Google Cloud Whitepaper
December 2019

Google Cloud & the California Consumer Privacy Act

Google Cloud

Introduction

What is the California Consumer Privacy Act (CCPA)?

The California Consumer Privacy Act (CCPA)[1] is a data privacy law that provides California consumers with a number of privacy protections, including right to access, delete, and opt-out of the "sale"[2] of their personal information. Starting January 1, 2020, businesses that collect California residents' personal information and meet certain thresholds (e.g., revenue, volume of data processing) will need to comply with these obligations.

Google is committed to helping our customers meet their CCPA obligations by offering convenient tools and building robust privacy and security protections into our services and contracts.

You can find more information about your responsibilities as a business under the CCPA on the California Office of the Attorney General's website.[3]

This paper is intended to be for informational purposes only. You should seek independent legal advice relating to your status and obligations under the CCPA, as only a lawyer can provide you with tailored legal advice for your situation. Nothing in this whitepaper is intended to provide you with or should be used as a substitute for legal advice.

---

1 Page 2, California Legislative Information

2 CCPA *1798.140. (t) (1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.*

3 Page 2, State of California Department of Justice

Who must comply with the CCPA?

A range of entities that do business in California, collect personal information of California consumers, and meet certain thresholds (e.g., revenue, volume of data processing) qualify as "businesses" and are therefore subject to the CCPA's requirements. In short, if you are a business that collects personal information about California consumers, then you may be subject to the CCPA and should consult the statute, regulations, and legal counsel to determine your obligations.

Where should you start?

As a current or future customer of Google Cloud, there are many ways for you to begin preparing for the CCPA. Consider these tips:

1. Familiarize yourself with the text of the CCPA and its regulations, particularly the sections which may impose new obligations on your business.
2. 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,[4] to help identify and classify data.
3. Review the current controls, policies, and processes that govern your use of personal information to assess whether they meet the requirements of CCPA, and build a plan to address any gaps.
4. Consider the best process for your business to accept and verify a California consumer request.
5. Review our G Suite and Google Cloud Platform third-party audit and certification materials, as well as our guidance documents and mappings, to see how they may help with this exercise. You can learn more in our Compliance resource center.[5]
6. Consider how you can leverage existing data protection features on Google Cloud to support your CCPA compliance.
7. Monitor the latest regulatory guidance as it becomes available, and consult a lawyer to obtain legal advice tailored to your business's circumstances.

4 Page 3, Cloud Data Loss Prevention
5 Page 3, Google Cloud Compliance resource center

CCPA: What we're doing

At Google Cloud, the security and privacy of customer data[6] is our highest priority. We are committed to supporting your CCPA journey by:

Providing tools and support to help you to address CCPA requirements applicable to you with respect to your consumers' rights.

You can use G Suite and Google Cloud Platform's administrative consoles and services to help access, export or delete data that they and their users put into our systems. This functionality can be used to help Customers fulfill their obligations to respond to requests from consumers who exercise their rights under CCPA.

Offering security products and features that can help you to protect customer personal data.

Google operates global infrastructure designed to provide state-of-the-art security through the entire 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. G Suite 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 Overview whitepaper.[7]

Continuing to monitor the regulatory landscape, and evolve as needed.

Our cross-functional teams of privacy advocates, user experience researchers, and privacy legal experts regularly engage with customers, industry stakeholders, and supervisory authorities to shape our G Suite and Google Cloud Platform services in a manner that helps customers meet their compliance needs. As the regulatory landscape shifts, we evolve to support our customers' changing compliance needs.

6 As defined in the Google Cloud customer agreements

7 Page 4, Google Infrastructure Security Design Overview whitepaper

- ***Providing you with the documentation and resources to assist you in your privacy assessment of our services.***

  We will support your efforts by providing you with detailed documentation and resources, such as our Google Security whitepaper,[8] G Suite data protection implementation guide,[9] and Compliance resource center.[10]

- ***Addressing our G Suite and Google Cloud Platform customers' data protection related inquiries.***

  For more information, refer to Google's Businesses and Data website.[11] We also encourage you to visit our help center and articles.

Product Offerings to Help Support CCPA Compliance

Google Cloud customers can leverage our product features and configurations to protect their customer data and assist with their CCPA readiness.

Google Cloud Platform (GCP)

Data Governance

Cloud Data Loss Prevention (DLP)[12] helps customers to discover, classify, and de-identify their data, such as credit card numbers, social security numbers, healthcare information, etc. DLP provides several techniques like pseudonymisation, tokenization, bucketing, date-shifting, and more, which can help you de-risk your structured and unstructured data. For more details on these techniques, refer to our blog post: Take charge of your data: using Cloud DLP to de-identify and obfuscate sensitive information.[13]

When customers use DLP to classify data, they can attach the data class, and other business metadata (such as owner, quality, lineage) to the actual data via tagging. Data Catalog[14] is a metadata management service allowing such tagging. Data Catalog simplifies data discovery, allowing search across your entire data warehouse. The search facilities from Data Catalog are enterprise access control enabled - meaning users cannot discover data they do not have permission to - all managed by Cloud IAM controls.[15] To learn more, read our whitepaper, Principles and best practices for data governance in the cloud.[16]

---

8 Page 5, Google Security whitepaper
9 Page 5, G Suite Data Protection Implementation Guide
10 Page 5, Google Cloud Compliance resource center
11 Page 5, Google Businesses and Data
12 Page 5, Cloud Data Loss Prevention
13 Page 5, Take charge of your data: using Cloud DLP to de-identify and obfuscate sensitive information
14 Page 5, Data Catalog
15 Page 5, Cloud Identity and Access Management (IAM)
16 Page 5, Principles and best practices for data governance in the cloud

Access Control

With data stored in the Cloud, Identity and Access Management (IAM)[17] helps customers to define fine-grained access control and visibility, apply identity policies, and precisely control access to GCP-hosted data. Similarly, enterprises storing data in the Cloud seek visibility into data access. Cloud Audit Logs[18] help security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events.

For services integrated with Access Transparency,[19] Google uses a tool to validate that the business justification presented for access is valid, and log the justification to Access Transparency Logs. Access Transparency logs are generated when Google administrators access data uploaded by you into an Access Transparency supported service (for example, viewing one of the labels on your GCP Compute Engine instance).[20] Customers can monitor the logs[21] by using the Stackdriver APIs or using Cloud Functions in GCP. Learn more about Access Transparency for Google Cloud Platform.[22]

Export

All GCP storage and database solutions offer the capability to export your data. If you choose to remove your data completely from GCP, you can take a copy of your data from the service, and it can be removed from Google's systems using the deletion capability described below.

GCP storage and database solutions offer fine-grained IAM permissions[23] to control which employees can export data. In addition, GCP implements limitations,[24] such as preventing the export of BigQuery tables to raw files or Google Sheets, inability to export more than 1GB of table data, inability to export data from multiple tables all at once, and others.

Deletion

When our customers delete data in GCP, we immediately start the process of removing it from the product and our systems. First, we aim to immediately remove it from view. We then begin a process designed to safely and completely delete the data from our storage systems. Each Google storage system from which data gets deleted has its own detailed process for safe and complete deletion. This might involve repeated passes through the system to confirm all data has been deleted. Our services also use encrypted backup storage as another layer of protection to help recover from potential disasters. Data can remain on these systems for up to 6 months.

17 Page 6, Cloud Identity and Access Management (IAM)
18 Page 6, Cloud Audit Logs
19 Page 6, Google Cloud Access Transparency
20 Page 6, There are exceptions which are detailed in the Access Transparency documentation.
21 Page 6, Stackdriver Monitoring documentation
22 Page 6, Google Cloud Access Transparency
23 Page 6, Exploring table data
24 Page 6, Exploring table data

Encryption

GCP enables Encryption in transit[25] by default to encrypt requests before transmission and protect the raw data using the Transport Layer Security (TLS) protocol. Once data are transferred for storage at GCP's data centers, GCP applies Encryption at Rest[26] by default.[27] To gain more control over how data is encrypted at rest, GCP customers can use Cloud Key Management Service (KMS)[28] to generate, use, rotate, and destroy customer managed encryption keys (CMEK). Customers with stringent requirements for key storage can use Cloud Hardware Security Module (HSM),[29] allowing customers to host encryption keys and perform cryptographic operations in FIPS 140-2 Level 3 certified HSMs. For customers who require their keys to be stored outside GCP we also offer an External Key Management product[30] for GCE and BigQuery.

Security Management

Forseti Security[31] is a collection of community-driven, open-source tools that helps customers to manage security policies, stay on top of human errors, and continue to enforce security policies at scale. Config Validator,[32] for example, helps customers to enforce constraints that validate whether deployments can be provisioned enabling developers to operate within safe guardrails. Administrators can publish Config Validator's results to Cloud Security Command Center (CSCC)[33] to keep track of configuration violations over time.

G Suite

Data Governance

Data Loss Prevention (DLP)[34] for Gmail[35] and Drive[36] adds another layer of protection to prevent sensitive or private information from leaking outside of an organization. DLP is a tool that enables rules to prevent people from accidentally sending confidential data and is one step in a long term investment to bring rule based security across G Suite.

The reports and logs available in the Google Admin Console make it easy for a super administrator to monitor account activity,[37] examine potential security risks, measure user collaboration, track access, analyze administrator activity, and much more. Notifications are configurable to receive activity alerts, such as: suspicious login attempts, user suspended by an administrator, new user added, suspended user made active, user deleted, user's password changed by an administrator, user granted admin privileges, and user's admin privileges revoked.

---

25 Page 7, Encryption in Transit in Google Cloud
26 Page 7, Encryption at rest
27 Page 7, For further details, please refer to the Encryption at Rest White Paper.
28 Page 7, Cloud Key Management Service
29 Page 7, Cloud HSM
30 Page 7, Advancing control and visibility in the cloud
31 Page 7, Forseti Security
32 Page 7, Config Validator | Setup & User Guide
33 Page 7, Config Validator | Setup & User Guide
34 Available to G Suite Enterprise, Drive Enterprise and G Suite Enterprise for Education customers only.
35 Page 7, Google Data Loss Prevention for work
36 Page 7, Scan and protect Drive files using DLP rules
37 Page 7, G Suite Data Protection Implementation Guide

Access Control

For services integrated with Access Transparency,[38] Google uses a tool to validate that the business justification presented for access is valid, and logs the justification. Access Transparency for G Suite[39] enables customers to get more visibility into actions taken by Google staff related to your data. You can view the reason for each access, including references to specific support tickets where relevant, which may help you support your audit requirements.

Export

The Data Export tool[40] available in your G Suite Admin Console enables super administrators to export all core services data for the entire organization.[41] Please review the help center article (Data Export tool)[42] for details on what is included and what is excluded in the export. We also provide the ability for your users to directly download their data[43] on an individual level.

Deletion

When our customers delete data in G Suite, we immediately start the process of removing it from the product and our systems. First, we aim to immediately remove it from view. We then begin a process designed to safely and completely delete the data from our storage systems. Each Google storage system from which data gets deleted has its own detailed process for safe and complete deletion. This might involve repeated passes through the system to confirm all data has been deleted. Our services also use encrypted backup storage as another layer of protection to help recover from potential disasters. Data can remain on these systems for up to 6 months.

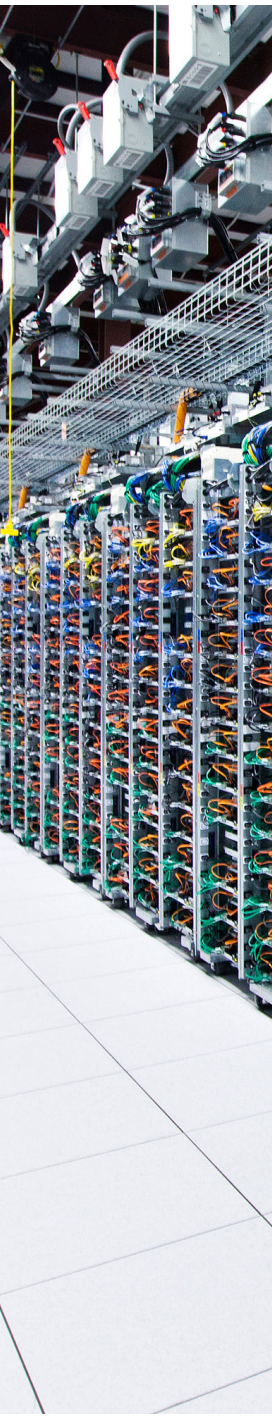
eDiscovery allows organizations to respond in case of lawsuits and other legal matters. Google Vault[44] is the eDiscovery solution for G Suite that lets customers retain, search and export their data. If you are required to preserve data for a period of time, you can use Vault to retain it, even if users delete messages and files, and then empty their trash. You can customize retention rules that control how long specific types of data are retained. You can create as many custom rules as your organization needs. Learn more[45] about how Vault manages retention and holds.

Encryption

G Suite customers' data is encrypted[46] when it's on a disk, stored on backup media, moving over the Internet, or traveling between data centers.Providing cryptographic solutions that address customers' data security concerns is our commitment. Encryption is an important piece of the G Suite security strategy, helping to protect your emails, chats, Google Drive files, and other data.

---

38 Page 8, Google Cloud Access Transparency
39 Page 8, Use Access Transparency to report Google access
40 Page 8, Export your organization's data
41 Customers cannot partially export certain types of data, and cannot export data for a subset of users
42 Page 8, Export your organization's data
43 Page 8, Download your data
44 Page 8, Vault
45 Page 8, How retention works
46 Page 9, How Google Uses Encryption to Protect Your Data



Google's processing of customer data

At Google Cloud we've set a high bar for what it means to host, serve, and protect customer data. Security and data protection are at the core of how we design and build our products. We start from the fundamental premise that Google Cloud customers own their data and control how it is used. Our Google Cloud Trust Principles[47] summarize our commitment to protecting the privacy of data stored by customers in Google Cloud.

Additionally, all Google employees are required to sign a confidentiality agreement and complete mandatory confidentiality and privacy trainings, as well as our Code of Conduct training. Google's Code of Conduct[48] specifically addresses responsibilities and expected behavior with respect to the protection of information. In addition, we've designed our systems to limit the number of employees that have access to customer data and to actively monitor the activities of those employees. Google follows a formal process to grant or revoke employee access to Google resources, and access is automatically removed for departing employees.

Access authorization is enforced at all relevant layers of the system. Approvals are managed by workflow tools and logged. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud products. Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams actively monitor access patterns and investigate unusual events.

For further information on employee onboarding and security and privacy training, please refer to our Security and Compliance whitepaper.[49]

Finally, Google Group companies directly conduct the majority of data processing activities required to provide the G Suite and Google Cloud Platform services. However, we do engage some third-party vendors to assist in supporting these services. Each vendor goes through a rigorous selection process to determine it has the required technical expertise and can deliver the appropriate level of security and privacy. We make information available about Google group subprocessors supporting G Suite and Google Cloud Platform services, as well as third-party subprocessors involved in those services, and we include commitments relating to subprocessors in our current data processing agreements.

47 Page 9, Google Cloud Privacy
48 Page 9, Google Code of Conduct
49 Page 9, Google Cloud Security and Compliance whitepaper

Independent verification of our control framework

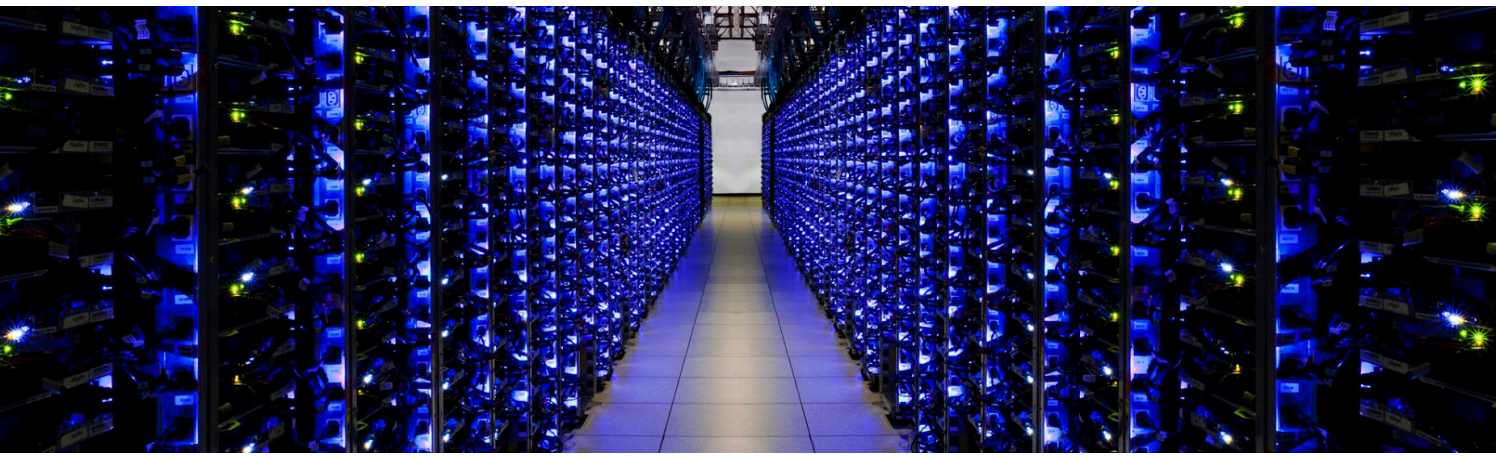
Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Some of the key international standards we are audited against are:

- ISO 27001 (Information Security Management)
- ISO 27017 (Cloud Security)
- ISO 27018 (Cloud Privacy)
- SOC 2 and SOC 3 reports

Google also participates in sector and country-specific frameworks, such as FedRAMP59 (US government), BSI C5 (Germany), MTCS (Singapore), and many others. We also provide resource documents and mappings for certain frameworks where formal certifications or attestations may not be required or applied.

Conclusion

We understand that compliance with the CCPA and other privacy regulations is a top priority for our customers. The CCPA aims to provide California consumers with a number of privacy protections, and impacts the way we all do business. We're sure you have many questions, and we're here to help. For more information, please visit our Compliance resource center.[50]



50 Page 10, Google Cloud Compliance resource center

Appendix: URLs

Page 2

1. California Legislative Information: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
3. State of California Department of Justice: https://oag.ca.gov/privacy/ccpa

Page 3

4. Cloud Data Loss Prevention: https://cloud.google.com/dlp/
5. Google Cloud Compliance resource center: https://cloud.google.com/security/compliance/

Page 4

7. Google Infrastructure Security Design Overview whitepaper: https://cloud.google.com/security/infrastructure/design/?utm_medium=et&utm_source=google.com%2Fcloud&utm_campaign=gdpr&utm_content=commitments_to_the_gdpr

Page 5

8. Google Security whitepaper: https://cloud.google.com/security/overview/whitepaper
9. G Suite Data Protection Implementation Guide: https://cloud.google.com/files/gsuitedataprotectionimplementationguide_012019.pdf
10. Google Cloud Compliance resource center: https://cloud.google.com/security/compliance/
11. Google Businesses and Data: https://privacy.google.com/businesses/?uri=CELEX:31995L0046&from=EN?utm_medium=et&utm_source=google.com%2Fcloud&utm_campaign=gdpr&utm_content=gdpr_faqs
12. Cloud Data Loss Prevention: https://cloud.google.com/dlp/
13. Take charge of your data: using Cloud DLP to de-identify and obfuscate sensitive information: https://cloud.google.com/blog/products/identity-security/taking-charge-of-your-data-using-cloud-dlp-to-de-identify-and-obfuscate-sensitive-information
14. Data Catalog: https://cloud.google.com/data-catalog/
15. Cloud Identity and Access Management (IAM): https://cloud.google.com/iam/
16. Principles and best practices for data governance in the cloud: https://services.google.com/fh/files/misc/principles_best_practices_for_data-governance.pdf

Appendix: URLs

Page 6

17. Cloud Identity and Access Management (IAM): https://cloud.google.com/iam/
18. Cloud Audit Logs: https://cloud.google.com/audit-logs/
19. Google Cloud Access Transparency: https://cloud.google.com/logging/docs/audit/access-transparency-overview
20. Access Transparency documentation: https://cloud.google.com/logging/docs/audit/access-transparency-overview
21. Stackdriver Monitoring documentation: https://cloud.google.com/monitoring/docs/
22. Google Cloud Access Transparency: https://cloud.google.com/logging/docs/audit/access-transparency-overview
23. Exporting table data: https://cloud.google.com/bigquery/docs/exporting-data
24. Exporting table data: https://cloud.google.com/bigquery/docs/exporting-data

Page 7

25. Encryption in Transit in Google Cloud: https://cloud.google.com/security/encryption-in-transit/
26. Encryption at rest: https://cloud.google.com/security/encryption-at-rest/
27. Encryption at rest whitepaper: https://cloud.google.com/security/encryption-at-rest/default-encryption/
28. Cloud Key Management Service: https://cloud.google.com/kms/
29. Cloud HSM: https://cloud.google.com/hsm/
30. Advancing control and visibility in the cloud: https://cloud.google.com/blog/products/identity-security/new-security-tools-for-google-cloud-and-g-suite
31. Forseti Security: https://forsetisecurity.org
32. Config Validator | Setup & User Guide: https://github.com/forseti-security/policy-library/blob/master/docs/user_guide.md
33. Config Validator | Setup & User Guide: https://github.com/forseti-security/policy-library/blob/master/docs/user_guide.md
35. Google Data Loss Prevention for work: https://storage.googleapis.com/gfw-touched-accounts-pdfs/Gmail_dlp_whitepaper.pdf
36. Scan and protect Drive files using DLP rules: https://support.google.com/a/answer/6321530?hl=en
37. G Suite Data Protection Implementation Guide: https://services.google.com/fh/files/misc/gsuitedataprotectionimplementationguide_092018.pdf

Appendix: URLs

Page 8

38. Google Cloud Access Transparency: https://cloud.google.com/logging/docs/audit/access-transparency-overview
39. Use Access Transparency to report Google access: https://support.google.com/a/answer/9230474
40. Export your organization's data: https://support.google.com/a/answer/100458?hl=en
42. Export your organization's data: https://support.google.com/a/answer/100458?hl=en
43. Download your data: https://support.google.com/accounts/answer/3024190
44. Vault: https://gsuite.google.com/products/vault/index.html
45. How retention works: https://support.google.com/vault/answer/2990828?hl=en#
46. How Google Uses Encryption to Protect Your Data: http://services.google.com/fh/files/helpcenter/google_encryptionwp2016.pdf

Page 9

47. Google Cloud Privacy: https://cloud.google.com/security/privacy/
48. Google Code of Conduct: https://abc.xyz/investor/other/google-code-of-conduct/
49. Google Cloud Security and Compliance whitepaper: https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-cloud-security-and-compliance-whitepaper.pdf

Page 10

50. Google Cloud Compliance resource center: https://cloud.google.com/security/compliance/