Safeguards for international data transfers with Google's advertising and analytics products

February 2025

Introduction

This paper explains safeguards and supplementary commitments to EU GDPR, UK GDPR and Swiss FDPA[1] requirements (collectively, "**European Data Protection Legislation**") Google offers to protect personal data processed when you[2] use Google's advertising and analytics products.

European Data Protection Legislation does not require data localisation. In addition, the European Data Protection Legislation does not prohibit the transfer of European personal data outside the EEA, the UK and Switzerland, as applicable. European Data Protection Legislation imposes conditions on transfers outside the EEA, the UK and Switzerland, as applicable, to ensure an adequate level of data protection.

As described in Google's Data Privacy Framework certification, we comply with the EU-US and Swiss-US Data Privacy Frameworks and the UK Extension to the EU-US Data Privacy Framework (collectively the "**DPF**") as set forth by the US Department of Commerce regarding the collection, use and retention of EEA, UK and Swiss personal information.

Google LLC and its wholly-owned US subsidiaries (unless explicitly excluded), have certified that they adhere to the DPF Principles. To learn more about the DPF, and to view Google's certification, please visit the DPF website.

---

1. In this paper, "**EU GDPR**" refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; "**UK GDPR**" refers to the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018 and applicable secondary legislation made under that Act; and "**Swiss FDPA**" refers to, as applicable, the Federal Data Protection Act of 19 June 1992 (Switzerland) (with the Ordinance to the Federal Data Protection Act of 14 June 1993), or the revised Federal Data Protection Act of 25 September 2020 (with the Ordinance to the Federal Data Protection Act of 31 August 2022).
2. In this paper, "you" or "your" refers to customers of Google's advertising and analytics products listed at privacy.google.com/businesses/adsservices.

When you use Google's advertising and analytics products then as of 1 September 2023, Google relies on the EU-US Data Privacy Framework ("**EU DPF**") to transfer EEA personal data to Google LLC and its wholly-owned US subsidiaries in the US. As of 16 September 2024, Google relies, in certain circumstances, on the Swiss-US Data Privacy Framework ("**Swiss DPF**") and the UK Extension to the EU DPF ("**UK DPF**") for the transfer of personal data from Switzerland and the UK, respectively, to Google LLC and its wholly-owned US subsidiaries in the US. You can find more information about international data transfers in connection your use of Google's advertising and analytics products, including information about Google and/or its affiliates' adoption of, or certification under, any legal frameworks or solutions that enable the lawful transfer of personal data to a third country in accordance with European Data Protection Legislation at business.safety.google/adsdatatransfers.

As recognised by the European Commission in an adequacy decision under Article 45 GDPR, the EU DPF ensures an adequate level of protection for personal data transferred to entities that are self-certified under the EU DPF in accordance with Article 45(1) GDPR. The Swiss DPF and the UK DPF are also recognised by Switzerland and the United Kingdom, respectively, as ensuring an adequate level of protection for Swiss and UK personal data transferred to entities that are self-certified under those frameworks.

The onward transfer by Google LLC of personal data — including personal data to entities in non-adequate third countries is made in accordance with the DPF's onward transfer provisions. An adequate level of protection for personal data is maintained by the legal framework applicable to these onward transfers.

We are committed to improving user privacy, helping our customers protect their data, and assisting our customers in their compliance with applicable laws and regulations when using our services. This paper provides information on the additional safeguards and supplementary commitments offered by Google's advertising and analytics products to enhance the protection for transferred personal data. Please note, however, that we are not in a position to provide you with legal advice — this is something only your legal counsel can provide.

Technical safeguards

1. State of the art security

Security features are built into all our products, services and infrastructure to keep data protected at every layer. We invest in teams and technology to continually improve that security, protecting not only our operations, but your business as well.

Google has global scale technical infrastructure designed to provide security through Google's entire information processing life cycle. Specifically, this infrastructure is designed to provide secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, and safe operation by administrators.

The security of the infrastructure is designed in progressive layers starting from the physical security of data centres, continuing on to the security of the hardware and software that underlie the infrastructure, and finally the technical constraints and processes in place to support operational security. Find out more in the Data centres and physical security section of this paper below.

Our infrastructure is not designed to, and does not, give any government "backdoor" access to user data (including customer personal data) or to our servers storing user data. That means no government entity has direct access to our users' information or to customer personal data. In addition, we utilise robust technical measures (such as encryption, as described below) to protect against unlawful interception in transit, including unlawful surveillance attempts by government authorities around the world.

2. Encryption

Encryption is a process that takes readable data as input (often called plaintext), and transforms it into an output (often called ciphertext) that prevents reading of the plaintext. If data is encrypted, it will be unreadable to a third party without the encryption key, and therefore cannot be accessed in a meaningful form by any third party, including a government agency, that unlawfully intercepts or otherwise accesses the ciphertext. Access to the plaintext requires going through formal access channels, as described in the Organisational safeguards section of this paper below. Encryption is therefore an effective means of preventing any "covert" or unauthorised access to customer personal data.

Encryption in transit

Google encrypts data at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google, for example, when data is transferred between Google's data centres. Even if any data were unlawfully intercepted during these transfers, it would be unreadable.

Google's security policies require that all user data, including personal data, must be encrypted when transmitted over networks outside of Google's physical control.

Protecting data in transit within Google's infrastructure:
Google protects service-to-service communications at the application layer using a mutual authentication and transport encryption system developed by Google called Application Layer Transport Security (ALTS). ALTS is similar in concept to mutually authenticated TLS but has been designed and optimised to meet the needs of Google's data centre environments. ALTS authenticates the communication between Google services and helps to protect data in transit. ALTS is a highly reliable, trusted system that provides authentication and security for Google's Remote Procedure Call (RPC) communications. ALTS requires minimal involvement from Google services themselves. When Google services communicate with each other they do not need to explicitly configure anything to ensure data transmission is protected; this is protection of user data by design and by default.

Protecting data in transit between data centres:
ALTS ensures the integrity of Google traffic is protected, and encrypted as needed. After a handshake protocol between the client and the server is complete and the client and the server negotiate the necessary shared cryptographic secrets for encrypting and authenticating network traffic, ALTS secures RPC (Remote Procedure Call) traffic by forcing integrity, using the negotiated shared secrets. Google supports multiple protocols for integrity guarantees, e.g. AES-GMAC (Advanced Encryption Standard) with 128 bit keys. Whenever traffic leaves a physical boundary controlled by or on behalf of Google, e.g. in transit over WAN (Wide Area Network) between data centres, all protocols are upgraded automatically to provide encryption as well as integrity guarantees.

Protecting communication between users and websites:
HTTPS (Hypertext Transfer Protocol Secure) encryption helps keep users' browsing safe by securely connecting their browser or app with the websites they visit. HTTPS relies on encryption technology — SSL (Secure Sockets Layer) or TLS (Transport Layer Security) — to secure these connections. Such encryption prevents intruders from being able to passively listen to communications between websites and users. Since 2008 Google has been working to make sure Google services use strong HTTPS encryption by default. In 2015 Google announced a set of initiatives to bring this "HTTPS Everywhere" mission to our advertising products as well, to support our advertiser and publisher customers. We publish a report that provides data on the status of HTTPS adoption and usage at Google and across the web, including for our advertising and analytics products, as well as additional information about Google's use of encryption.

Encryption at rest

Encryption “at rest” means encryption used to protect user data that is stored on a disk (including solid-state drives) or backup media.

All user data is encrypted at the storage level, generally using AES256 (Advanced Encryption Standard). Data is often encrypted at multiple levels in Google’s production storage stack in data centres, including at the hardware level, without requiring any action by Google customers. Using multiple layers of encryption adds redundant data protection and allows Google to select the optimal approach based on application requirements.

Google uses common cryptographic libraries which incorporate Google’s FIPS 140-2 validated module to implement encryption consistently across products. Consistent use of common libraries means that only a small team of cryptographers needs to implement and maintain this tightly controlled and reviewed code.

Google’s security policies require encryption at rest for all user data, including personal data.

3. Pseudonymous advertising and measurement data

Online advertising data is commonly associated with online identifiers stored in cookies or mobile advertising identifiers, such as IDFA, or Android Ad IDs. This data on its own, to the extent it is personal data, is considered “pseudonymous” if it cannot be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

Google has a robust set of policies and technical and organisational controls in place to ensure the separation between pseudonymous online identifiers and personally identifiable user data (i.e. information that could be used on its own to directly identify, contact, or precisely locate an individual), such as a user’s Google account data.

Technical protection measures for keeping pseudonymous online identifiers separate from identifiable user data include the encryption of identifiers with rotating keys. This prevents records, e.g. in log files, from being linkable across pseudonymous and identifiable ID spaces. In addition, Google has controls in place aimed at preventing the joinability of data sets through common data elements, e.g. precise, stable time stamps associated with an event other than the pseudonymous online identifiers themselves.

Only a strictly limited set of Google employees has access to user data in line with their job function and strict authorisation procedures. Google has an additional authorisation and allowlisting process in place to provide another layer of protection in case individual engineers require access to both pseudonymous advertising data and Google user account data. Engineers must acknowledge Google’s policies about user data access and agree not to join these ID spaces.

Launch reviews for new products and features are another pillar for the enforcement of Google’s privacy and security policies across its products and infrastructure. Any launch at Google has to undergo a privacy review prior to launch. Privacy reviews are conducted by specially trained privacy engineers. In launch reviews related to advertising and measurement products, privacy engineers ensure that all applicable policies and guidelines are followed, including but not limited to those regarding the processing of pseudonymous data.

4. Data centres and physical security

Google operates data centres globally and to maximise the speed and reliability of our services, our infrastructure is generally set up to serve traffic from the data centre that is the closest to where the traffic originates. Therefore the precise location of Google advertising and analytics personal data may vary depending on where such traffic originates, and this data may be handled by servers located in the EEA, UK and Switzerland or transferred to third countries. Our customers' properties where Google advertising and analytics products are implemented are generally available globally and often attract a global audience. The technical infrastructure that supports these products is deployed globally to reduce latency and ensure redundancy of systems. Information about the locations of Google data centres is available here. The safeguards described in this paper apply regardless of the location of the data.

Security is part of Google's data centres' DNA. Google custom-builds servers exclusively for its data centres and maintains an industry-leading security team to ensure that Google's data centres are among the safest in the world. Google's production data centres are protected by several layers of security to prevent any unauthorised access to data, including specifically:

- **Boundary security and secure perimeter:** Data centre site boundaries are physically secured with fencing, signage and other measures. Secure perimeter defence systems are also used, including full thermal and standard camera coverage, smart fencing, visitor movement analysis, crash barriers and 24/7 guard patrols.
- **Building access:** Visitors are authenticated using badge readers before access through secure doors is permitted. Google uses multiple physical security layers to protect each floor. They include technologies like biometric identification, metal detectors, cameras, physical barriers, and laser-based intrusion detection.
- **SOC:** Google's security operations centre (SOC) monitors the data centre 24/7.
- **Data centre floor:** Access to the data centre floor is strictly "as needed". Google's security policies require encryption at rest for all user data, including personal data. Rather than storing each user's data on a single machine or group of machines, Google distributes all data across many computers in different locations. Data is chunked and replicated across multiple systems to avoid any single point of failure. Google names these data chunks randomly for additional security.
- **Secure disposal of data storage devices:** Google rigorously tracks the location and status of each hard drive in its data centres. Hard drives that have reached the end of their lives are destroyed in a thorough, multi-step process to prevent access to data.

Find out more in Data and Security — Data Centres.

5. Strong controls to limit access to trusted personnel

We limit access to Google's advertising and analytics personal data to Google personnel who need it to do their jobs:

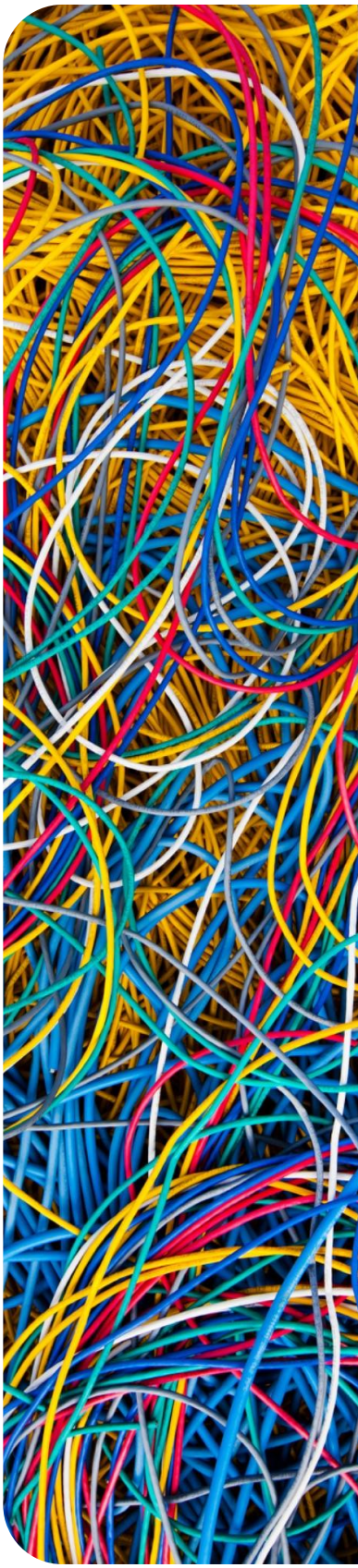
- **Infrastructure security personnel:** Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of Google's advertising and analytics products, and responding to security incidents.
- **Access control and privilege management:** Administrators and users of Google's advertising and analytics products must authenticate themselves via a central authentication system or via a single sign on system in order to use the products.
- **Internal data access processes and policies:** The group of Google employees with access to advertising and analytics personal data is strictly limited. For Google employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorisation settings and the approval process to ensure consistent application of the approval policies. An employee's authorisation settings are used to control access to all resources, including data and systems for Google advertising and analytics products. Google employee access is monitored and audited by our dedicated security, privacy, and internal audit teams. The systems are designed to detect any inappropriate access.

Google employs a centralised access management system to control personnel access to production servers, and only provides access to a limited number of authorised personnel. LDAP, Kerberos and a proprietary system utilising digital certificates are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimise the potential for unauthorised account use. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g. login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength. As part of its Insider Risk Program, Google also has controls in place to address unilateral access risks, i.e. the ability of an individual Google employee to perform actions without approval or oversight by another Google employee including reading or modifying user data.

6. Additional information about Google Analytics

- **First party cookies:** The cookies set by Google Analytics for measurement are first party cookies, which means that data subjects' cookie values will be different for each customer (i.e. there is not a single Google Analytics cookie ID that is used across unaffiliated sites that use Google Analytics).
- **No logging of IP-addresses (Google Analytics 4):** Google Analytics 4 does not log or store IP-addresses. Any IP-addresses that arrive in Google Analytics collection servers are discarded before data is transferred to storage logs. As a result, IP-addresses for EU, Swiss and UK user traffic collected in the EU, Switzerland or the UK are not transferred out of region.
- **Secure transmission of Google Analytics JavaScript libraries and measurement data:** Google Analytics by default uses HTTP Strict Transport Security (HSTS), which instructs browsers that support HTTP over SSL (HTTPS) to use that encryption protocol for communication between end users, websites, and Google Analytics servers. Find out more in How Google Analytics secures your web traffic.
- **Customer controls:** Google Analytics offers a set of tools and functionalities to help you control how data is used in Google Analytics, including regional controls for collection of granular location and device data in Google Analytics 4. Find out more in this EU-focused data and privacy page and this Data Controls in Google Analytics 4 page.
- **User controls:** Google Analytics provides privacy controls to users, including a Google Analytics opt-out browser add-on for websites. If users install this add-on, it prevents the Google Analytics JavaScript that is running on websites from sharing information with Google Analytics about visit activity. In addition, Google Analytics 4 provides privacy controls to property editors and admins to disable collection of Google-signals data and/or granular location and device data, both on a per-region basis. If property editors/admins disable either or both of these data collections, then no Google-signal data and/or the relevant location and device data (as applicable) is collected following the change.

Contractual safeguards



1. General

The Google Ads Data Processing Terms, Google Ads Controller-Controller Data Protection Terms and Google Measurement Controller-Controller Data Protection Terms offer strong legal protections, including:

- **Security commitments:** Where Google acts as a data processor, Google commits to implementing and maintaining technical and organisational measures providing an appropriate level of security, as specified in Appendix 2 of the Google Ads Data Processing Terms, and to ensuring appropriate security compliance by its staff. The measures specified in the Google Ads Data Processing Terms include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Google further commits to notifying customers of any data incidents without undue delay and to promptly take steps to secure any affected data. Where Google acts as a data controller, Google contractually commits in the Google Ads Controller-Controller Data Protection Terms to comply with its obligations under European Data Protection Legislation, which include its security obligations in Article 32 of the EU GDPR and in Article 32 of the UK GDPR.
- **Processing in accordance with instructions:** Where Google acts as a data processor, Google commits to processing customer personal data strictly as instructed by the customer.

2. Subprocessing

Google engages third party subprocessors to perform limited activities in connection with Google's advertising and analytics products, such as customer and service support. Information about Google's subprocessors and the services they support is available at privacy.google.com/businesses/subprocessors. Google's engagement of third party subprocessors is subject to strong commitments and protections, which provide sufficient guarantees regarding the implementation of appropriate technical and organisational measures to protect personal data, including:

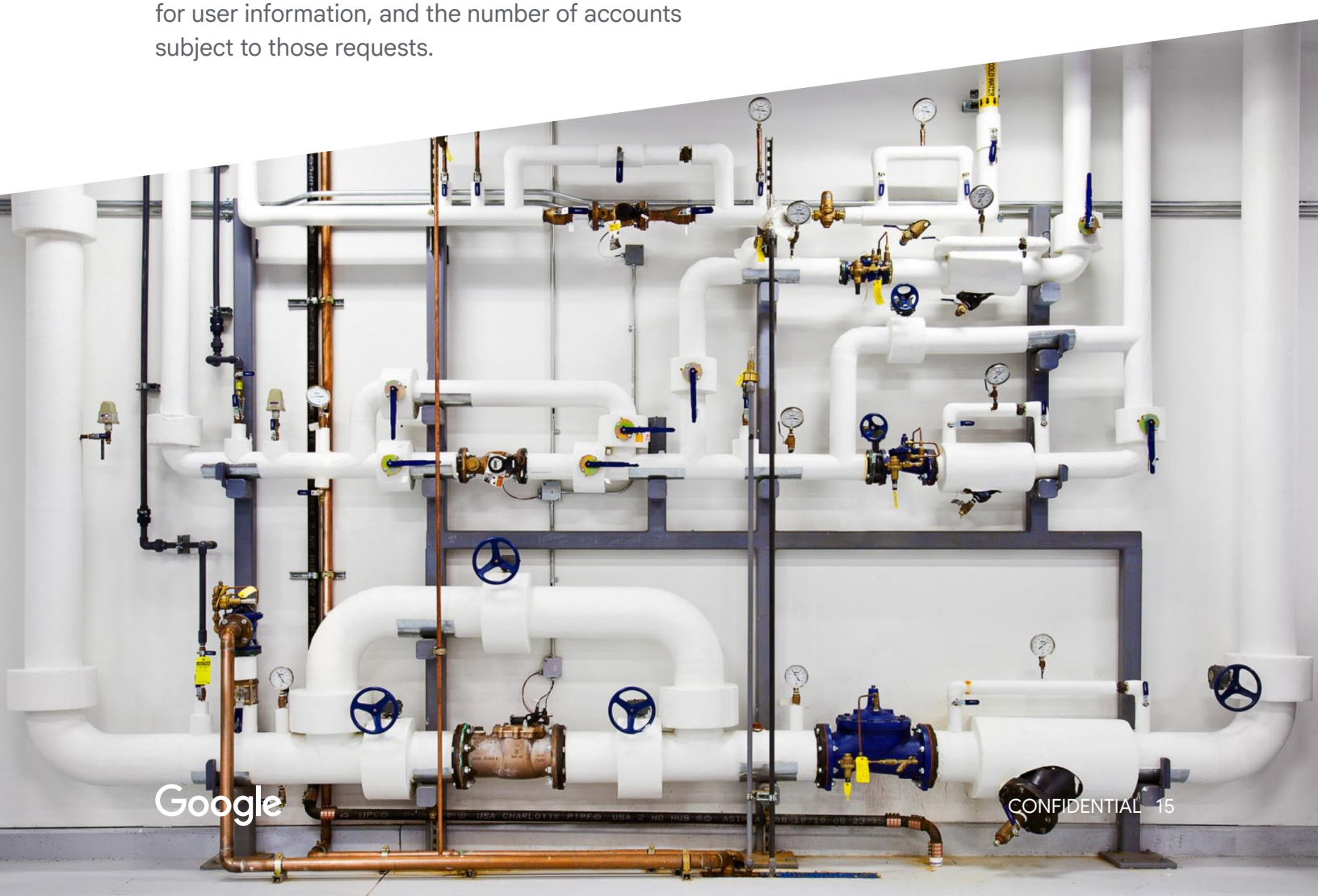
- **Audit:** Before onboarding a subprocessor, Google conducts an audit of the security and privacy practices of the subprocessor to ensure the subprocessor provides a level of security and privacy appropriate to their access to data and the scope of services they are engaged to provide.
- **Contract:** Once Google has assessed the risks presented by the subprocessor, the subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms. In particular, Google will ensure via the contract that the subprocessor accesses user data only if and to the extent required to perform their limited activity and that all access is in accordance with Google's data protection terms. Google remains fully liable for all the activities of its subprocessors and continuously monitors their performance and contractual compliance, including via regular assessments and audits.
- **Limited data:** The majority of personal data processed by third party subprocessors is service-related data (as opposed to end user personal data comprised in user accounts or direct customer data).
- **Opportunity to object:** In accordance with our Google Ads Data Processing Terms, Google will inform customers by email of its engagement of any new third party subprocessor prior to them processing any personal data (including the name and location of the relevant new subprocessor, and the activities it will perform). Should they object, customers can then terminate their agreement with Google for the relevant advertising or analytics service within 90 days of being informed of the new subprocessor's engagement.
- **Restrictions on sub-sub-processing:** Subprocessors are contractually prohibited from subcontracting any part of their services to a third party (e.g. a sub-subprocessor) without Google's prior written consent.
- **International data transfers:** Subprocessors must provide at least the same level of protection for any personal data they process as is required by any applicable data protection framework adopted by Google, which includes the DPF where personal data is transferred to a subprocessor in accordance with the DPF's onward transfer principles.

Organisational safeguards

1. Transparency

At Google, 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 user data. We understand that a big part of being transparent is providing information on when requests are being made for access to data.

In our Transparency Reports, we share information about how the policies and actions of governments affect privacy, security and access to data. Twice a year, we report the number of requests made by governments for user information, and the number of accounts subject to those requests.



2. Government requests for data

If a government seeks Google's advertising and analytics personal data during the course of an investigation, a dedicated team of Google lawyers and specially trained personnel will carefully review the request to verify that it is lawful, proportionate and complies with Google's policies.

Generally speaking, for us to produce any data, the request must be made in writing, signed by an authorised official of the requesting agency and issued under an appropriate law. Our legal team rejects requests that are invalid and pushes back when we believe the request is overly broad.

We will notify a customer before any of their information is disclosed unless such notification is prohibited by law or the request involves an emergency, such as an imminent threat to life. We will provide delayed notice to the customer if a legal prohibition on prior notification is lifted, such as when a statutory or court ordered disclosure prohibition period has expired.

To learn more about how we handle government requests for data, please see:

- Transparency Report
- Policies & Procedures
- FAQs on United States national security requests

3. Internal audits and reviews

We conduct regular internal audits on matters relating to international transfers. We also review our internal policies to assess the suitability of the supplementary measures we have implemented.

Third party certifications and compliance offerings

Google has earned ISO 27001 certification for a number of Google advertising and analytics products, which provides independent accreditation of their systems, applications, people, technology, processes and data centres. Customers with a Google account representative may request our ISO 27001 Statement of Applicability (SOA) from their representative. In addition, Google will allow customers or a third party auditor appointed by a customer to conduct audits (including inspections) to verify Google's compliance with its obligations in accordance with the terms outlined in the Contractual safeguards section of this paper above.

Summary

In addition to Google and/or its affiliates' adoption of, or certification under, any legal frameworks or solutions that enable the lawful transfer of personal information to a third country in accordance with European Data Protection Legislation, we are committed to providing and continuing to advance technical, contractual, and organisational safeguards that will support Google's advertising and analytics customers in assessing the risk of international data transfers. We firmly believe that the transfers of personal data outside the EEA, Switzerland or the UK as discussed in this paper are in compliance with the strict requirements imposed by European Data Protection Legislation regarding international data transfers.

We hope this paper is helpful for customers conducting compliance risk assessments, but encourage all customers to consult with their legal counsel as this paper should not be used as a substitute for legal advice.