Privacy FAQ

General Data Protection Regulation (GDPR)

Frequently Asked Questions

How Qlik® manages privacy in its products

In today's world of data breaches and cyberattacks, Qlik realises that privacy is a significant concern for customers. Qlik takes this concern seriously and adhears to data protection laws by implementing both security- and privacy-by- design methods in its development process. This document addresses frequently asked questions on how data privacy is managed within the Qlik product portfolio.

Qlik Sense® and QlikView®

This section focuses on QlikView and Qlik Sense on-premise product lines.

1. When is Qlik a Data Controller/Processor?

a) Who is the data processor for Qlik On-Premises Products?

Qlik Sense and QlikView (referred to collectively in this document as the "**On-Prem Products**") are on-premises software. This means that the software is downloaded to, and resides on, the customer's system(s). Whatever content the customer chooses to load into the On-Prem Product stays within the customer's system(s). Qlik does not have access to this content; therefore, the customer, and not Qlik, is the data controller and the data processorof this content in data protection law terms. While there may be instances related to Support or Consulting services where a customer shares with Qlik applications developed within the On-Prem Products that contain personal data, such sharing is at the discretion of the customer and not an aspect of the ordinary operation and use of the On-Prem Products.

b) When is Qlik a data controller?

If a user creates a Qlik Account (e.g. to download Qlik Sense Desktop) or when a customer purchases licences, Qlik does collect basic personal data for which it is the data controller. For example, we collect name and password data so that a user can set up a Qlik Account (https://community.qlik.com/welcome). When licences are purchased, we maintain like all business a database of customer and partner contacts for billing, marketing and other ordinary business purposes.

2. What Data is sent back to Qlik by virtue or a customer using an On-Prem Product?

a) License file: When deploying Qlik Sense Enterprise, it needs to be activated using a License Enabler File (LEF). This file will be transferred from the Qlik license server when the administrator fills in the license information in the administrative panel. The information that is filled in includes owner name, owner organization, serial number, and control number. This information is transferred to the Qlik License Server, which then returns the license file to Qlik Sense Enterprise. The license file contains license details, but no personal data.

b) Authentication: Authentication is a process that happens once per session. Once logged in, the user does not have to authenticate again until the session that tracks the user has timed out, or the user chooses to actively log out. Its purpose is to prove the identity of the user. Authentication differs from authorization; authentication determines whether a user can access the Qlik On-Prem installation at all, whereas authorization determines what the user, once authenticated, can see (as determined by the customer Administrator—see FAQ 4(d), below). Authentication data (i.e. username and password) is only sent back to Qlik if the user is authenticated using Qlik ID (see section 1 b) above regarding Qlik Accounts).

c) Usage data: Qlik Sense Desktop (but not Qlik Sense Enterprise, QlikView Desktop or QlikView Enterprise), collects user login data to monitor user engagement to enable Qlik to continuously improve the Sense Application. All data is collected and processed on an anonymous, aggregated basis.

3. Privacy-By-Design at Qlik

Qlik has implemented within its R&D/Product development process a Privacy-By-Design step, so that privacy concerns (and Privacy-By-Default) are taken into account in the development of our products and any changes to these.

4. How can Qlik On-Prem Products help me to comply to the GDPR?

Qlik is aware that compliance with Privacy / Data Protection law, in particular the General Data Protection Regulation (GDPR), is top-of-mind for customers. To that end, we believe there are some useful features in our products that can help you, as the data controller and processor, to comply with EU Data Protection law requirements:

a) How can I anonymise / pseudoanonymise personal data?
The On-Prem Products do not have any specific 'out-of-the-box' anonymizing functionality. Instead, the built-in scripting language can be utilized to hash data that is deemed too sensitive to retain in its original form. In addition, the source data can be anonymized before an app is built over it.

b) How can I easily retrieve all personal data relating to a particular Data Subject (e.g. in response to a Data Subject Access Request) and create copies to supply to the Data Subject?
The On-Prem Products are built around the ability of visualizing and analysing the data that is entered into it. In addition to the ability to visualize and automatically build relations, there is an in-built search function that users can use.

c) How can I delete personal data relating to a particular Data Subject?
As the owner of the data, the customer can use different ways to access it. This includes searching for data, or adding more visualizations to display the data. Modifying the data load script manually will offer the possibility to choose what data to include at the next reload, and can act as a delete function. Alternatively, users can delete personal data form the source data before an app is built over it.

d) How do I control sharing / restricting of personal data access within an app?
For each installation of an On-Prem Product, the customer can have one (or more) Administrator users. Administrators set access rights for others to applications. These access rights can be set individually for each app, or for a group ("stream") of apps. The Administrator can control these access rules from their Qlik Management Console, available within the software. The Qlik authentication system (described in section 2 above) helps to ensure that only those authorized users with access to a particular app or stream can access it. A further level of authorization called Section Access is also available within applications. Section Access is a way to define what data inside an app should be available to a particular user. Please note that the Administrator controls described above are tied to the local platform installation, and not the Qlik apps themselves. It is recommended that Qlik apps that contain personal data or sensitive content be kept within their associated On-Prem Product production (live) environment to ensure that intended Administrator control settings are maintained.

For questions related to the information in this document, please contact your usual Qlik representative. This document describes Qlik's On-Prem product Data Protection/Privacy Law compliance. For Security related questions (e.g. encryption), you can find further information resources at https://help.qlik.com/.

The information in this document is accurate as of July 2017. Qlik reserves the right to amend its products and services from time to time. For any updates, please check our Terms and Conditions, and Privacy Policy.

qlik.com