Tableau products and the General Data Protection Regulation

Table of contents

Introduction

This white paper discusses considerations of which Tableau users subject to the European Union (EU) General Data Protection Regulation (GDPR) need to be aware if you are using Tableau products to process personal data as defined by the GDPR. It covers personal data that Tableau processes as part of Tableau Server, Tableau Online, and Tableau Public user accounts. Personal data that Tableau processes as part of product registration is covered under the terms of your license or subscription agreement and the Tableau Software Privacy Policy.

Disclaimer

As with most regulations and laws, interpretations of how to apply GDPR in practice may vary, especially early in its implementation. Our view of the impact of GDPR on Tableau customers is based on our current understanding of the law and how to apply it in practice. This position may change over time as standard practices and expectations become clearer. Note that data subjects have many rights under GDPR, not all of which may be relevant to Tableau products.

Tableau provides this white paper for informational purposes only, not for the purposes of legal advice or as comprehensive education on this complex subject. We encourage you to work with appropriately qualified legal professionals to determine how the GDPR applies to your specific situation and how best to maintain compliance.

Overview of the GDPR

The GDPR (General Data Protection Regulation) is a regulation by which the European Union strengthens and unifies data protection for all individuals in the EU. It applies to all organizations doing business with individuals in the EU, whether the organizations are based in the EU or not. It also addresses the export of personal data outside the EU.

The regulation specifies a number of rights for individuals (“data subjects”) as well as responsibilities both for organizations that collect the personal data of data subjects (“data controllers”) and organizations that process data on behalf of data controllers (“data processors”). A data subject’s personal data includes information such as name, phone number, email address, birth date, IP address (if traceable to an individual), and so on. Sensitive personal data may include information about an individual’s health, ethnicity, or religion. Key elements of the GDPR include:

- Strengthened personal privacy rights for individuals
- Increased responsibility for protection of personal data
- Mandatory reporting of breaches of personal data
- Rules for transfer of personal data outside of the EU
- Right to request removal of personal data
- Penalties for non-compliance

Definitions

In the context of this document, following are the definitions of key concepts and roles under the GDPR.

Controller

"The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

Personal Data

"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Processor

"A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

Processing

"Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

Recipient

"A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing."

Roles and Responsibilities

Depending on your use of Tableau products, responsibility for complying with GDPR may be shared between Tableau and you. The "Personal Data in Tableau" section below describes the roles for different types of personal data depending on the specific Tableau product you are using.

The GDPR and Tableau Products

The Tableau Platform contains many capabilities and features that will enable your organization to achieve compliance with the GDPR when using Tableau to process personal data. The first step in assessing the implications of GDPR for your use of Tableau is to understand where personal data may be found.

Understanding the Location of Personal Data in Tableau

Personal data in Tableau takes multiple forms and may be found in multiple locations within the Tableau Platform. The two categories of personal data that Tableau products may have access to are:

1. Personal data in data sources (i.e. your data)

2. Personal data that is part of Tableau Server, Tableau Online, or Tableau Public user accounts

Personal Data in Data Sources

Data sources (e.g. files, databases) to which you connect Tableau Desktop, Tableau Prep, Tableau Server, Tableau Online, or Tableau Public may contain personal data subject to the GDPR. You are responsible for identifying personal data within your data sources.

If you choose to extract data from a data source, then that customer data will also reside in a Tableau data extract (.hyper or .tde file) on either a client computer (in the case of Tableau Desktop) or in Tableau Server, Tableau Online, or Tableau Public.

Tableau Prep can produce data extract (.hyper or .tde) or comma-separated value (.csv) files as part of a flow. If the data source(s) used in a flow contain personal data, these files may also contain personal data.

Also note that Tableau packaged workbook (.twbx), Tableau packaged data source (.tdsx), and Tableau Prep packaged flow (.tflx) files can contain copies of file-based data sources and extract files that may contain personal data.

Additionally, Tableau Desktop, Tableau Server, Tableau Online, and Tableau Public employ data caching techniques to accelerate performance. These caches temporarily store data from data sources queries in memory or on disk. Tableau Desktop stores cached results in workbook (.twb) and packaged workbook (.twbx) files as well as in a query cache. Tableau Desktop users can clear this query cache. Tableau Server administrators have some control of this caching behavior and the ability to clear the cache.

For Tableau Desktop, Tableau Server, Tableau Online, and Tableau Public, you are the controller of personal data found in your data sources. For Tableau Online and Tableau Public, Tableau is the processor of this personal data.

Personal Data in User Accounts

Tableau Server, Tableau Online, and Tableau Public user accounts also contain personal data subject to the GDPR. This data includes name, email address, location, and IP address and is stored in an internal PostgreSQL database. These products also log records of a user's historical activity to the PostgreSQL database and log files. Tableau Server administrators have some control of this logging behavior and the ability to clear historical logs.

Fulfilling Data Controller Responsibilities

As a controller of personal data, you have certain responsibilities under the GDPR. Tableau products have capabilities that allow you to fulfill these responsibilities. To comply with the GDPR, you may need to perform the following actions involving Tableau:

- Identify personal data
- Secure personal data
- Govern access to and use of personal data
- Facilitate the rights of data subjects

Identify Personal Data

Any plan for compliance with the GDPR should include a thorough identification of all personal data and where it is located. To determine whether Tableau workbooks or data sources contain personal data, you can employ the search capabilities in the Data side bar to look for the use of fields that contain personal data.

If you have a large number of workbooks to analyze, the TWB Auditor available on the Tableau Community is a useful tool for determining which data sources and fields are used in multiple workbooks.

Secure Personal Data

Controllers and processors are responsible for keeping personal data protected and secure. As such, you should follow the best practices outlined in the Tableau Server Security Hardening Checklist for Tableau Server installations that have access to personal data. Tableau follows similar security best practices in Tableau Online and Tableau Public.

You can find more information about Tableau Software security practices and other resources on the Security page at tableau.com.

Govern Access to and Use of Personal Data

Tableau users should ensure that only those individuals who have the need to access personal data are able to do so. The rich permissions settings on Tableau Server and Tableau Online allow control of which locations and assets users are able to access, such as sites, workbooks, worksheets, and data sources. Tableau Desktop additionally offers user-based filtering to restrict access to data at the row level.

Facilitate the Rights of Data Subjects

Under the GDPR, data subjects have the right to request that controllers perform certain actions related to their personal data. The relevant rights that Tableau products can help you facilitate are:

- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Data Portability

Please see the Tableau Software Privacy Policy for information about how to exercise these rights regarding any personal data that Tableau processes as part of Tableau Online and Tableau Public user accounts.

Right of Access

Under GDPR data subjects have a right to request information about the personal data that a controller is processing, including a copy of the data itself. If you are using Tableau to analyze personal data in a data source, you can use the data exporting capabilities of Tableau Desktop, Tableau Server, Tableau Online, or Tableau Public to download that data into a CSV file.

Right to Rectification

A data subject has a right to request rectification of inaccurate personal data concerning him or her. If you update personal data in a data source for which there is an extract, you must perform a full extract refresh (not an incremental refresh) to remove the data from the extract. Scheduling regular extract refreshes on Tableau Server and Tableau Online can ensure that extracts are automatically refreshed in a reasonable timeframe after changes to the data source.

Right to Erasure

Under the GDPR, data subjects have a right to removal of their personal data under certain circumstances. A data subject can make a written request to a data controller or data processor to remove their personal data from the organization’s systems. It is your obligation to delete data if you get such a request; however, Tableau will provide reasonable assistance, primarily in helping the customer understand the tools and processes they can use to remove data.

Personal Data in Data Sources

If you delete personal data from a data source for which there is an extract, you must perform a full extract refresh (not an incremental refresh) to remove the data from the extract. Scheduling regular extract refreshes on Tableau Server and Tableau Online can ensure that extracts are automatically refreshed in a reasonable timeframe after changes to the data source.

If a Tableau Prep flow produces a file (.hyper, .tde, or .csv) file that contains personal data, you must rerun the flow if you delete data from any underlying data source(s).

As described previously, Tableau Desktop, Tableau Server, Tableau Online, and Tableau Public cache data from data sources to accelerate performance. You can clear the query cache for Tableau Desktop. By default, Tableau Server caches data only for a limited amount of time, up to about one week. You can configure caching behavior for workbooks and data connections as well as manually clear the cache if you would like more granular control.

Tableau Online and Tableau Public also cache data for up to about one week.

Personal Data in User Accounts

Deleting a user account from Tableau Server, Tableau Online, or Tableau Public removes the primary user data from the underlying PostgreSQL databases.

Tableau Server automatically removes historical logs after a period of time. Tableau Server administrators can configure this logging behavior to turn off historical logging altogether or automatically delete logs in a different timeframe. Additionally, Tableau Server administrators can clear the historical logs.

For Tableau Public and Tableau Online, this data is deleted from the products after a period of time.

As stated above, Tableau collects and stores data related to users pursuant to the restrictions and for the purposes described in its Privacy Policy.

Right to Data Portability

Like with the Right to Access, data subjects have a right to request a copy of their personal data in a “structured, commonly-used and machine-readable format”. You can use the CSV data files that Tableau exports to fulfill these requests.

Conclusion

The GDPR imposes new responsibilities on controllers and processors as well as establishes new rights for data subjects with the goal of increasing data privacy for individuals within the EU. Tableau products offer capabilities to help you maintain compliance with the GDPR when using Tableau to process personal data in data sources as well as maintain personal data as part of Tableau Server, Tableau Online, and Tableau Public user accounts.

About Tableau

Tableau helps people see and understand their data, no matter how big it is, what channel it’s coming from, or what database it’s stored in. Quickly connect, blend, and visualize your data with a seamless experience from the PC to the iPad. Create and publish marketing dashboards with automatic data updates, and share real-time insights with colleagues, teams, executive leaders, partners or customers—no programming skills required. Try it for free today!

References

Tableau Software Privacy Policy

Tableau Software Security

European Commission Data Protection

Full text of the GDPR