

Trusting your data with Google Cloud Platform

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 fundamental to how we design and build our products. We start from the fundamental premise that Google Cloud Platform (GCP) customers own their data and control how it is used. The data a customer stores and manages on GCP systems is only used to provide that customer with GCP services and to make GCP services work better for them, and for no other purpose. Not advertising, not for anything else. Period.

We have robust internal controls and auditing to protect against insider access to customer data. This includes providing our customers with near real-time logs of Google administrator access on GCP; GCP is the only major cloud to provide this level of access transparency. In addition to continuous security monitoring, all customer data stored in GCP is encrypted at rest and in transit by default. Customers can also choose to manage their own encryption keys using GCP's Cloud Key Management Service, a feature commonly referred to as "customer-managed encryption keys (CMEK)."

We also enable our customers to monitor their own account activity. We provide reports and logs that make it easy for a customer's administrator to examine potential security risks, track access, analyze administrator activity, and much more. Administrators in your organization can also leverage Cloud Data Loss Prevention (DLP) capabilities to protect sensitive information. DLP adds a layer of protection to identify, redact, and prevent sensitive or private information from leaking outside of an organization. Additionally, your administrators can also enforce policies over mobile devices in their organization, encrypt data on devices, and perform actions like remotely wiping or locking lost or stolen devices.

Furthermore, we undergo independent, third-party audits and certifications to verify that our data protection practices match our commitments. For example, as part of the [ISO 27018](#) certification process associated with the protection of personally identifiable information (PII), Google is audited against a set of controls relating to purpose legitimacy and specification, thereby ensuring that PII is not processed by public cloud providers for commercial use.

Google will continue to invest in our security, innovation, and operational procedures to evolve our GCP platform to allow customers to benefit from our services in a secure and transparent manner. For more information, please visit cloud.google.com/security/.

