[GA4] Google Analytics Data Controls 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 and Google's tagging solutions provide a variety of features and controls that allow customers to 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.

Note: Server-side tagging with Google Tag Manager- While this document outlines options for controlling or modifying data via server-side tagging, please note that some modifications may significantly impact key use cases. Also note that app data streams and some features–such as Google signals–are not yet supported for server-side implementations of GA4. We continue to explore new options for server-side implementations.

Data Collection

Note: 360 and free versions share the same technical infrastructure and 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	Google Analytics support	Server-side Tagging support	Feature details

Consent Mode	Consent Mode- 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	Consent Mode is natively supported when using a client-side GA4 config tag to route data to your server-container. Server-side Google tags will respect the consent state captured by the client-side tag without any additional configuration server-side. Server-side Tagging supports both Basic and Advanced consent mode implementations.	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.
Measurement Protocol	Measurement Protocol is a server-to-server method to send data to Google Analytics . The Measurement Protocol defines how to construct the events and how to send them to Analytics. Notably, this makes it easy to measure interactions that happen server-to-server and offline.	You can utilize Measurement Protocol by sending data to your server-container in the Measurement Protocol schema and utilizing the Measurement Protocol Client in your server-container. .	The purpose of measurement protocol in GA4 is to augment existing events collected via gtag, GTM, or the Google Analytics for Firebase SDK. Some event and parameter names are reserved for use via automatic collection and cannot be sent through the measurement protocol. So while it is possible to send events to Google Analytics solely with measurement protocol, only partial reporting may be available.

Data type	Native Analytics Data Controls	Server-Side Tagging 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 configuration field • Consent Mode allows you to adjust how your Google tags behave based on the consent	You have the control to modify or remove the Client ID value in Server-Side GTM with a Custom Variable and Sandboxed JavaScript.	If the client ID is different between the cookie value and the value used in Google Analytics (including when client ID is not present), you will not be able to use audience remarketing functionality. Modification of client ID may

	status of your users.		reduce accuracy of user/visitor counts. If client ID is removed, Analytics may begin to report on multiple users as a single user and deflate user counts. If client ID is changed, Analytics may begin to recognize a single user as multiple users and inflate user counts. 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 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 web data streams, Google Analytics collects the information it normally does, as well as Google advertising cookies when those cookies are present. For app streams, Google Analytics collects DSID for Android and identifier for advertisers (IDFA) for iOS. Controls available: • At property and regional level with Google Signals admin settings on/off toggle • At user level with gtag.js function GTM template option	*Server-side tagging does not yet support Google signals or collect advertising identifiers. There are plans to launch Google Signals support later in 2023.*	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 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	User ID can be transmitted to Server-Side GTM and then utilized by your server-side GA4 tags once User ID is configured in your web container (Tag Manager and User ID). Server-Side GTM can be used to redact or modify User ID if required with a Custom Variable or with the parameters to drop/add section in the server-side GA 4 tag.	If User-ID is not collected by Analytics: • No User-ID-based reporting when Reporting Identity is set to Blended Views • If a unique identifier is not available, you may experience inflated user counts, as the same visitor on a different browser or device would be recognized and reported as a new unique user by Analytics • No cross-device or cross-platform ads personalization
Granular Location & Device	You have control over the granular location and device data that is collected about your visitors. When collection is disabled, city-level location data as well as certain device-level metadata is redacted prior to collection in Google Analytics' servers. Controls available: Disable collection at property and region level with granular location and device data collection setting	Server-side GTM supports the location and device controls as configured in your Google Analytics property. Server-side GA4 tags will automatically respect your location and device data settings.	If you deactivate granular location and device data collection, Analytics stops collecting this information and it will not be available in reporting and related Analytics features. • City • Latitude (of city) • Longitude (of city) • Browser minor version • Browser User-Agent string • Device brand • Device model • Device name • Operating system minor version • Platform minor version • Screen resolution
Referrer and **URL Parameters**	You have control over the page referrer and URL parameter values that are used by Google Analytics. • Page referrer • URL parameters	You have the control to modify or redact the referrer and UTM parameter values in Server-Side GTM with a Custom Variable and Sandboxed JavaScript.	Removal of URL parameters or referrer could impact the accuracy of conversions and traffic source attribution. For example, modification of UTM parameters could lead to misattributed traffic sources.

Transaction ID	You have control over the Transaction ID value that will be used by Google Analytics. Transaction ID field reference	Server-Side GTM can be used to redact or modify Transaction ID if required with a Custom Variable or/and with the parameters to drop/add section in the server-side GA 4 tag.	If altered, the same-session transaction ID deduplication process might not work and may result in inflated or inaccurate transaction reporting.
IP address	Location data is inferred from the visitor IP address. IP addresses are immediately discarded after location data is inferred and IP address data is never logged or stored on Analytics databases.	The GA4 server tag in Server-Side GTM allows you to redact IP addresses in your server container. If the option to redact is not selected, the IP address will automatically be masked by your GA4 server-tag.	Location data is not collected by Analytics (GA4). 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. Spam and bot detection will also be impacted when IP address is not sent to Analytics from server-side GTM.
Cookie parameters	Google Analytics' 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. Visit this dev page for more information on available Cookie parameters. Cookie parameters Google Analytics' cookie expiration period can be overridden by changing the default cookie settings.	Server-Side GTM allows you to customize Google Analytics' cookie behavior. Similar to the client-side GA4 tag, Server-Side GTM allows you to adjust the prefix name, restrict a cookie to a specific subdomain, set up an expiration date and disable auto update. Additionally, Server-Side GTM supports 'Server Managed cookies', which are only accessible via HTTP. You can read more about Cookie parameters available in Server-Side GTM on this developer page. There is also more general guidance on this Tag Manager developer page.	Altering cookies could result in less reliable attribution data.
Personally Identifiable Information (PII)	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	N/A

Data Usage

Usage Control	Available Data Controls	Impacts if altered or redacted
Google signals	Google signals is an optional feature that can be enabled to provide demographics and interest data, cross-platform reporting, remarketing audiences, and ads personalization (when ads personalization is also enabled). Controls available: • At property and regional level with the Google Signals admin settings on/off toggle *Google signals are not supported for Analytics data that are sent to Analytics through Measurement Protocol or server-side tagging.	When disabled, the following settings and features are also disabled: • Remarketing with Google Analytics • Advertising Reporting Features • Demographics and Interests Reports • Cross Device reports
Ads Personalization	Customers may choose to disable Advertising 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) • Event controls in Measurement Protocol • Consent Mode	If you disable ads personalization for a given 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	In order to benefit from Predictive Metrics, you must enable the Modeling contributions & business insights data sharing setting.

	necessary to maintain and protect the Analytics service.	

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 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 Google Analytics 4 properties, the setting applies to event-level data. You can choose: 2 months 14 months 26 months (360 only) 38 months (360 only) 50 months (360 only)

Data Portability

Portability Option	Available Data Controls
User-level Data Access and Portability	For Google Analytics 4 properties, you can pull event information for any given user identifier via User Explorer. This allows you to analyze and export event level data for a single user identifier.
BigQuery Export	GA4 customers can integrate with BigQuery to create a full export of all event data associated with their users to 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	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

	to the Google Analytics User Deletion API or via our User Explorer report.	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.