisory authorities to shape our cloud services in a manner that helps customers meet their compliance needs. These teams work closely with our customers to understand their unique compliance requirements and then collaboratively develop a strategy to address the requirements identified.

In addition, Google has a dedicated team of internal auditors and compliance specialists that reviews compliance with security laws and regulations around the world. As new auditing standards are created, the internal audit team determines what controls, processes, and systems are needed to meet them. This team facilitates and supports independent audits and assessments by third parties. The regulatory environment around the world is constantly evolving and Google Cloud will continue to evolve with it.

Google Cloud

APPI Security Guidelines

The PPC has published Guidelines (Japanese) that include recommended security measures for APPI compliance. Below is a summary of that guidance along with Google Cloud features and services that may be helpful in meeting them.

The PPC Guidelines sections 8.3-8.6 breakdown the security controls required into 4 categories:

1. Organizational Measures
2. Personnel Controls
3. Physical Security Controls
4. Technical Controls

Below are the requirements of each category mapped to security concepts. In the sections that follow we will explain how Google Cloud provides a secure foundation covering its side of the shared security model. Then we will introduce Google Cloud products and services that help customers with each security concept so they can meet the recommended security measures of the PPC Guidelines.

Organizational Measures

Requirement	Security Concept
Clarify roles & responsibilities of persons involved in PII handling.	Identity Data Governance
Have a mechanism for detection and reporting of PII incidents.	Threat Detection
Maintain records of PII handling including access & changes	Logging Data Governance
Maintain records on PII under management including its nature, purpose, consent and who has access.	Data Governance Access Controls
Be able to investigate a potential leak and report to relevant authorities the facts.	Logging Threat Detection
Be able to audit PII handling activities	Logging Data Governance

Personnel Security Measures

Requirement	Security Concept
Ensure supervision of those handling PII	Logging Contracts Assurance
Provide training on the handling of PII	Training & Consulting
Ensure employees maintain confidentiality	Training & Consulting

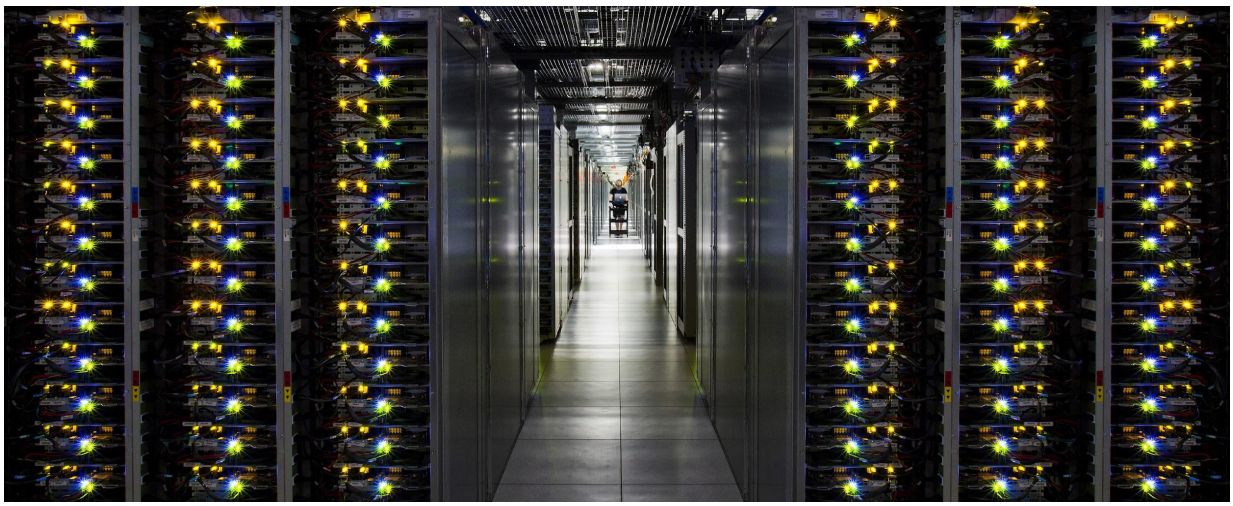
Physical Security Measures

Requirement	Security Concept
Implement management & restrictions on PII handling areas	Infrastructure Identity Data Governance Data Transformation
Put in barriers on PII handling areas such that access or viewing by unauthorized persons is not possible.	Infrastructure Data Transformation
Ensure prevention of physical theft of PII in storage & in transit	Infrastructure Data Transformation
Implement an irreversible method of PII data deletion	Data Deletion

Technical Security Measures

Requirement	Security Concept
Limit access to PII to only those who need access	Identity Access Controls Data Governance Data Transformation
Limit access to minimal PII required for each role	Access Controls

Ensure each PII handler can be identified and authenticated	Identity
Implement network access controls to limit potential access	Access Controls
Utilize security technologies to protect systems from unauthorized access	Endpoint CI/CD Pipeline Partners Solutions
Maintain systems at latest secure state by auto-updates	CI/CD Pipeline Managed Services
Analyze logs and detect threats in them	Threat Detection
Continuously evaluate systems for vulnerabilities	Risk Detection
Protect PII in storage and transport	Data Transformation

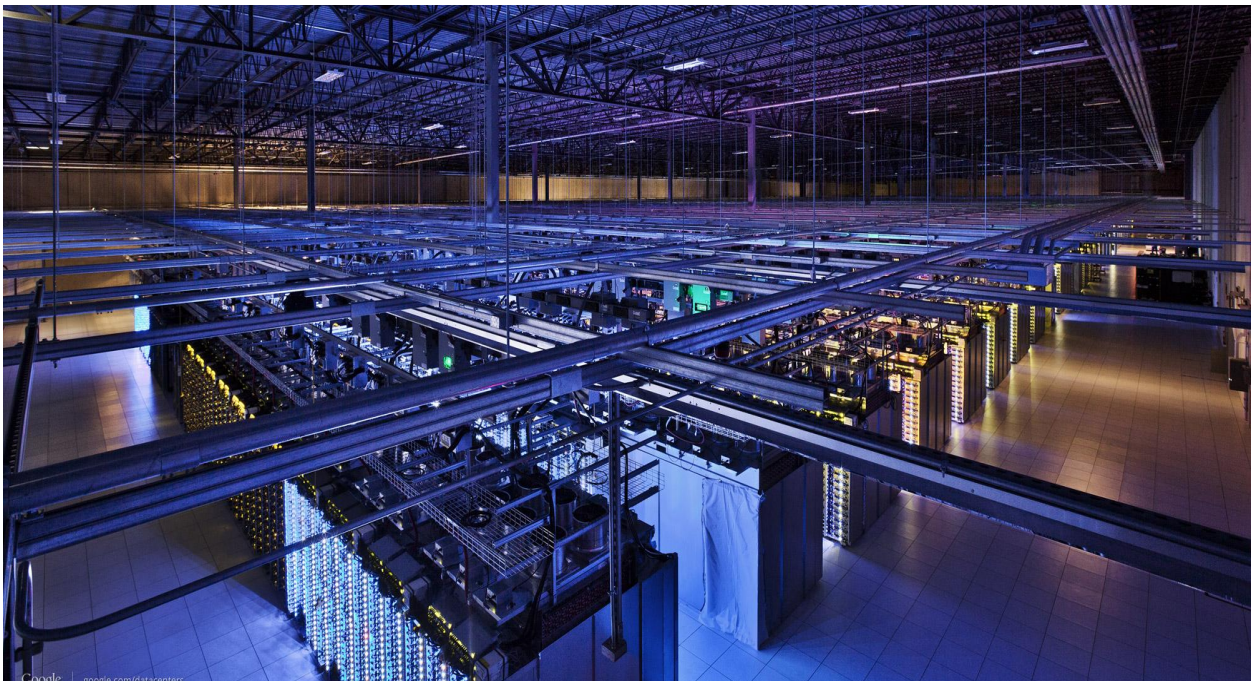


Google Cloud Security

Security in our infrastructure

Google operates global infrastructure designed to provide state-of-the-art security through the information processing lifecycle. This infrastructure is built to 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. Google Workspace and Google Cloud Platform run on this infrastructure.



We designed the security of our infrastructure in layers that build upon one another, from the physical security of data centers, to the security protections of our hardware and software, to the processes we use to support operational security. This layered protection creates a strong security foundation for everything we do. A detailed discussion of our Infrastructure Security can be found in our Google Infrastructure Security Design Whitepaper.

Security in our contracts

Our GCP and Google Workspace data processing terms clearly articulate our security & privacy commitments to customers. We have evolved these terms over the years based on feedback from our customers and regulators. Core to this is the understanding that any data that a customer puts into our systems will only be processed in accordance with the customer's instructions.

Google Cloud also commits to take security measures to ensure the confidentiality, integrity and availability of our systems. These are laid out in some detail in the agreement along with a further commitment that any changes we make to our security measures going forward will not degrade security. Our goal in stating this is to provide our customers continuous security improvement.

Security assurance

Google Cloud Platform and Google Workspace undergo several independent third party audits to test for data safety, privacy, and security. Our third party audit approach is designed to be comprehensive in order to provide assurances of our level of information security with regard to confidentiality, integrity and availability. Customers may use these third party audits to assess how Google's products can meet their compliance and data-processing needs. The relevant third-party certifications for our customers subject to the APPI are listed below. For more information see our Compliance Resource Center.

ISO/IEC 27001

ISO/IEC 27001 is a security standard that outlines and provides the requirements for an information security management system. The 27001 standard lays out a framework and checklist of controls that allow Google to ensure a comprehensive and continually improving model for security management. Google Cloud Platform and Google Workspace are certified as ISO 27001 compliant.

ISO/IEC 27018

ISO/IEC 27018 is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Google Workspace and Google Cloud Platform are certified as ISO/IEC compliant

Google Cloud Services

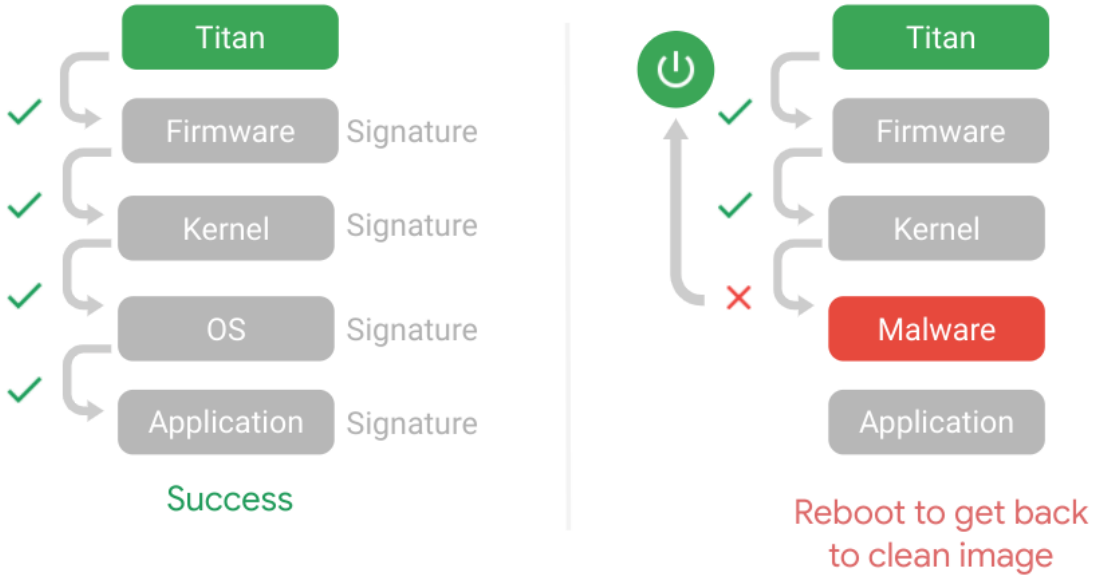
Endpoint

At Google, we have developed browser and OS technologies as part of the Chrome product family. These products have a very small attack surface in order to prevent common threats from taking hold on an endpoint. These solutions are available to our customers as Chrome Browser, Chrome OS and ChromeBooks centrally managed by Chrome Enterprise.

Chrome Browser is a minimal browser that automatically updates itself. It uses SafeBrowsing to check URLs against a database of known bad URLs and can warn or block sites that are

deemed high risk. Chrome tabs are sandboxed. Even I-frames in a tab are sandboxed. Chrome itself is isolated on the OS and has no access to other processes.

ChromeBooks run Chrome OS. Chrome OS is a read-only OS so malware has no way to infect or change the system files. ChromeBook's maintain 2 copies of Chrome OS; a working copy and a standby copy. Failure to boot the working copy will pull up the standby copy. This is beneficial for upgrades which are done on the standby copy and then it becomes the working copy on reboot. So not only do you get security but you get no downtime for upgrades. ChromeBooks have a Titan-C chip that will verify the firmware, OS and browser code. Should it detect a change it will not boot that version of the OS.



ChromeBooks encrypt data at rest but Chrome users tend not to have much data on their ChromeBooks since most of their data is in Google Cloud Services such as Google Workspace. Thus there is nothing to steal and even if ransomware could take hold, it would have nothing to ransom.

Chrome Enterprise Upgrade is a cloud based management system for having consistent administration over the Chrome OS environment. Software deployment, upgrades and Chrome settings can be configured for your entire fleet from one single console. Using Chrome Enterprise and ChromeBooks customers can easily meet and greatly exceed the PPC's expectations for security controls on the endpoint.

Identity

Identity is the backbone of access control and a core requirement in the PPC Guidelines. Google Cloud supports multiple identity providers as well as our own Cloud Identity.

Cloud Identity uses machine learning to detect unauthorized access and can even detect and block unauthorized intruders using the correct password.

Cloud Identity also supports the strongest forms of account protection including multiple 2FA options such as FIDO compliant security keys. Googlers use security keys on our own accounts to provide stronger identity protection and to prevent phishing attacks. We recommend our customers do the same.

Access Controls

Core to the PPC Guidelines is the rule of least privilege. PII handlers should only have the minimum access required to do their jobs.

In Google Cloud all services require authorization to use. Authorization is managed primarily in IAM. IAM allows you to grant roles to members such as users and groups. These roles are made up of fine grained permissions. Curated roles are provided and customers can create custom roles as needed.

Conditions can also be applied to roles. So for example a contractor that is only supposed to work 9 to 5 can have a condition added to the roles attached to them that limits their access to just 9 to 5.

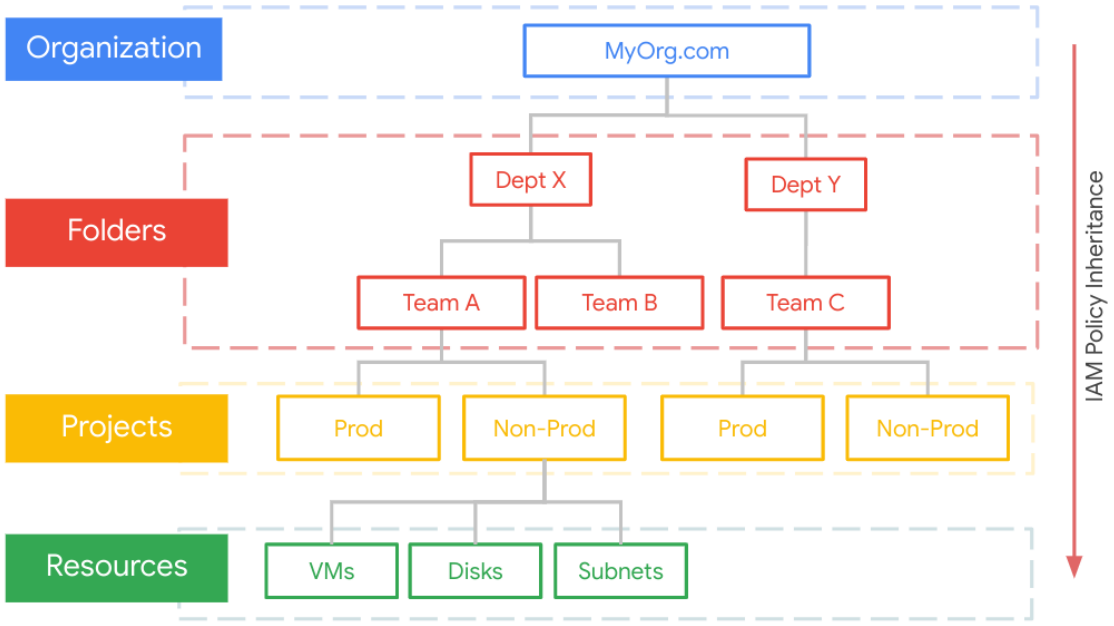
GCP has a resource manager where you can set up a folder tree to organize your projects. Access controls can be managed at any layer of the hierarchy and inherited down which is beneficial for good governance. PII specific folder(s) could be established and access controls applied there so as to have them consistent across all projects in that folder.

One of the biggest challenges for enterprise customers is not granting access but rather taking it away when it is not needed or excessive. IAM Recommender uses machine learning to see what permissions are being used and which are not and then makes recommendations to remove excess access. Policy analyzer can help you figure out who has access to what which is helpful in an audit situation.

Some Google Cloud services include service specific access controls that exceed what IAM can offer. For example in BigQuery you can set up limited views of data tables and you can

filter rows and columns meeting certain criteria. This can be very useful for minimizing the PII data analysts can see or filtering it out entirely.

In Google Workspace you can apply access controls on services based on the context of the user's identity and device. You can define at the file level who can read, comment or edit each individual file or folder.



Network Access Controls

One fundamental layer for access controls that is explicitly called out in the PPC guidelines is the network layer.

In a traditional network, including most cloud providers, firewall rules for network access control can only be applied at choke points. In Google Cloud firewall rules are much more flexible. They can be applied to a single VM, tagged assets, assets that share the same service account or a combination of factors.

Instead of applying the same rules to every project, common rules can be applied across projects at folder or organization level using hierarchical firewall policies.

The rules affecting an asset can be analyzed both from the command line as well as in the Network Intelligence Center.

It is also important to control access to service APIs. In Google Cloud you determine what APIs you want to turn on or off. Furthermore you can place a perimeter around the APIs of your

project using VPC Service Controls. VPC-SC can block data egress and place conditions on ingress.

Application Access Controls

Google Cloud provides the infrastructure for our customers to build their applications. The access controls inside those applications are part of the application logic the customer provides. However the access to those applications can leverage our context aware access system called BeyondCorp.

BeyondCorp allows you to define which users can access which applications under which conditions. Those conditions can be related to the situation (eg time), the device (eg corporate managed) and the user's identity and authentication (eg MFA).

These conditions can be used to apply different security to different risk scenarios. That can be critical to handling the APPI requirement for access controls as well as vendor supervision. For example many companies outsource payroll and may grant their payroll vendor access to an internal system with employee PII. BeyondCorp would allow a security check to be done on the vendor's PCs as a condition of granting them system access. That could include ensuring the PC has full disk encryption so as to protect any data on it should it be lost or stolen.

Logging

The PPC Guidelines speak to the need for access logs and the APPI law itself speaks to supervision which can be supported by access logs. Google Cloud offers extensive audit logging for services.

Network logs provide both network and security operations with in-depth network service telemetry. VPC Flow Logs can be used for network monitoring, forensics and real-time security analysis. Packet level capture can be done with Packet Mirroring for content analysis or to feed into a Network Intrusion Detection System. Firewall Rules Logging allows you to audit, verify, and analyze the effects of your firewall rules. NAT and DNS logs are also available for threat analysis.

Google Cloud Platform has Cloud Audit logging to log API activities including who did what, where and when. Data access logs can provide additional details at the data level and are especially useful for data management services. Google cloud does not handle customer data but if a customer specifically instructs us to access their data as part of support troubleshooting then that access is also logged and those logs can be made visible to customers via Access Transparency.

Cloud Operations provides a centralized tool for logging that can take in logs from a multitude of sources including custom logs sent from OS level agents, Fluentd, REST APIs, client libraries

or 3rd party applications. Logs can be analyzed in real time with Logs Viewer, or you can visualize and alert on your logs with logs-based metrics and Cloud Monitoring.

GCP provides a variety of log storage and retention options to meet both security & compliance requirements. System logs and data access logs are retained for 30 days by default or optionally up to 10 years. Admin logs are retained for 400 days in locked storage. Log data is immutable, encrypted at rest and monitored via Access Transparency.

Google Workspace includes extensive logging capabilities for everything from administration to users to services to devices. These logs can be fed to Cloud Operations in GCP for consolidated analysis.

Threat Detection

The PPC Guidelines recommend that logs be examined for threats. Security Command Center (SCC) in Google Cloud provides wing to wing risk management for Google Cloud customers. One component of SCC is threat detection. SCC will compare logs to known indicators of compromise as well as suspicious behaviors and surface alerts. Those alerts can be acted on automatically by triggering cloud functions. So for example a VM detected to be compromised could be imaged and isolated on the network all automatically.

Logs can also be exported from Google Cloud to Chronicle or 3rd party SIEMs like Splunk for further threat analysis or correlation with non-cloud logs to see the bigger enterprise threat picture. Chronicle continuously compares all your logs to a huge database of indicators of compromise (IOC) and surfaces any matches. Chronicle can search petabytes of logs in a single second.

Managed Services

The PPC guidelines require that systems holding PII be continuously maintained. Maintaining systems is complicated, costly and distracting for most customers. We recommend using managed services which we maintain for you. As you can see by the diagram below the more managed a service is the more you can focus on your data and leave the responsibility for the underlying infrastructure to Google.

Even in cases where compute services are required, we recommend taking advantage of the most managed form. For example a simple function can be run in cloud functions without any need for further management. Containers can be managed in GKE with node auto-upgrades which decreases the maintenance burden.

The team that manages the security of GKE is the same team that designed and wrote large parts of K8s identity, authorization and security policy code. The same team that led or contributed to the investigation, triage, patching, and notification of every serious K8s vulnerability since day 0. So you could not pick a better team to handle K8s management.

Secure CI/CD Pipeline

Human beings are not the only ones who access PII, application code does as well. So one way a threat actor might abuse PII is to alter the code that is loaded into an application handling PII. This is why having security as part of your continuous integration and delivery pipeline (CI/CD) is so important.

We recommend having a healthy code review process in place and have provided a guide to the public where we share our own practices and thoughts on this subject.

Google Cloud provides COS (Container Optimized OS) for nodes. Container-Optimized OS's small OS footprint minimizes security exposure while still containing essential built-in security features like a minimal read-only root file system, file system integrity check, locked-down firewall, and audit logging. Automatic updates patch security vulnerabilities for you and in a timely manner, further reducing your risk of compromise. Shielded GKE is built on hardware with a Titan chip that sets off a provenance validation sequence from host bootloader right up to the guest COS kernel in order to ensure end to end supply chain security.

Ensuring vulnerable containers are detected and addressed is key. Google Cloud can scan your containers added to Container Registry and report any defects.

Container policies can be set using Anthos Container Policy Controller. This is great for governance and can be used to ensure that a project team doesn't deploy containers with rights exceeded that allowed by company policy.

Using Binary Authorization it is possible to define signatures for passing various steps of the CI/CD pipeline and these signatures can be checked as a condition of deployment. This not only ensures all steps were passed but also keeps unauthorized code from being deployed to production.

Risk Detection

Application code can also be checked while running by Web Security Scanner which looks for common misconfigurations and vulnerabilities targeted by OWASP. Our premium offering even scans GCP looking for web applications and can surface shadow applications that may have been built without authorization.

Security Command Center checks your entire Google Cloud organization for misconfigurations and vulnerabilities and then maps those against a list of your cloud assets. In fact SCC will map risks and threats not only to assets but also to different compliance frameworks such as ISO 27001, PCI DSS and the CIS best practices for GCP. This allows you to meet your obligations to prevent and detect incidents affecting PII you place in GCP.

In Google Workspace you can get insights into security events and metrics that demonstrate your security effectiveness in a single, comprehensive dashboard called Security Center. From there you can Identify, triage, and take action on security and privacy issues such as deleting malicious emails across your organization and examining PII file sharing to spot and stop potential data exfiltration.

Data Governance

Under APPI the PPC has the right to audit PII records of a PII handler and making false reports to the PPC can result in fines. Individuals also have the right to request to know if a data handler has their PII, and if so what PII.

The reality is that keeping track of PII can be a challenge for organizations as different systems and functions in the company make different copies. Data Governance is key and Google Cloud can help with this. By data governance we mean:

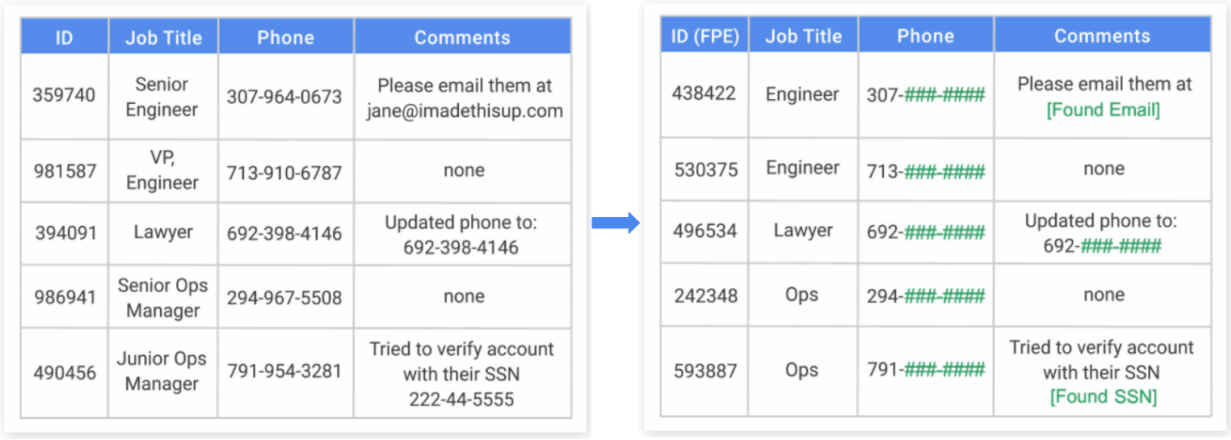
1. Discover PII
2. Label PII
3. Apply rules to PII

Data Catalog can use DLP API to find and apply metadata labels to your PII regardless of its location. Those labels can be used to apply rules so as to screen in/out certain data in processing jobs or data analytics systems.

Google Workspace also has DLP capabilities which administrators can configure to detect PII in files and take actions such as alerts or set restrictions on them such as to restrict outside sharing.

Data Transformation

PII can be hidden or removed at different handling points using transformation techniques. DLP API can remove PII by masking or redacting the PII. This applies not only to text but to images as well.



ID	Job Title	Phone	Comments
359740	Senior Engineer	307-964-0673	Please email them at jane@imadethisup.com
981587	VP, Engineer	713-910-6787	none
394091	Lawyer	692-398-4146	Updated phone to: 692-398-4146
986941	Senior Ops Manager	294-967-5508	none
490456	Junior Ops Manager	791-954-3281	Tried to verify account with their SSN 222-44-5555

ID (FPE)	Job Title	Phone	Comments
438422	Engineer	307-###-####	Please email them at [Found Email]
530375	Engineer	713-###-####	none
496534	Lawyer	692-###-####	Updated phone to: 692-###-####
242348	Ops	294-###-####	none
593887	Ops	791-###-####	Tried to verify account with their SSN [Found SSN]

There may be times when you both need to use PII but also need to hide the PII. There are two ways to do that. In the case of using it as a field in a data table you can use DLP API to replace

the PII with unique tokens (tokenization). If you only need to hide the data in storage or transit but would like to unhide it later then encryption makes more sense.

Google Cloud offers many encryption options. Key Management Service (KMS) can have cryptographic operations as a managed service that you access via an API. Under Cloud HSM you can use the same KMS front end knowing the backend is a FIPS-2 Level 3 certified HSM. In fact you can even use the KMS front end with an External Key Manager if you wish to separate duties.

Data Deletion

Once the purpose for handling PII expires or a customer withdraws their consent, the PII handlers are obliged to stop using the data and make efforts to delete the data. APPI and the PPC acknowledge that there may be legal reasons to keep using data that differ from the purpose of its initial collection. It is also acknowledged that deletion may take time for systems that have multiple components and backups.

Customer data in Google Cloud belongs to the customer and the customer can select to delete it at any time. Doing so makes the data immediately unavailable and kicks off wipe out procedures that extend to the various service components involved. These wipe out procedures can take up to 180 days. These procedures once complete provide for irreversible destruction of the data. Details are in the following whitepapers for GCP & Google Workspace.

Training & Consultation

The PPC lists training as a key requirement in their Guidelines. The focus there is on the PII handling processes but when those processes use a technology like Google Cloud then training on that technology is advisable as well. Google Cloud has a wide range of training and consultation support for our customers such as:

- Pre-sales staff to walk you thru our services and help choose the right ones
- Training and education staff to train your team
- Cloud on Air and Youtube Videos
- Online training partners so you can train on your own schedule
- Certification program to level set required skills
- Online documentation in multiple languages
- Qwiklabs to practice using our services
- Post-sales consulting services

- System integrator partnerships to build and manage solutions at scale
- A lively online community of blogs, articles, videos and chat rooms to share ideas and derive inspiration

Partner Solutions

Google Cloud has partnered with a wide variety of security solutions companies to make their solutions available to our customers either via the Google Cloud Marketplace or other partnership agreements. In addition we provide basic compute services that can support most security solutions regardless of whether they are a Google Cloud partner or not.

Our sales team is happy to hear your security requirements and provide consultation on which partner solutions best match your use cases.

Conclusion

Google cloud's world class infrastructure is the perfect foundation upon which to build your PII solutions. Our commitment to security and privacy is backed up by our contract terms and verified by our auditors. We offer a wide range of unique products and services to help customers meet and exceed the recommendations in the APPI guidelines and protect their customer's PII.