

Data Controls in Google Analytics (Universal Analytics) Guide

Rising consumer expectations and changing industry regulations have set higher standards for user privacy and data protection. This has led many businesses to revisit how they are managing data in their Google Analytics accounts.

Customers are the controllers of the data that they collect through Google Analytics. To help businesses manage this data, Analytics provides a variety of features and customer controls that govern how data is collected, stored, and used—all of which can be adjusted at any time.

The purpose of this document is to offer a central guide to Google Analytics' data practices and controls for protecting the confidentiality and security of data (information publicly available in our Google Analytics Help Center).

This document is not legal guidance. Google does not provide legal advice to customers but shares product functionality that may help customers comply based on their own assessment of local laws and regulations.

Data Collection

Note: 360 and free versions share the same technical infrastructure, data collection principles apply to both.

Customers may customize data collection by using the following Data Controls (if you want to learn more on how Google Analytics collects Data, [you can visit this page](#)):

Features	Available Data Controls	Impact if altered or redacted
Consent Mode	Consent Mode (beta) allows you to adjust how your Google tags behave based on the consent status of your users. Google's tags will dynamically adapt, only utilizing measurement tools for the specified purposes when consent has been given by the user. Instructions for Global site tag (gtag.js) Instructions for Google Tag Manager	When consent for ad storage or analytics storage is denied, the associated Google measurement functions deployed via global site tags (gtag.js) or Google Tag Manager will adjust their behavior accordingly. For example, when analytics_storage=denied, Google Analytics will not read or write first-party analytics cookies . When ad_storage=denied, Google Analytics will not read or write Google Ads cookies, and Google signals features will not accumulate

		data for this traffic.
Server-side tagging with Google Tag Manager	Server-side tagging allows you to carry out a variety of functions before your data is sent to its destination (e.g., Google Analytics). Server-side tagging has built in and customizable features to redact or anonymize data in a local customer owned environment prior to sharing it with end destinations.	Depending on how you choose to customize your implementation, there are a variety of ways that your data or functionality may be impacted. Although this document is about Universal Analytics, it's worth noting that Google signals for Google Analytics 4 will not work with server-side tagging. Furthermore, Google Analytics 4 audiences won't work for Google Ads remarketing.
CustomTask	CustomTask lets you process the client-side data collection before any data is sent. You could use it to dynamically add custom dimensions to requests, to duplicate a request to other measurement IDs, to prevent duplicate transactions, etc.	Depending on how you choose to use CustomTask, there are a variety of ways that your data or functionality may be impacted.
Measurement Protocol	Measurement Protocol allows you to send data to Google Analytics. The Measurement Protocol defines how to construct the hits and how to send them to Analytics.	While using Measurement Protocol, you manually build data collection hits.
Data type	Available Data Controls	Impact if altered or redacted
Client ID	You have control over the Client ID value that will be used by Google Analytics. • Client ID field reference • Consent Mode allows you to adjust how your Google tags behave based on the consent status of your users.	If the client ID is different between the cookie value and the value used in Google Analytics, you will not be able to use audience remarketing functionality. Please note that the value used in Google Analytics is the one being used in case of data deletion or data portability. Google Analytics will not read or write first-party analytics cookies when analytics_storage=denied.
Advertising Identifiers	When Google Signals are enabled (optional feature), Google Analytics collects visitation information and associates it with Google information from accounts of signed-in users who have consented to this association for the purpose of ads personalization. It is used to provide aggregated and anonymized insights into your users' cross device behaviors. If you activate Google signals, the controls to enable Remarketing and Advertising Reporting Features are replaced by the Google-signals control.	If you deactivate Google signals, Analytics stops collecting Demographics and Interests information. When disabled, the following settings and features are also disabled: • Remarketing with Google Analytics • Advertising Reporting Features • Cross Device reports If you deactivate Advertising Reporting Features, Analytics stops collecting Demographics and Interests information.

	When you enable Remarketing and Advertising Reporting Features for a web property, Analytics collects the information it normally does, as well as Google advertising cookies when those cookies are present. Controls available: - At property level with feature Google Signals on/off toggle - At user level with gtag.js function, analytics.js function, or GTM template option Advanced settings (regional control) Advertising reporting features on/off toggle	When disabled, the following settings and features are also disabled: - Remarketing with Google Analytics - Advertising Reporting Features
User ID	A User ID is a unique, persistent, and non-personally identifiable ID string that represents a user. It enables the analysis of groups of sessions across devices. You must first enable it in your Analytics account and then implement it in your tracking code. You have control over the User ID value that will be used by Google Analytics. Set up User ID	If User-ID is turned off: - No User-ID Views - No cross-device or cross-platform ads personalization
Transaction ID	You have control over the Transaction ID value that will be used by Google Analytics. Transaction ID field reference	If altered, the same-session transaction ID deduplication process might not work.
IP address	Location data is inferred from the visitor IP address. Available controls are: IP anonymization feature for IP truncation. IP override field for measurement protocol - Redact visitor IP address using Server-side measurement (Server Side GTM)	If you anonymize (truncate) IP addresses, location data will be less accurate. If you redact IP addresses using Measurement Protocol or server-side GTM, Google Analytics would not be able to automatically supply you with location data in reports.
HTTP Headers data (e.g. metadata)	Google Analytics uses HTTP Headers Data to detect some dimensions such as browser, operating system, device information, etc. You have control if you prefer to send another User Agent string that will be used for processing using UserAgent override	Inferred browser and device dimensions from metadata will need to be supplied explicitly to have values in your GA reports.

Cookie parameters	Google Analytics's cookies default behavior can be customized. For example, you can define a prefix name, restrict the cookie to a specific subdomain, set up an expiration date and disable its auto-update. • Cookie parameters	Altering cookies could result in less reliable attribution data.
PII Data	Google policies mandate that no data be passed to Google that Google could use or recognize as personally identifiable information (PII). Here are some best practices to avoid sending PII.	N/A

Data Usage

Usage Control	Available Data Controls	Impacts if altered or redacted
Google Signals	Controls for activating/deactivating Google Signals are details in the Data Collection table above. In addition, data derived from Google Signals can be controlled or prevented from use in ads personalization. See the sections on Consent Mode and Ads Personalization for more details.	When disabled, the following settings and features are also disabled: • Remarketing with Google Analytics • Advertising Reporting Features • Demographics and Interests Reports • Cross Device reports
Remarketing and Advertising Reporting Features	When you enable these features, you can create remarketing audiences and share them with your advertising accounts. You can also see data in the Demographics and Interests reports, see GDN Impression data in the Multi-Channel Funnel reports, and can take advantage of Google Marketing Platform integrations. Note: If you activate Google signals, the controls to enable Remarketing and Advertising Reporting Features are replaced by the Google-signals control. Controls: • Google Signals on/off toggle or Advertising reporting features on/off toggle • Advanced settings (regional control)	When remarketing features are disabled, you will not be able to do remarketing or benefit from some advanced features like cross-device analysis. You will also experience loss of some data from GMP integrations including DV360 and CM view-through reporting.
Ads	Customers may choose to disable Advertising	If you disable ads personalization for a given

Personalization	Personalization for data collected from their entire property, or to disable it for individual events or users (for apps, websites, and measurement protocol). Controls: • Control by region • Disable advertising features (gtag.js) • Disable advertising features (analytics.js) • Event controls in Measurement Protocol • Consent Mode	user/property/region, then all events collected from those locations will be marked as not eligible for use for ads personalization (NPA). This means that any conversions from these users will be marked as not for use for ads personalization even when exported to your linked ads accounts. In addition, any end user coming from a disabled location will not be added to any lists that may be exported to your linked ads accounts, although lists that have already been exported will not be affected. All events collected for the property, and any audiences based on that data, are still available within Analytics for use in reports, Analysis, and audience building.
Data sharing settings	Customers may choose to share their Google Analytics data for various purposes (Google Product & Services, Benchmarking, Account Specialists, Technical Support) Any data collected and used by Google under the “Google products & services” setting is subject to the Controller-Controller Data Protection terms and Google is, for GDPR purposes, an independent controller of such data. Regardless of your data sharing settings, your Analytics data may also be used only insofar as necessary to maintain and protect the Analytics service.	N/A

Data Storage

Setting	Definition	Available Data Controls
Data Retention	The Google Analytics Data Retention controls give you the ability to set the amount of time before user-level and event-level data stored by Google Analytics is automatically deleted from Analytics servers. The retention period applies to user-level and event-level data associated with cookies, user-identifiers (e.g., User-ID), and advertising identifiers (e.g., DoubleClick cookies, Android’s Advertising ID [AAID or AdID], Apple’s Identifier for Advertisers [IDFA]).	For Universal Analytics properties, the setting applies to user-level and event-level data. You can choose: 14 months 26 months 38 months 50 months - Do not automatically expire

Data Portability

Portability Option	Available Data Controls
User-level Data Access and Portability	For Universal Analytics properties, you can pull event information for any given user identifier via the User Explorer report or the User Activity API . These features allow you to analyze and export event level data for a single user identifier.
BigQuery Export	360 customers can integrate with BigQuery to create a full export of all event data associated with their users in a single queryable repository.

Data Deletion

Data Erasure Option	Available Data Controls	Impacts if altered or disabled
Data Deletion Requests	If you need to delete data from the Analytics servers for any reason, then you can use the Data Deletion Requests feature to issue a request for its removal.	You can select All to delete all data for the property, or select one or more individual fields (e.g., URL*, Page Title, Event Category).
User Data 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 or via our User Explorer report .	Once deletion is requested, data associated with this user identifier will be removed from the Individual User Report within 72 hours, and then deleted from Analytics servers during the next deletion process. Reports based on previously aggregated data (for example, user counts in the Audience Overview report) will not be affected.