Google Cloud

Google Cloud Whitepaper
March 2024

The California Consumer Privacy Act (CCPA) and Consumer Privacy Rights Act (CPRA)

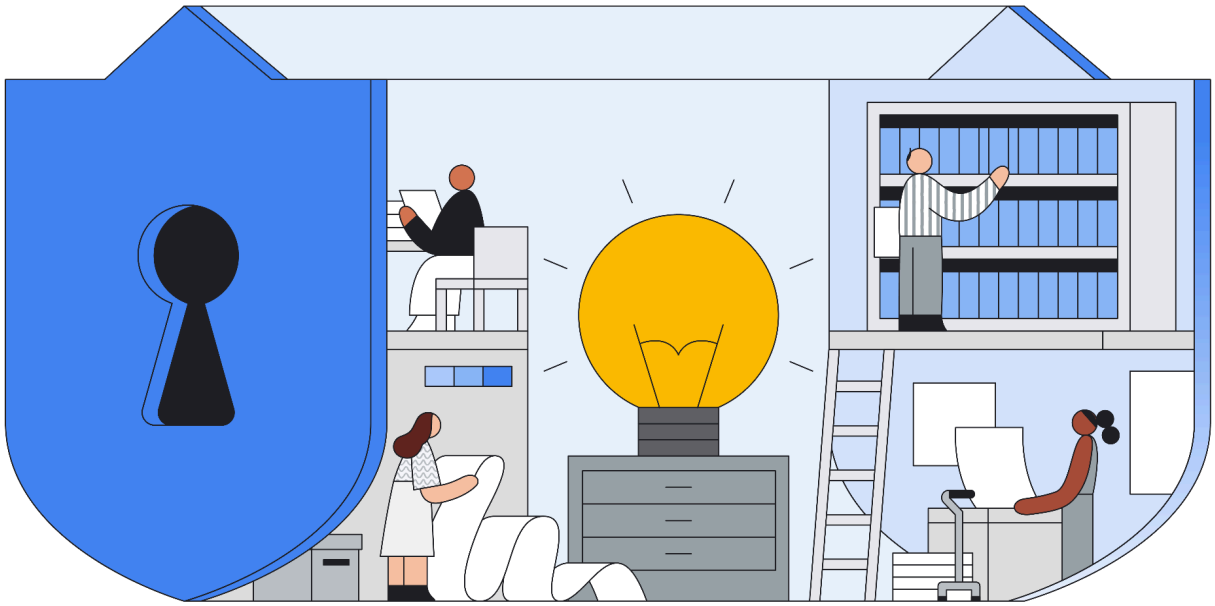


Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of March 2024 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

The California Consumer Privacy Act (CCPA), effective as of January 1, 2020, represents a significant milestone in the evolution of privacy laws in the United States. The CCPA was amended effective January 2023 by the California Privacy Rights Act (CPRA), and the California government has issued regulations implementing the law on numerous occasions. The amended CCPA is what will be referenced for the remainder of this whitepaper.

The CCPA introduces privacy rights for consumers and imposes data protection obligations on entities handling personal information. This overview provides a detailed analysis of the CCPA's key legal requirements, reflecting its comprehensive scope and impact on businesses and consumers.

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

Overview of the California Consumer Privacy Act (CCPA)

Who is subject to the CCPA?

The CCPA applies primarily to "businesses," which the law defines as for-profit entities that do business in California, determine the purposes and means of processing personal information, and meet certain revenue (annual revenue above $25,000,000) or data processing (e.g., processing the personal information of 100,000 consumers) thresholds. The CCPA also applies to parties to whom a business discloses information, which are referred to as third parties, service providers, or contractors depending on the nature of their relationship with the business.

Whose Information does the CCPA Protect?

The CCPA protects the personal information of "consumers," who are California residents. The CCPA applies even if the "consumer" is acting in their capacity as an employee or other professional capacity.

What are the CCPA's Key Legal Requirements?

1. **Consumer Rights**

    - **Right to Know**: Consumers have the right to know about the personal information a business collects about them and how it is used and shared.

- **Right to Delete**: Consumers can request the deletion of their personal information held by businesses.
- **Right to Correct.** Consumers have the right to correct information that the business maintains about them.
- **Right to Opt-Out**: Consumers can opt out of the sale of their personal information. For minors under 16, affirmative consent (opt-in) is required.
- **Right to Limit.** Consumers may limit the purposes for which a business uses their sensitive information.
- **Right to Non-Discrimination**: Businesses cannot discriminate against consumers who exercise their CCPA rights.

2. **Business Obligations**
    - **Notice at Collection**: Businesses must provide a notice at the point of collection, informing consumers of the categories of personal information to be collected and the purposes for which it will be used.
    - **Data Security**: Businesses are required to implement reasonable security procedures and practices to protect consumers' personal information.
    - **Verification of Requests**: Businesses must verify the identity of consumers who make requests to exercise their rights under the CCPA.
    - **Training and Record-Keeping**: Businesses are required to train employees to handle consumer inquiries and maintain records of consumer requests and responses for 24 months.

3. **Scope and Applicability**
    - The CCPA applies to for-profit businesses that do business in California and meet certain thresholds, such as annual gross revenues over $25 million, buying, receiving, selling, or sharing the personal information of 100,000 or more consumers, households, or devices, or deriving 50% or more of annual revenues from selling consumers' personal information.

4. **Penalties and Enforcement**
    - The California Attorney General enforces the CCPA. Violations can result in fines of to $7,500 per intentional violation and $2,500 per unintentional violation.
    - The CCPA also provides a private right of action for consumers in the event of a data breach caused by a business's failure to implement and maintain reasonable security procedures, with statutory damages between $100 to $750 per consumer per incident, or actual damages, whichever is greater.

5. **Special Considerations**
    - **Children's Privacy**: The CCPA requires businesses to obtain opt-in consent from consumers under 16 years of age before selling their personal information. For consumers under 13, parental consent is required.
    - **Sale of Personal Information**: The CCPA broadens the definition of "sale" beyond its plain-English meaning, to include sharing, making available, or transferring personal information for monetary or other valuable consideration.

6. **Updates and Amendments**

- The CCPA is subject to ongoing amendments and interpretations, necessitating continuous monitoring for compliance updates.

The CCPA marks a paradigm shift in data privacy regulation in the United States, emphasizing consumer control over personal data. Businesses, unless they are exempt from CCPA, must adapt to these comprehensive requirements, ensuring transparency, accountability, and enhanced data protection measures in their operations.

Google Cloud data protection overview & the Shared Responsibility Model

Google Cloud's robust security and privacy controls give customers the confidence to utilize Google Cloud services and Google Workspace in a manner aligned with the requirements of the CCPA.

Moreover, we are constantly working to expand our privacy and security capabilities. To help customers with compliance and reporting, Google shares information and best practices, and provides easy access to documentation. In this section, we describe our comprehensive data protection and privacy capabilities and our robust data security features most relevant to the CCPA. We then explain how we share security and compliance responsibilities according to the Shared Responsibility Model.

Google Cloud's approach to security and data protection

Google's focus on security and protection of information is among our primary design criteria. Security is at the core of everything we do; it is embedded in our culture and our architecture and we focus on improving it every day. In this section, we provide an overview of the organizational and technical controls we use to protect your data. To learn more about our approach to security and compliance, refer to the Google security whitepaper for Google Cloud services and the Google Workspace Security whitepaper.

Data protection and privacy trust principles
We want our customers to feel confident when using Google Cloud and Google Workspace products.

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

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

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

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

1. **Know that your security comes first in everything we do.**
We promptly notify you if we detect a breach of security that compromises your data.

2. **Control what happens to your data.**
We process customer data according to your instructions. You can access it or take it out at any time.

3. **Know that customer data is not used for advertising.**
You own your data. Google Cloud does not process your data for advertising purposes.

4. **Know where Google stores your data and rely on it being available when you need it.**
We publish the locations of our Google data centers; they are highly available, resilient, and secure.

5. **Depend on Google's independently-verified security practices.**
Our adherence to recognized international security and privacy standards is certified and validated by independent auditors — wherever your data is located in Google Cloud.

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

Dedicated privacy team
The Google privacy team operates separately from product development and security organizations but participates in every Google product launch by reviewing design documentation and performing code reviews to ensure that privacy requirements are followed.

They help release products that reflect strong privacy practices: transparent collection of user data, providing users and administrators with meaningful privacy configuration options, and continuing to be good stewards of any information stored on our platform. To learn more about our privacy team, refer to the privacy team section of the Google security whitepaper for Google Cloud services and the Google Workspace Security whitepaper.

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

Restricted access to customer data
To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when the data is stored on the same physical server. Only a small group of Google employees has access to customer data under explicit reasons based on job function and role. Any additional access is granted according to stringent procedures and tracked through audit records.

Google Cloud's approach to data security

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

Strong security culture

Security is central to Google's culture. It is reinforced in employee security training and company-wide events to raise awareness and drive innovation in security and privacy.
To learn more about our security culture, refer to the security culture sections in our Google security whitepaper and our Google Workspace Security whitepaper.

Security team

Google employs hundreds of security professionals, including some of the world's foremost experts. This team maintains the company's defense systems, develops security review processes, builds security infrastructure, implements Google's security policies, and actively scans for security threats.

Our team also takes part in research and outreach activities to protect the wider community of Internet users, beyond just those who choose Google solutions. Our research papers are available to the public.

As part of our outreach efforts, we have a team known as Project Zero that aims to prevent targeted attacks by reporting bugs to software vendors.

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

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

Trusted infrastructure

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

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

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

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

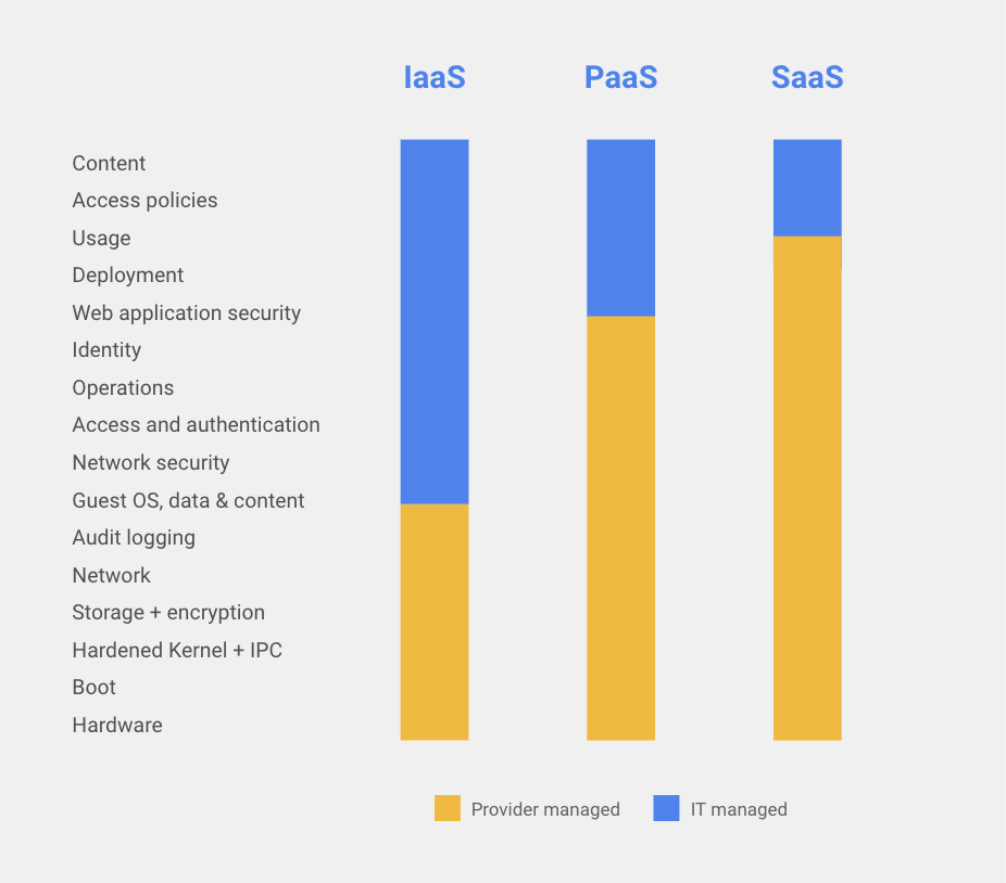
Data encryption
Google encrypts data at rest and encrypts data in transit, by default. The type of encryption used depends on the OSI layer, the type of service, and the physical infrastructure component. By default, we encrypt and authenticate all data in transit at one or more network layers when data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

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

The Shared Responsibility Model

Under our Shared Responsibility Model, the cloud customer and its CSP share the responsibilities of managing the IT environment, including those related to security and

compliance. As a trusted partner, Google Cloud's role in this model includes providing services on a highly secure and controlled platform and offering a wide array of security features from which customers can benefit. Shared responsibility enables our customers to allocate resources more effectively to their core competencies and concentrate on what they do best. The shared responsibility model does not remove the accountability and risk from customers using Google Cloud services, but it does help relieve the burden as we manage and control system components and physical control of facilities. It also shifts a portion of the cost of security and compliance onto Google Cloud and away from our customers. The figure below visually demonstrates an example of the shared responsibility model across on-prem, infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings. Keep in mind that responsibilities will vary depending on the specific services being used.



For more information on Google Cloud products and security configurations, customers should reference the applicable product documentation.

How Google Cloud helps customers meet the requirements of the CCPA

Data Protection Obligations	How Google Supports CCPA Requirements
Collection, use, and disclosure of personal information	
Notice of Collection • A business must provide consumers with a notice at collection of personal	Customer Responsibility:

Data Protection Obligations	How Google Supports CCPA Requirements
information at or before the time of collection. The "notice at collection" must list the categories of personal information businesses collect about consumers and the purposes for which they use the categories of information. • Develop comprehensive processes to inform consumers in detail about the categories of personal information being collected, the sources from where it is collected, the business or commercial purpose for collecting or selling personal information, and the categories of third parties with whom the business shares personal information. This includes providing information in online privacy policies or notices and upon consumer request.	• Ensure the personal information is collected in a lawful manner. • Customers must also make disclosures about how they collect and process personal information, including the purposes for processing. Google Cloud Commentary: • Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms.
• Businesses must collect personal information for only the purposes disclosed to consumers at the time of collection and for purposes within the consumer's reasonable expectations.	Customer responsibility: • You decide what information to put into the services and which services to use, how to use them, and for what purpose. Google Cloud Commentary: • Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms. Google will not use it for any other products or to serve advertising. Refer to the Data Usage section of the Google security whitepaper.
Accountability	
• Implement effective systems to handle and fulfill consumer requests for deletion of their personal information, considering legal exceptions for data retention. This involves confirming receipt of deletion requests within ten days and	Google Cloud Commentary: • Google provides functionality to enable customers to access, rectify, and restrict the processing

Data Protection Obligations	How Google Supports CCPA Requirements
responding to requests within 45 days.	of their data as well as retrieve or delete data. ● Businesses can use the following functionality of Google Cloud services: ○ Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources. ○ Admin Console: A web-based graphical user interface that customers can use to manage their Google Workspace resources. ○ gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. ○ Google APIs: Application programming interfaces which provide access to Google Cloud.
● A consumer may request that a business disclose to that consumer or his or her agent the specific pieces of personal information collected about the consumer.	Google Cloud Commentary: ● Customers may access their data on Google Cloud services at any time. ● If Google receives a request from an individual relating to their personal information, our privacy team will advise the requester to submit the request to you, the Google Cloud customer. Google Cloud customers can then take control for responding to these requests as per their internal procedures and requirements.

Data Protection Obligations	How Google Supports CCPA Requirements
	• Google Cloud's administrative consoles and services possess the functionality to access any data that you or your users put into our systems.
• Consumers have a right to dispute the accuracy of or an error in the personal information concerning them and to have the businesses correct it unless the business can document why the information is accurately maintained.	Google Cloud Commentary: • Customers may access their data on Google Cloud services at any time. If Google receives a request from an individual relating to the correction of their personal information, our privacy team will advise the requester to submit the request to you, the Google Cloud customer. Google Cloud customers can then take control for responding to these requests as per their internal procedures and requirements. • Google Cloud's administrative consoles and services possess the functionality to rectify any data that you or your users put into our systems.
Privacy & Security Program • The CCPA requires that entities have a comprehensive privacy and security program in place. Specifically, entities involved in the processing of personal information must develop, implement and review procedures for collecting personal information, obtaining consent for processing, and limiting use of personal information to declared purposes. Entities must also develop policies for access management, system monitoring, and protocols to follow during security incidents or technical	Customer Responsibility • Customers should implement sufficient security controls to protect the personal information including proper configuration of features in the cloud under customer management. Google Cloud Commentary: Google helps customers fulfill this requirement in the following ways: (1) Security of Google's infrastructure Google manages the security of our infrastructure (i.e., the hardware, software, networking and facilities that support the services). Google provides detailed information to customers about our security practices at:

Data Protection Obligations	How Google Supports CCPA Requirements
problems; policies and procedures for data subjects to exercise their rights under the Act; and a data retention schedule, including timeline or conditions for erasure or disposal of records.	● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page ● Our Cloud compliance page (2) Security of your data and applications in the cloud (a) Security by default ● Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. ● Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products Information on Google's security products is available on our Cloud Security Products page. The below illustrative list of Google Cloud and Google Workspace services may be used to help with your storage and security requirements: Access control 2-Step Verification ● 2-Step Verification puts an extra barrier between customers' businesses and cybercriminals who try to steal usernames and passwords to access business data. With 2-Step Verification, customer's users

Data Protection Obligations	How Google Supports CCPA Requirements
	sign in to their account in two steps with something they know (their password) and something they have (their mobile phone with Google OTP installed) Identity and Access Management (IAM) ● Identity and Access Management (IAM) can be used to assign roles and permissions to administrative groups, incorporating principles of least privilege and separation of duties. VPC Service Controls ● VPC Service Controls allow customers to address threats such as data theft, accidental data loss, and excessive access to data stored in Google Cloud multi-tenant services. It enables clients to tightly control what entities can access what services in order to reduce both intentional and unintentional losses. ● VPC Service Controls delivers zero-trust style access to multi-tenant services. Clients can restrict access to authorized IPs, client context, and device parameters while connecting to multi-tenant services from the internet and other services. Examples include GKE, BigQuery, etc. It enables clients to keep their entire data processing pipeline private. Access Log Cloud Logging ● Cloud Logging is a fully managed service that allows you to store, search, analyze, monitor, and alert on logging data and events from Google Cloud and Amazon Web Services. You can collect logging data from over 150 common application components,

Data Protection Obligations	How Google Supports CCPA Requirements
	on-premises systems, and hybrid cloud systems. Access Transparency ● Access Transparency Maintain visibility of insider access to your data through near real-time logs from Access Transparency. Protection from External Threats Cloud Security Command Center ● Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security posture by evaluating your security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities, and threats; and helping you mitigate and remediate risks. Virtual Machine Threat Detection ● Virtual Machine Threat Detection, a built-in service of Security Command Center Premium, provides threat detection through hypervisor-level instrumentation. Monitoring ● The Google Cloud Status Dashboard provides status information on the services. ● The Google Workspace Status Dashboard provides status information on the services. ● Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including the availability and uptime of the services. ● Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and

Data Protection Obligations	How Google Supports CCPA Requirements
	when, analyzing administrator activity, and much more. (c) Security resources Google also publishes guidance on: ● Security best practices ● Security use cases ● Security blueprints
Care of Personal Information	
● California law requires a business to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. ● Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General.	Customer Responsibility: ● Customers should develop policies and procedures for effectively addressing data breaches, including early warning systems, effective communication protocols, and robust remediation procedures. Google Cloud Commentary: ● Google recognizes that to effectively manage your use of the services, including handling potential data breaches, you need sufficient information about the services on a regular basis. We provide a number of mechanisms to assist you in effectively overseeing the services on an ongoing basis. ● Google will make information about developments that materially impact Google's ability to perform the services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard for Google Cloud and the Status Dashboard for Google Workspace. ● Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is

Data Protection Obligations	How Google Supports CCPA Requirements
	available in our Data incident response whitepaper. ● To fulfill this obligation, Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide an early indication of potential incidents. Refer to our Data incident response whitepaper for more information.
● Any time a business discloses personal information to another party, such as a technology vendor, the business must enter into specific contractual terms with such recipient of the personal information.	Google Cloud Commentary: ● Google Cloud makes robust confidentiality, data protection, and security commitments in our contracts. ● Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you and to only access and use your data to the extent required to perform the obligations subcontracted to them.

Conclusion

At Google, we recognize that your data is yours only, and guaranteeing the privacy of your data is key.

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

For these reasons and more, over five million organizations across the globe, including 64 percent of the Fortune 500, trust Google with their most valuable asset: their information. Google will continue to invest in our platform to allow you to benefit from our services in a secure and transparent manner. The information within this whitepaper should be used to help customers determine whether Google Cloud and Google Workspace products or services are suitable for them in light of the CCPA.