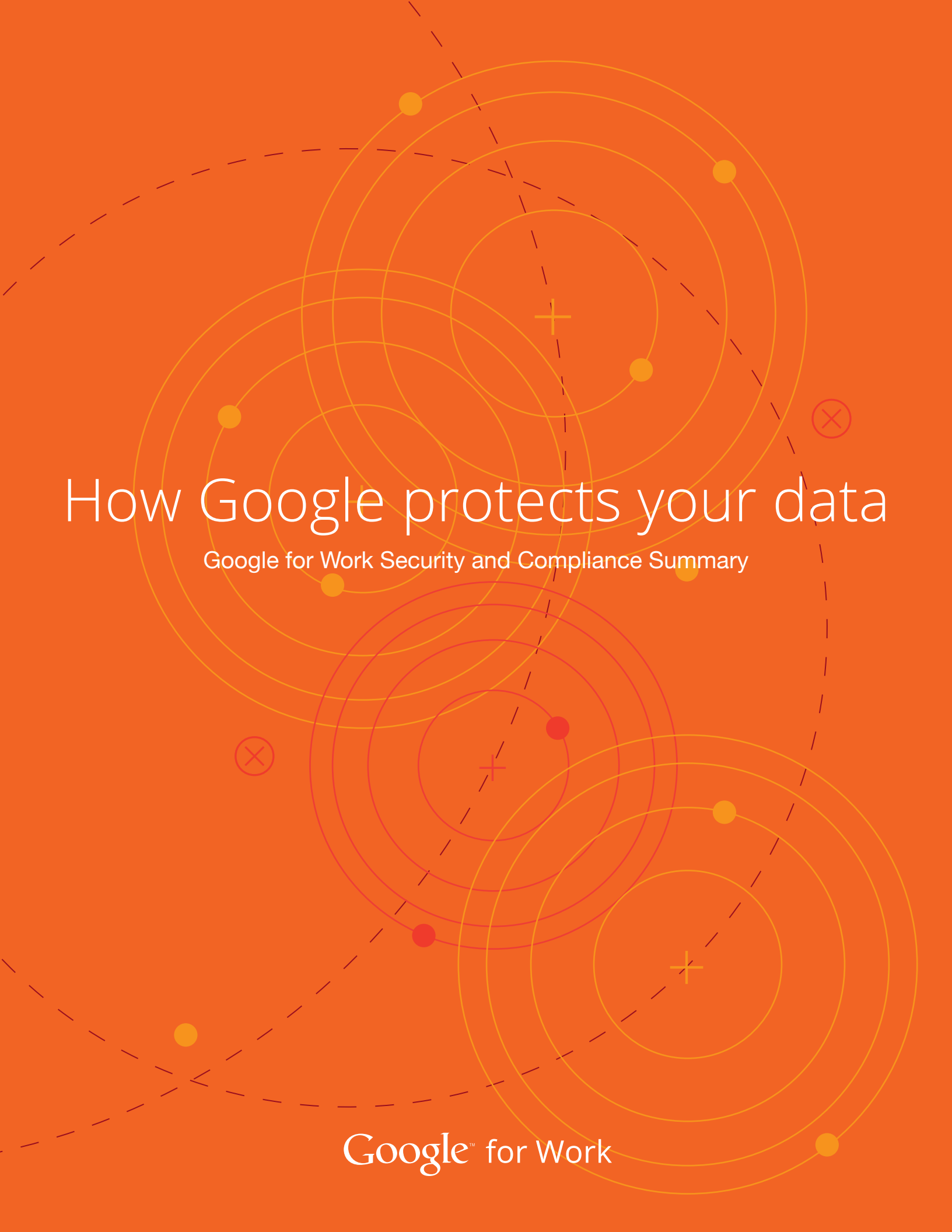


How Google protects your data

Google for Work Security and Compliance Summary

Google™ for Work

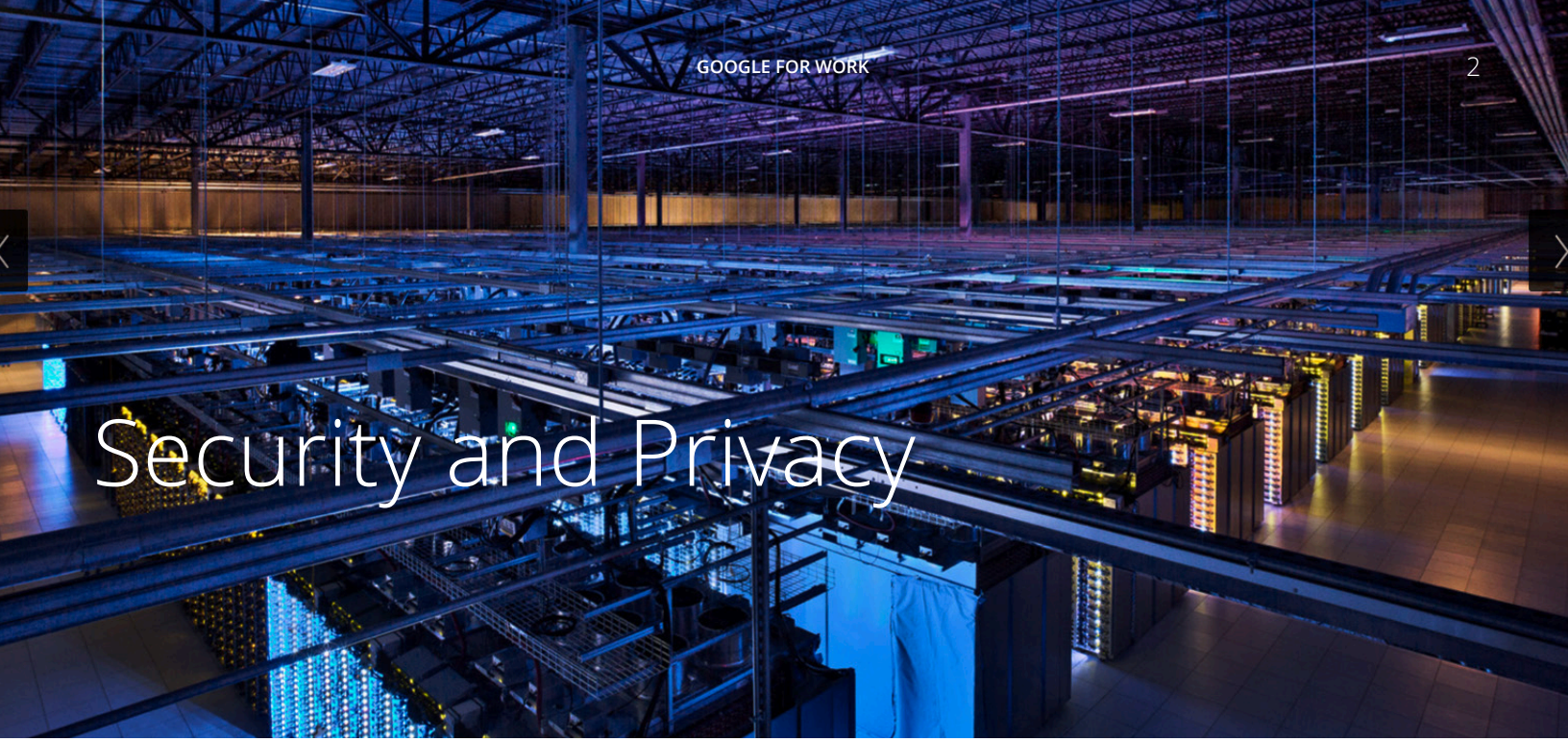
Data Security, Transparency & Privacy How Google Protects Your Data

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 58% of the Fortune 500 are actively using a paid, enterprise product from Google. Google Apps has a large international customer base representing over 50% 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.”

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 companies, schools and students put into our systems is theirs. Google does not sell your data to third parties. Google offers our customers a detailed Data Processing Amendment that describes our commitment to protecting your data. For example, Google will not process your data for any purpose other than to fulfil our contractual obligations. Further, we commit to deleting data from our systems within 180 days of your deleting it in our services. Finally, we provide tools to make it easy for you to take your data with you if you choose to stop using our services altogether, without penalty or additional cost imposed by Google.

No advertising. There is no advertising in Google Apps Services and we have no plans to change this in the future. Google does not collect or use data in Google Apps Services for advertising purposes.

Privacy controls. Google Apps privacy controls are configured by your organization's administrator. For example, Apps administrators can enforce default profile discoverability for Google+, which prevents external Google+ users from finding your users in a public Google+ search. Administrators can also set a policy determining whether users can share their Google Drive documents outside your organization, whether they can access documents created outside your organization and the default visibility level for new documents. For more information on administrative controls and settings, please refer to our Administrative Help Center.

> "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 500 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 runs its data centers using custom hardware, running a custom operating system and file system. Each of these systems has been optimized for security and performance. Since Google controls the entire hardware stack, we are able to quickly respond to any threats or weaknesses that may emerge.

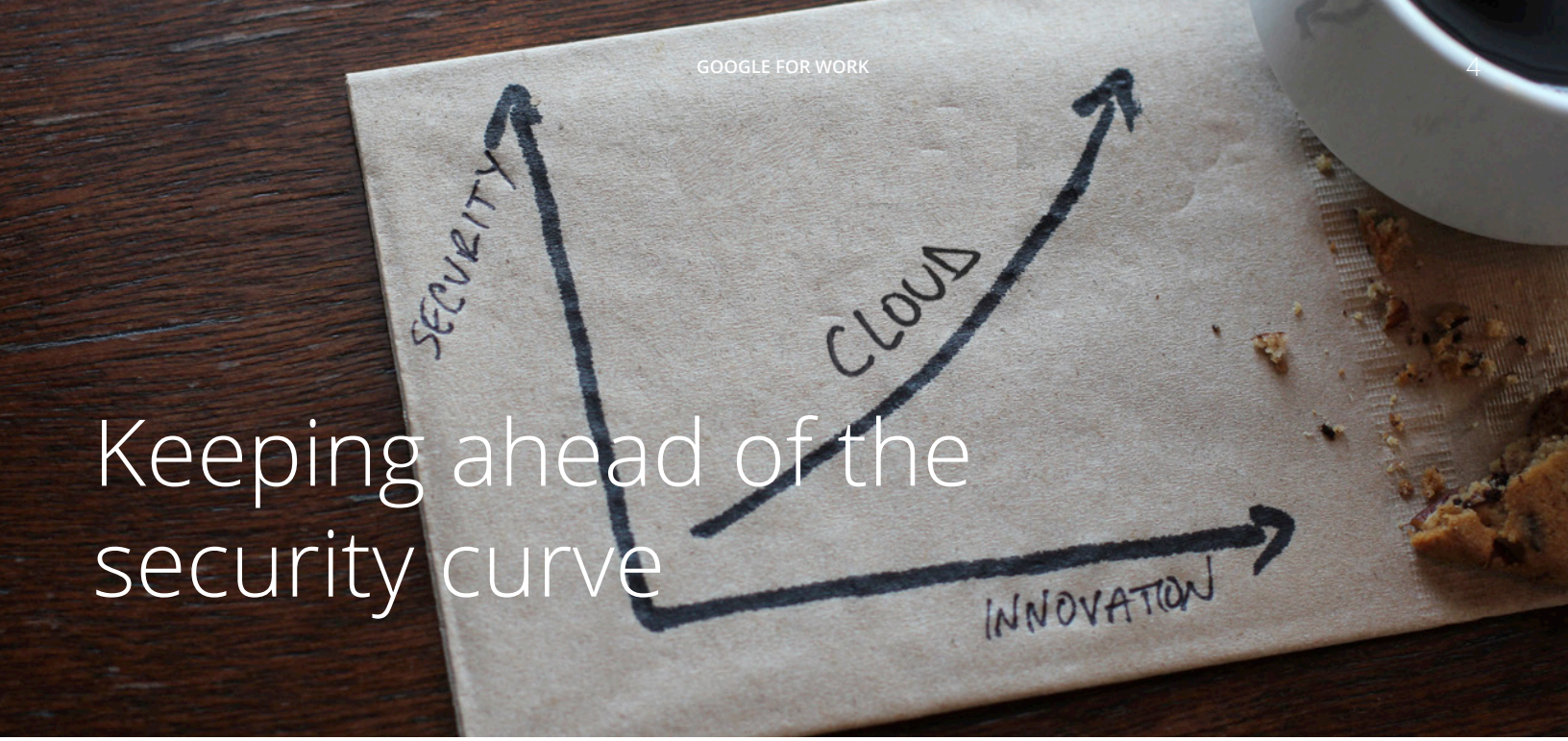
- Google's application and network architecture is designed for maximum reliability and uptime. Data is distributed across Google's servers and data centers. If a machine fails or even an entire data center your data will still be accessible. Google owns and operates data centers around the world to keep the services you use running 24 hours a day, 7 days a week.

- Google Apps offers a 99.9% service level agreement, and in recent years, we've exceeded this promise; most recently, Gmail achieved 99.978% availability in 2013. Furthermore, Google Apps has no scheduled downtime or maintenance windows. Unlike most providers, we do not plan for our applications to be unavailable, even when we're upgrading our services or maintaining our systems.

- 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.

- Administrators can elect to receive notifications when events occur, such as suspicious login attempts, or service setting changes by other administrators.

- Google is constantly working to extend and strengthen encryption across more services and links.



Keeping ahead of the security curve

Security has always been a top priority for Google. Here are a few ways we're setting new standards in security:

- Google is the first major cloud provider to enable perfect forward secrecy, which encrypts content as it moves between our servers and those of other companies. Many industry peers have followed suit or have committed to adoption in the future.
- Every single email message you send or receive—100% of them—is encrypted while moving internally. This ensures that your messages are safe not only when they move between you and Gmail's servers, but also as they move between Google's data centers.
- To protect against cryptanalytic advances, last year Google doubled the length of our RSA encryption keys to 2048 bits and we change them every few weeks raising the bar for the rest of the industry.
- Google has long enjoyed a close relationship with the security research community. To honor all the cutting-edge external contributions that help Google keep our users safe, we maintain a Vulnerability Reward Program for Google-owned web properties. Google was the first major cloud provider to offer a program of this type.

> Every single message is encrypted

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

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.

This means that an independent auditor has examined the controls present in our data centers, infrastructure and operations. Google has annual audits for the following standards:

- SSAE16 / ISAE 3402 Type II, SOC 2 detailed audit report of the SOC 2 controls and SOC 3 public audit report
- ISO 27001 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 centers serving Google Apps.
- FISMA FISMA Moderate accreditation (Google Apps for Government only)

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.

EU Data Privacy and Model Contract Clauses

The Article 29 Working Party is an independent European advisory body focused on data protection and privacy. They have provided guidance on how to meet European data privacy requirements when engaging with cloud computing providers.

> 50% of our business customers are based outside of the United States.

Google has a broad customer base in Europe. As previously stated, over 50% of our business customers are based outside of the United States. Our clients operate across regulated industries, including finance, pharmaceutical and manufacturing. Google provides capabilities and contractual commitments created to meet data protection recommendations provided by the Article 29 Working Party. Google offers EU Model Contract Clauses and a Data Processing Amendment. In addition to other privacy and security protections, Google will contractually commit to:

- Safe Harbor. Google will maintain compliance to Safe Harbor (or an appropriate alternative compliance solution) during the term of the agreement;
- Data Portability. Administrators can export customer data in standard formats at any time during the term of the agreement. Google does not charge a fee for exporting data;
- Google maintains adherence to ISO 27001 and SSAE 16 / ISAE 3402 audits during the term of the agreement;
- Access to our Data Privacy Officer. Customers may contact Google's Data Privacy Officer for questions or comments;
- Defined Security Standards. Google will define how data is processed, stored, and protected through specific defined security standards.

Continuing with our push for openness, we make our EU Model Contract Clauses, Data Processing Amendment and Subprocessor Disclosure publicly available for review. In addition, we have realtime availability status dashboards publicly available for our customers.

Our representatives in Europe and all over the world are standing by to help answer other questions you might have.

U.S. Healthcare Information Privacy obligations, HIPAA

Google Apps supports our customers' compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Customers who are subject to HIPAA and wish to use Google Apps with Protected Health Information (PHI) must sign a Business Associate Agreement (BAA) with Google. Administrators for Google Apps for Business, Education and Government domains can request a BAA before using Google services with PHI. Google offers a BAA covering Gmail, Google Calendar, Google Drive, Google Apps Vault and Google Sites services.

U.S. Family Educational Right Privacy obligations, FERPA

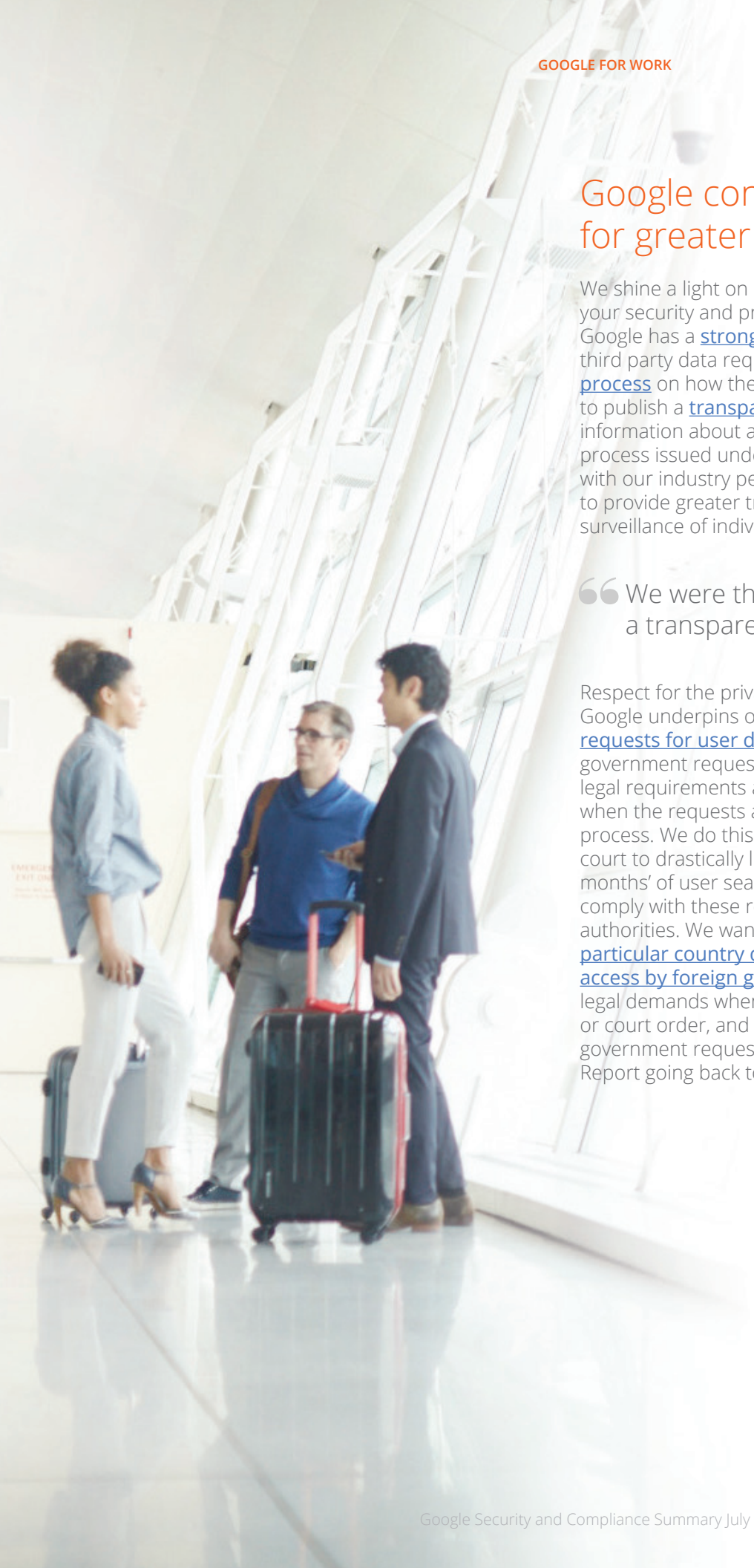
More than 40 million students rely on Google Apps for Education. Google Apps for Education complies with FERPA (Family Educational Rights and Privacy Act) and our commitment to do so is included in our agreements.

Children's Online Privacy Protection Act of 1998, COPPA

Protecting children online is important to us. We contractually require Google Apps for Education schools to obtain parental consent that COPPA calls for to use our services, and our services can be used in compliance with COPPA.

U.S. Information Security Management Act, FISMA

The Federal Information Security Management Act of 2002, or "FISMA", is a United States federal law pertaining to the information security of federal agencies' information systems. Google Apps has received an authority to operate at the FISMA-Moderate level -- the standard level for Federal email systems -- from the U.S. federal government. Hundreds of US Federal, State and local government agencies, including the U.S. General Services Administration (GSA) which has migrated over 17,000 employees and contractors to Google Apps for Government.



Google continues to push for greater transparency

We shine a light on how governments and other parties affect your security and privacy online because you deserve to know. Google has a strong track record of informing customers of third party data requests, in addition to having a transparent process on how these requests are handled. We were the first to publish a transparency report in 2010, and we now publish information about all types of legal process we receive, including process issued under national security authorities. Along with our industry peers, we've also called upon governments to provide greater transparency and accountability regarding surveillance of individuals and access to their information.

> We were the first to publish a transparency report in 2010.

Respect for the privacy and security of data you store with Google underpins our approach to complying with legal requests for user data. Our legal team reviews each and every government request for user data to make sure it satisfies legal requirements and Google's policies, and we push back when the requests are overly broad or don't follow the correct process. We do this frequently — like when we persuaded a court to drastically limit a U.S. government request for two months' of user search queries. When we are legally required to comply with these requests, we deliver that information to the authorities. We want you to know that storing your data in a particular country does not necessarily protect the data from access by foreign governments. Google notifies users about legal demands when appropriate, unless prohibited by law or court order, and have published aggregate statistics about government requests for user information in our Transparency Report going back to 2009.

Google™ for Work