




Google Apps Security and Compliance Summary

How Google Protects Your Data

Google for Work

August 2016

A man in a grey hoodie and blue jeans is kneeling in a server room, looking at a server rack. The room is filled with rows of server racks, with blue cables and lights visible. The man is holding a small object, possibly a tool or a component, and is looking down at it. The server racks are filled with various components, including circuit boards and cables. The room is well-lit, and the man is the central focus of the image.

Google Apps Security and Compliance Summary: How Google Protects Your Data

Google works hard to earn and maintain your trust by processing your data in a secure, reliable, and compliant environment. Security and privacy are critically important, which is why we have invested deeply to protect your data.

More than 5 million businesses have chosen Google Apps for Business and 64 percent of the Fortune 500 are actively using an enterprise product from Google. Google Apps has a large international customer base representing over 50 percent of our business customers. We understand that our customers have varying regulatory needs, and Google Apps helps address these diverse requirements by providing robust security, compliance, and data protection capabilities. Google has industry-leading knowledge and expertise building secure cloud infrastructure and applications at scale.

“ Trust begins with understanding.
Understanding requires transparency. ”

We welcome the opportunity to introduce you to our products and in particular, we invite you to review our detailed documentation, audit reports, and certifications.

Security and Privacy

Good privacy requires strong security. We've spent years developing an advanced, security-focused infrastructure to keep your information safe.

It's your data

Google Apps customers own their data, not Google. The data that Google Apps organizations and users put into our systems is theirs, and we do not scan it for advertisements nor sell it to third parties. We offer our customers a detailed [Data Processing Amendment](#) that describes our commitment to protecting customer data.

Furthermore, if customers delete their data, we commit to deleting it from our systems within 180 days. Finally, we provide tools that make it easy for customer administrators to take their data with them if they choose to stop using our services, without penalty or additional cost imposed by Google.

No advertising

There is **no** advertising in the [Google Apps Core Services](#), and we have no plans to change this in the future. Google does not collect, scan, or use data in Google Apps Core Services for advertising purposes. Customer administrators can restrict access to Non-Core Services from the Google Apps Admin Console. Google indexes customer data to provide beneficial services, such as spam filtering, virus detection, spellcheck, and the ability to search for emails and files within an individual account.

“ There is no advertising in Google Apps Services. ”



[Read our Data Processing Amendment](#)

A Secure and Reliable Infrastructure

We work exceptionally hard to keep your information safe.

Google employs more than 600 full-time professionals working to protect your data, including some of the world's foremost experts in computer security. Google invests millions of dollars in our technology and bakes security protections into our products.

Here are a few examples of how security and reliability are at the core of what we do:

- Google's **data centers** house energy-efficient, custom, purpose-built servers and **network equipment** that we design and manufacture ourselves. Unlike much commercially available hardware, Google servers don't include unnecessary components such as video cards, chipsets, or peripheral connectors, which can introduce vulnerabilities.
- Google Apps customers' data is encrypted when it's on a disk, stored on backup media, moving over the Internet, or traveling between data centers. Additional details on encryption key management and on how data is protected at rest, in transit, and on backup media can be found in our **Google Apps Encryption Whitepaper**.
- Google's application and network architecture is designed for maximum reliability and uptime. Data is distributed across Google's servers and data centers. If a machine fails — or even an entire data center — your data will still be accessible. Google owns and operates data centers **around the world** to keep the services you use running 24 hours a day, 7 days a week. In addition, we have real-time **availability status dashboards** which are publicly available.
- Google products are scrutinized by privacy, security, and compliance specialists throughout the product lifecycle. This helps ensure that data is handled appropriately and no unwarranted access is allowed or possible. Additional details can be found in our **Google Apps Security and Compliance Whitepaper**.
- Administrators can elect to **receive notifications** when events occur, such as suspicious login attempts, or service setting changes by other administrators.



Regulatory Compliance

At Google we work to continually meet rigorous privacy and compliance standards so that your users can rest easy knowing that their data is safe, private, and secure.

Independent audits of infrastructure, applications, and operations

Google's customers and regulators expect independent verification of our security, privacy, and compliance controls. In order to provide this, we undergo several independent third-party audits on a regular basis. For each one, an independent auditor examines our data centers, infrastructure, and operations.

Google operates one cloud, and regular audits are conducted to certify our compliance with the following auditing standards:

- **ISO 27001** – certification for the systems, applications, people, technology, processes, and data centers
- **ISO 27017** – security controls based on ISO/IEC 27002 specifically for cloud services
- **ISO 27018** – international standard of practice for protection of personally identifiable information (PII) in public cloud services
- **SOC 2/SOC 3** – audit framework for non-privacy principles that include security, availability, processing integrity, and confidentiality
- **FedRAMP** (U.S. Federal Risk and Authorization Management Program) – a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services

Google's third-party audit approach is designed to be comprehensive in order to provide assurances of Google's 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.

Data Processing Amendment

Google takes a global approach to our commitments on data processing. Google and many of our customers operate in a wide range of countries around the world. Google Apps offers a [Data Processing Amendment](#) and [EU Model Contract Clauses](#) to facilitate compliance with jurisdictional specific laws or regulations. Your organization can opt into our Data Processing Amendment by following the instructions in our [Help Center](#).

EU Data Protection Directive

The European Commission has provided guidance on how to meet European data privacy requirements when engaging with cloud computing providers. Google provides capabilities and contractual commitments created to meet data protection recommendations provided by the European Commission's Article 29 Working Party, an independent advisory body focused on data protection and privacy.

EU Model Contract Clauses

In 2010, the European Commission approved model contract clauses as a means of compliance with the requirements of the EU Data Protection Directive. Incorporating these clauses into a contract provides additional data safeguards, allowing providers to transfer and process personal data of EU users outside the EU. Google has a broad customer base in Europe. By adopting [EU Model Contract Clauses](#), we're offering customers an additional option for compliance with the Directive.

Continuing with our push for openness, we make our [EU Model Contract Clauses](#), [Data Processing Amendment](#), and [Subprocessor Disclosure](#) publicly available for review.





U.S. Health Insurance Portability and Accountability Act, HIPAA

Google Apps supports our customers' compliance with the U.S. Health Insurance Portability and Accountability Act (HIPAA), which governs the confidentiality and privacy of protected health information (PHI). Customers who are subject to HIPAA and wish to use Google Apps with PHI should sign a [Business Associate Agreement \(BAA\)](#) with Google. The BAA covers Gmail, Google Calendar, Google Drive, Google Sites, and Google Apps Vault. Additional information can be found in our [HIPAA Implementation Guide](#).

U.S. Family Educational Rights and Privacy Act, FERPA

More than 30 million students rely on Google Apps for Education. Google provides Apps for Education core services in accordance with the Family Educational Rights and Privacy Act (FERPA), and our commitment to do so is included in our Google Apps for Education agreements.

Children's Online Privacy Protection Act of 1998, COPPA

Protecting children online is important to us. Google Apps for Education is designed to allow our services to be used for educational purposes in schools in a manner consistent with the requirements of the Children's Online Privacy Protection Act (COPPA).

FedRAMP

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that is intended to expedite U.S. government agency security assessments and help agencies move to secure cloud solutions. [Google maintains a FedRAMP Authorization to Operate \(ATO\) for Google Apps and App Engine](#).

Conclusion

The protection of user data is a primary design consideration for all of Google's infrastructure, applications, and personnel operations. Protection of user data is far from being an afterthought or the focus of occasional initiatives – it's an integral part of what we do. We believe that Google can offer a level of protection that very few can match. Because protecting your data is part of our core business, Google can develop security innovations such as **two-step authentication** and **stronger encryption methods**.

“ We are able to make extensive investments in security, resources, and expertise at a scale that few can afford.

Joe Kava, VP, Google Data Center Operations ”

Our scale of operations and collaboration with the security research community enable Google to address vulnerabilities quickly or prevent them entirely. Google's security and operational procedures are verified by independent third-party auditors.

Data protection is more than just security: Google offers strong contractual commitments in our **Data Processing Amendment** to make sure our customers maintain control over their data and how it is processed, including the assurance that your data in the Apps Core Services is used for the purposes specified in your agreement, and not used for advertising.

For these reasons and more, over 5 million organizations across the globe, including 64 percent of the Fortune 500, trust Google with their most valuable asset: their information. Google will continue investing in security and innovation to evolve our platform, which allows our users to benefit from our services in a secure and transparent manner.

Want to know more?

Please review our complete **Security and Compliance Whitepaper** or **contact our Sales Team**.

