Google Cloud and Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)

Cloud Whitepaper

February 2018

Google Cloud

0101101 01101001
001101 11010101
101101 101001
00110 101
10 001
101
001

Table of Contents

Disclaimer 3

Introduction 3

1. The Canada PIPEDA 4
    1.1 Google Cloud and the Canada PIPEDA 5

2 . Security and Trusted Infrastructure 7
    2.1 Google data centre infrastructure redundancy 7
    2.2 Google data centre security 8
    2.3 Data in transit 10
    2.3.1 Between a customer and Google 10
    2.3.2 Within Google data centres 10
    2.4 Data at rest 10

3. Data Protection and Privacy 13
    3.1 Identity and authentication 13

4. Conclusion 15

Google Cloud

Disclaimer

This paper is for **informational** purposes only. Google does not intend the information in this paper to constitute legal advice. Each customer is responsible for independently evaluating its own particular use of Google services to support its legal compliance obligations.

Introduction

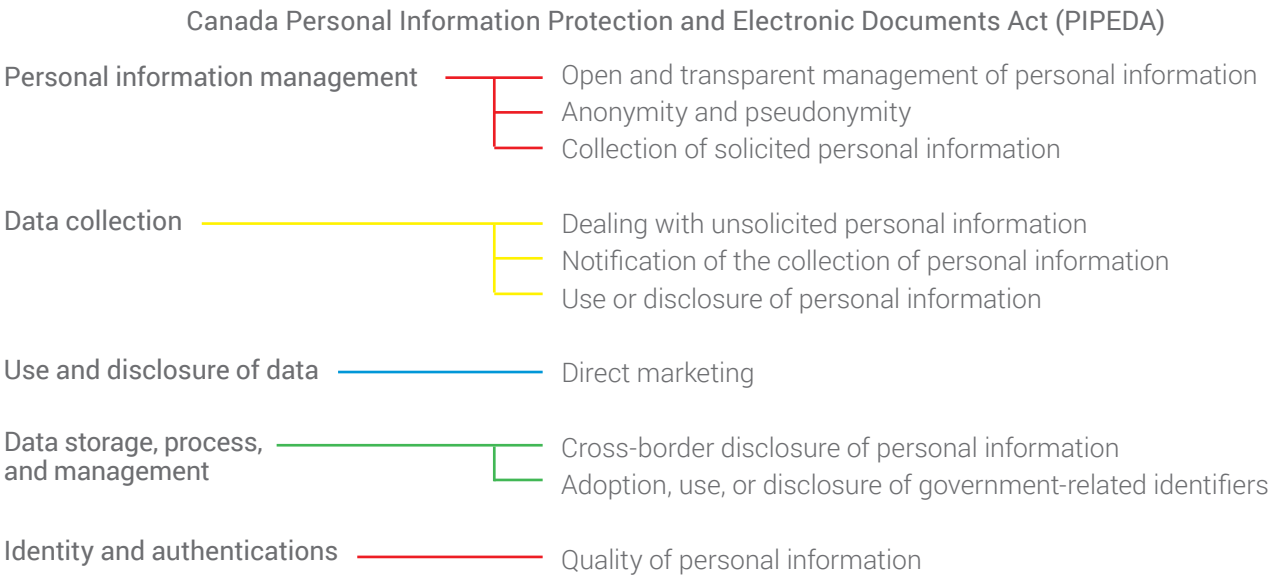
In this paper Google Cloud refers to the Google Cloud Platform and G Suite products. This paper is intended to help customers of Google Cloud understand Google's security and privacy features. Specifically, this paper explains how information is stored, processed, secured, accessed, and maintained in Google Cloud.

This paper has four sections:

- Section 1: The Canada PIPEDA
- Section 2: Security and Trusted Infrastructure
  This section provides technical information on how Google Cloud can help customers keep data secure.
- Section 3: Data Protection and Security
  This section provides technical information on how Google Cloud can help customers with identity protection and security.
- Section 4: Conclusion

Section 1: The Canada PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the Canadian federal privacy law for private-sector organizations to regulate the way private-sector organizations handle the personal information in a commercial activity. There are 10 PIPEDA principles.



These PIPEDA principles give individuals the right to know why their personal information is being collected, how their personal information will be used, and to whom their personal information will be disclosed, and to have the ability to ask for access to, or correction of, their personal information. More details on the PIPEDA principles can be found on the Office of the Privacy Commissioner of Canada website. Customers of cloud computing providers are responsible for ensuring they comply with their obligations under PIPEDA.

Section 1.1: Google Cloud and the Canada PIPEDA

Google Cloud provides security and privacy capabilities and contractual commitments created to help customers when considering whether Google's products are suitable for them. Our customers may execute our Data Processing Amendment for G Suite customers and Data Processing and Security Terms for Google Cloud Platform customers, which articulate our privacy and security written commitment to customers.

Google undergoes several 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. For more information on Google certifications, audits, and assessments, see the Compliance section of Google Cloud Trust & Security.

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

Google Cloud Platform

- SSAE 16 / ISAE 3402 Type II:
  SOC 1
  SOC 2
  SOC 3 public audit report

- **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.

G Suite is an SaaS public cloud-based offering from Google. G Suite is a set of intelligent apps including Gmail, Docs, Drive, Calendar, G+, Sites, and Hangouts. G Suite has annual audits for the following standards:

G Suite

- SSAE 16 / ISAE 3402 Type II:
  SOC 1
  SOC 2
  SOC 3 public audit report

- 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 G Suite. View the G Suite 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 G Suite 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 G Suite ISO 27018 Certificate.

Section 2: Security and Trusted Infrastructure

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

Section 2.1: Google data centre infrastructure redundancy

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

Certain Cloud Platform resources are hosted in multiple regions globally, while other resources, including Cloud Compute Engine Virtual Machine Instances, persistent disks, Cloud Storage buckets, Cloud App Engine applications, Cloud Bigtable, Cloud Dataproc, Cloud 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. The network could have an outage; the customer's latest application push might introduce a critical bug; or, in rare cases, the customer might even have to contend with a natural disaster. When things go awry, it's important to have a robust, targeted, and well-tested disaster recovery plan. Google Cloud Platform provides many of the facilities customers need to implement such a plan, such as redundancy, scalability, compliance, and security. The Disaster Recovery Cookbook provides some scenarios to show how Google Cloud Platform can help.

In G Suite, Google 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 dependant 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 G Suite 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. A full list of Google G Suite data centres can be found on the G Suite locations map.

Section 2.2: 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, seven 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 G Suite Data Processing Amendment, Appendix 2: Security Measures.

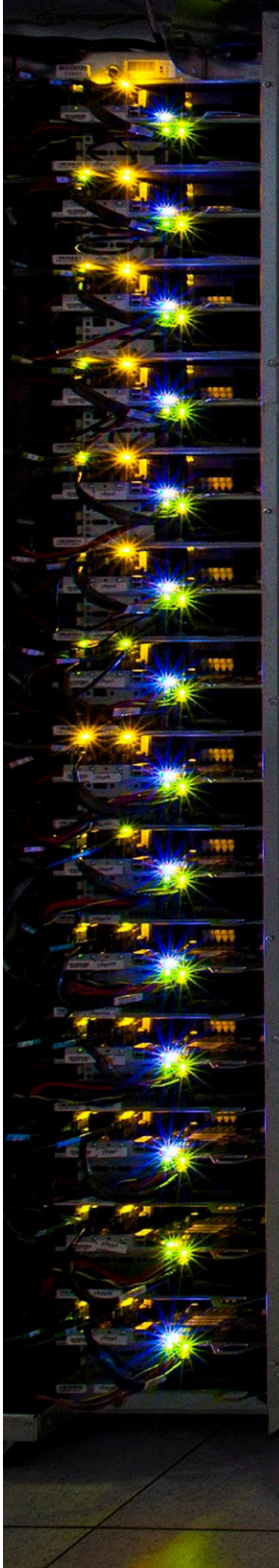
Google data centres have been designed to be robust and fault-tolerant in the following ways:

Power: To support Google's continuous 24-hours-a-day, seven-days-a-week operations, a Google data centre's electrical power systems are designed to be redundant. A primary and emergency power source, each with equal capacity, is provided for every critical component in the data centre. Upon failure of the primary electrical power source, an uninterruptible power supply (UPS) provides power until the backup generators can take over. The diesel-engine backup generators are capable of providing enough emergency electrical power to run the data centre at full capacity. Examples of events that can cause failures include utility brownouts, blackouts, over-voltage, under-voltage, or out-of-tolerance frequency conditions.

Climate and temperature: Air cooling is required to maintain a constant operating temperature for servers and other computing hardware. Cooling prevents overheating and reduces the possibility of service outage. Computer-room air conditioning units are powered by both primary and emergency electrical systems. For more information on cooling control, see Google data centre temperature control efficiency.

Fire detection and suppression: Automatic fire detection and suppression equipment helps prevent damage to computing hardware. The fire detection systems utilize heat, fire, and smoke detectors located in the data centre ceilings and underneath the raised floor. In the event of fire or smoke, the detection system triggers audible and visible alarms in the affected zone, at the security operations console, and at the remote monitoring desk. In addition to automatic fire suppression systems, manually operated fire extinguishers are also located throughout the data centre facilities. Google data centre technicians receive training on fire prevention and incipient fire extinguishment, including the use of fire extinguishers.

For more information about the Google data centre infrastructure, see Data Processing and Security Terms, Appendix 2: Security Measures.



Section 2.3: 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.

Section 2.3.1: 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.

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.

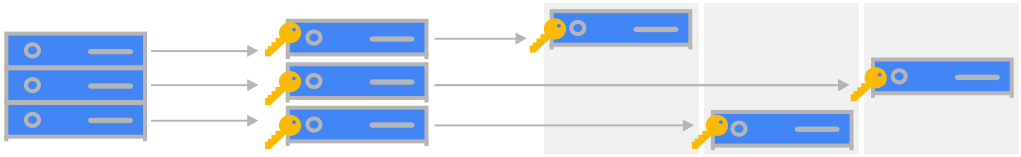
Section 2.3.2: Within Google data centres

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 that goes over the WAN between data centres, without requiring any explicit configuration from the service.

Section 2.4: Data at rest

Google Cloud encrypts customer content stored at rest, without any action required from the customer, using one or more encryption mechanisms. Data at rest is encrypted at the storage level using either AES256 or AES128.

To understand how specifically Google Cloud Storage encryption works, it's important to understand how Google stores customer data. The diagram below shows how Google protects data at rest using encryption. The encryption process begins when data is uploaded to Google Cloud by a customer. Data is broken into subfile chunks for storage; each chunk can be up to several GB in size. Each chunk is encrypted at the storage level with a unique data encryption key, which uses AES128 or higher: Two chunks will not have the same encryption key, even if they are part of the same Google Cloud Storage object, owned by the same customer, or stored on the same Google machine. If a chunk of data is updated, it is encrypted with a new key, rather than by reusing the existing key.



Data is uploaded to Google

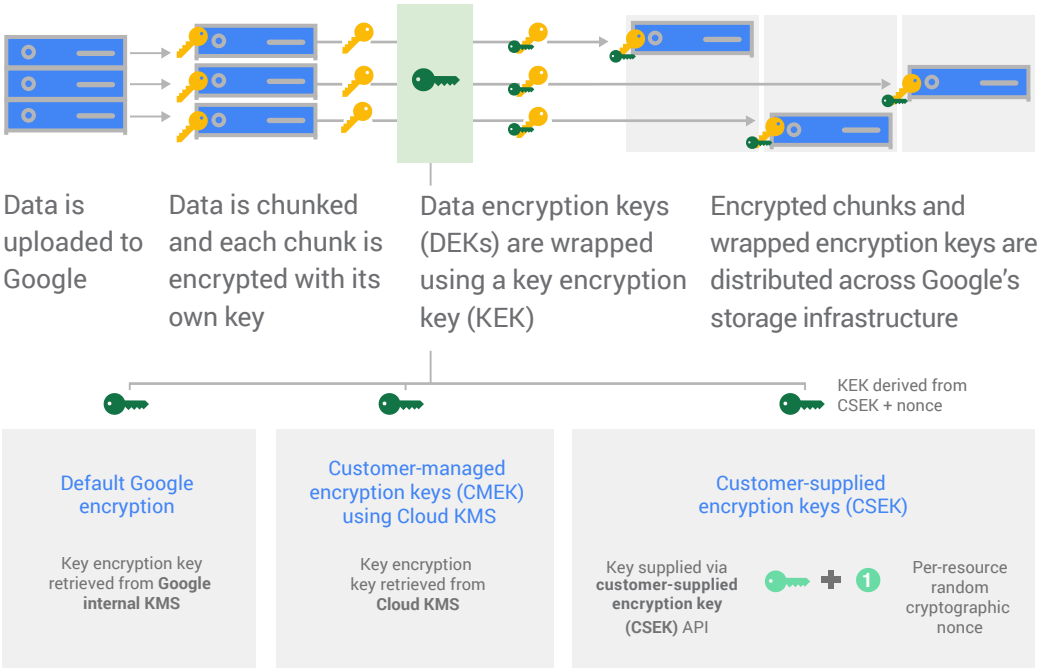
Data is chunked and each chunk is encrypted with its own key

Chunks are distributed across Google's storage infrastructure

Due to the high volume of keys at Google, and the need for low latency and high availability, data encryption keys are stored near the data that they encrypt. The data encryption keys are themselves encrypted with a key encryption key which uses AES128 or higher.

Access control lists (ACLs) in Google's internal Key Management Service ensure that each chunk can be decrypted only by Google services operating under authorized roles, which are granted access at that point in time. This prevents access to the data without authorization, bolstering both data security and privacy. If a malicious individual wanted to access customer data, that individual would need to: (1) know and be able to access all storage chunks corresponding to the data they want, (2) know and be able to access the encryption keys corresponding to the chunks, and (3) have authorized role credentials.

In Google Cloud Platform, customers can choose one of the key management solutions as shown in the diagram below to manage the key 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.

For more information on encryption and key management, see the G Suite Encryption, Application Layer Transport Security, Encryption at Rest in Google Cloud Platform, and Encryption in Transit in Google Cloud whitepapers.

Section 3: Data Protection and Security

ISO 27018, Cloud Privacy, is an international standard of practice for protection of personally identifiable information (PII) in public cloud services. For more information on the complete list of services that are ISO 27018 certified, see the Compliance section of Google Cloud Trust & Security.

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

Section 3.1: Identity and authentication

Google Cloud Platform and G Suite 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 Platform 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 G Suite administrator, you can manage all of your users and settings through the G Suite Admin Console. By default, all new users are assigned a G Suite license. If you have a subset of developers who don't require G Suite 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 (SSO): 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 G Suite accounts. This guide applies to both Cloud Platform and G Suite, 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, Google 2-Step Verification adds an extra layer of security to a customer account by requiring the user to enter a verification code or use 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, the Google Cloud Platform product, Google 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 policies or Access Control Lists. This access management can help the customer to address the privacy of the individual's data and ensure that each individual only has access to their own data.

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

Section 4: Conclusion

This document describes how information is stored, processed, maintained, secured, and accessed in Google Cloud using Google Cloud products. This information can help customers when considering whether Google's products are suitable for them. In particular it explains how Google approaches security and privacy. A more in-depth understanding of how Google Cloud products work can be found in references cited within this document.

Google Cloud security

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

Google Cloud compliance

For information on Google Cloud compliance and compliance certifications, see the Compliance section of Google Cloud Trust & Security.