# Safeguarding your data

This article summarizes Google Analytics' data practices and commitment to protecting the confidentiality and security of data. Visitors to sites or apps using Google Analytics (aka "users") may learn about our end user controls.

Site or app owners using Google Analytics (aka "customers") may find this a useful resource, particularly if they are businesses affected by the European Economic Area's General Data Protection Regulation. See also the Google privacy policy and Google's site for customers and partners.

## Information for Visitors of Sites and Apps Using Google Analytics

### Our privacy policy

At Google, we are keenly aware of the trust you place in us and our responsibility to keep your privacy and data secure. As part of this responsibility, we let you know what information we collect when you use our products and services, why we collect it, and how we use it to improve your experience. The Google privacy policy & principles describes how we treat personal information when you use Google's products and services, including Google Analytics.

### Google Analytics cookies and identifiers

Google Analytics mainly uses first-party cookies to report on visitor (aka. user) interactions on Google Analytics customers' websites. Users may disable cookies or delete any individual cookie. Learn more

In addition, Google Analytics supports an optional browser add-on that - once installed and enabled - disables measurement by Google Analytics for any site a user visits. Note that this add-on only disables Google Analytics measurement.

Where a site or app uses Google Analytics for Apps or the Google Analytics for Firebase SDKs, Google Analytics collects an app-instance identifier — a randomly generated number that identifies a unique installation of an App. Whenever a user resets their Advertising Identifier (Advertising ID on Android, and ID for Advertisers on iOS), the app-instance identifier is also reset.

Where sites or apps have implemented Google Analytics with other Google Advertising products, like Google Ads, additional advertising identifiers may be collected. Users can opt-out of this feature and manage their settings for this cookie using the Ads Settings. Learn more

Google Analytics also collects Internet Protocol (IP) addresses to provide and protect the security of the service, and to give website owners a sense of which country, state, or city in the world their users come from (also known as "IP geolocation"). Google Analytics provides a method to mask IPs that are collected (detailed below) but note that website owners have access to their users' IP addresses even if the website owners do not use Google Analytics.

## Information for Sites and Apps Using Google Analytics

### Google as a data processor

Google operates as a data processor for Google Analytics. This is reflected in our Ads Data Processing Terms, which are available to all Google Analytics customers with direct contracts with Google. Learn more

Google Analytics is a data processor under GDPR because Google Analytics collects and processes data on behalf of our clients, pursuant to their instructions. Our customers are data controllers who retain full rights over the collection, access, retention, and deletion of their data at any time. Google's use of data is controlled by the terms of its contract with Google Analytics customers and any settings enabled by customers through the user interface of our product.

### Data Collected by Google Analytics

#### First-party Cookies

Google Analytics collects first-party cookies, data related to the device/browser, IP address and on-site/app activities to measure and report statistics about user interactions on the websites and/or apps that use Google Analytics. Customers may customize cookies and the data collected with features like cookie settings, User-ID, Data Import, and Measurement Protocol. Learn more

Google Analytics customers who have for instance, enabled the analytics.js or gtag.js collection method can control whether or not they use cookies to store a pseudonymous or random client identifier. If the customer decides to set a cookie, the information stored in the local first-party cookie is reduced to a random identifier (e.g., 12345.67890).

For customers who use the Google Analytics for Apps SDK, we collect an App Instance Identifier, which is a number that is randomly generated when the user installs an app for the first time.

and used to enable features like Remarketing on the Google Display Network. These features are subject to the users' Ads Settings, the Policy requirements for Google Analytics Advertising Features and Google's EU User Consent policy, which requires customers to obtain consent for cookies where legally required—including consent for personalized ads. For more information about how Google uses advertising cookies, visit the Google Advertising Privacy FAQ. It is possible to implement Google Analytics without affecting normal data collection where Advertising features are disabled until consent is obtained.

### IP Address

Google Analytics uses IP addresses to derive the geolocation of a visitor, and to protect the service and provide security to our customers. Customers may apply IP masking so that Google Analytics uses only a portion of an IP address collected, rather than the entire address. In addition, customers can override IPs at will using our IP Override feature.

### PII Prohibition

Our contracts prohibit customers from sending Personally Identifiable Information to Google Analytics. Customers should follow these Best Practices to ensure PII is not sent to Google Analytics.

## What is the data used for?

Google uses Google Analytics data to provide the Google Analytics measurement service to customers. Identifiers such as cookies and app instance IDs are used to measure user interactions with a customer's sites and/or apps, while IP addresses are used to provide and protect the security of the service, and to give the customer a sense of where in the world their users come from.

## Data access

We do not share Google Analytics data without the customer's authorization (including via settings in the product user interface), or as otherwise expressly permitted under the terms of their Google Analytics agreement, except in limited circumstances when required by law.

Customers may control their own access to data in their Analytics accounts or properties by configuring view and edit permissions for employees or other representatives who may login to their Analytics account. Learn more

Security-dedicated engineering teams at Google guard against external threats to data. Internal access to data (e.g., by employees) is limited by strict access controls (both internal policy controls and automated technical controls such as authentication, SSL, and security logs) to only those with a business need to access it.

### Product linking summary

Where customers link their Analytics property to another Google product or service account ("Integration Partner"), certain data from that Analytics property may be accessed and exported into the linked account. Once data is exported through a linking integration, it becomes subject to the Integration Partner's terms and policies. Learn more

Note that once data is sent to an Integration Partner, that the data sent is subject to the terms of that Integration Partner and that Google Analytics no longer maintains access or control over that data.

Customers may review and manage their product integration linkings at any time within the Analytics product linking summary user interface.

### Data Sharing

Google Analytics provides several data sharing settings to customers, through which customers may customize how data collected using an Analytics data collection method (like the JavaScript code, mobile SDKs, and the Measurement Protocol) may be accessed and used by Google according to customer preferences. Note that these settings only apply to data collected from websites, mobile apps, and other digital devices using Analytics; they do not apply to data relating to a customer's use of Analytics, such as the number of properties and which additional features are configured. Regardless of a customer's data sharing settings, Analytics data may also be used only insofar as necessary to maintain and protect the Analytics service. Learn more

## Data Controls for retention, deletion and portability

### Data Retention

With the Data Retention controls, customers can limit or expand the duration for which their user-level and event-level data is stored in Google Analytics servers. All customers should review their Data Retention settings and ensure the appropriate retention is selected.

### User Deletion

Customers may delete a single user's data from Google Analytics by passing a single user identifier to the Google Analytics User Deletion API.

### User-level Data Access and Portability

Customers may pull event information for any given user identifier via our User Explorer report. This feature enables customers to analyze and export event level data for a single user. In addition, our 360 customers may integrate with BigQuery to create a full export of all event data associated with their users in a single queryable repository.

## Certifications

### EU Privacy Shield

The U.S. Department of Commerce has approved Google's certification to the Privacy Shield as fully compliant. View our Privacy Shield certification.

### ISO 27001

Google has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centers serving a number of Google products, including Google Analytics. Download our certificate here (PDF) or learn more about ISO 27001.

### Information security

In web-based computing, security of both data and applications is critical. Google dedicates significant resources towards securing applications and data handling to prevent unauthorized access to data.

Data is stored in an encoded format optimized for performance, rather than stored in a traditional file system or database manner. Data is dispersed across a number of physical and logical volumes for redundancy and expedient access, thereby obfuscating it from tampering.

Google applications run in a multi-tenant, distributed environment. Rather than segregating each customer's data onto a single machine or set of machines, data from all Google users (consumers, business, and even Google's own data) is distributed among a shared infrastructure composed of Google's many homogeneous machines and located in Google's data centers.

In addition, Google Analytics ensures secure transmission of its 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 all communication between end users, websites, and Google Analytics servers. Learn more

### Operational security and disaster recovery

To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, Google implements a comprehensive disaster-recovery program at all of its data centers. This program includes multiple components to eliminate single points of failure, including the following:

**Data replication** To help ensure availability in the event of a disaster, Google Analytics data stored in Google's distributed file system is replicated to separate systems in different data centers.

**Geographical distribution of data centers** Google operates a geographically distributed set of data centers that is designed to maintain service continuity in the event of a disaster or other incident in a single region.

**Resilient and redundant infrastructure** Google's computing clusters are designed with resiliency and redundancy in mind, helping minimize single points of failure and the impact of common equipment failures and environmental risks.

**Continuity plan in the event of disaster** In addition to the redundancy of data and regionally disparate data centers, Google also has a business-continuity plan for its headquarters in Mountain View, CA. This plan accounts for major disasters, such as a seismic event or a public-health crisis, and it assumes people and services may be unavailable for up to 30 days. This plan is designed to enable continued operations of our services for our customers.

Data privacy and security

- **Safeguarding your data**
- Data sharing settings
- Google Analytics opt-out browser add-on
- IP Anonymization in Analytics
- IP masking
- Policy requirements for Google Analytics Advertising Features
- Security and privacy in Universal Analytics
- We use our own products
- Google Analytics and the EU-US Privacy Shield
- Data Processing Terms
- Data retention
- ISO 27001 Certification
- Product linking summary
- Account setup with additional privacy features
- Best practices to avoid sending Personally Identifiable Information (PII)

Become a Power User

Check out *Google Analytics for Power Users* on Analytics Academy.

Sign Up Today



English