Privacy FAQ
V1.0

General Data Protection Regulation (GDPR) and Qlik Sense Cloud®

Frequently Asked Questions

How Qlik® manages privacy in Qlik Sense Cloud® Products

With increasing privacy/data protection regulations, in particular the EU General Data Protection Regulation (GDPR), Qlik realises that privacy is a significant concern for customers and partners. Trusted vendors are paramount. Qlik takes this concern seriously and adhears to privacy and data protection laws by implementing both security- and privacy-by- design methods in its development process. This document explains how data privacy is managed within Qlik Sense Cloud® products.

Qlik Sense Cloud® Products

This section focuses on Qlik Sense Cloud® product lines “Qlik Sense Cloud Basic”, “Qlik Sense Cloud Plus”, and “Qlik Sense Cloud Business” (referred to collectively in this document as the “Cloud Products”).

When is Qlik a Data Controller/Processor?

Who is the data processor for Qlik Sense Cloud Products?

Cloud Products refers to Software as a Service (SaaS) that is managed and hosted by Qlik. Whatever content the customer chooses to load into the Cloud Product remains the customer’s responsibility. The customer, and not Qlik, is the data controller and the data processor of this content in data protection law terms. The storing of personal data relating to identifiable individuals is not the primary function of our Cloud Products, and in conformance with the principe of data minimization and anonymization under GDPR, Qlik does not recommend users insert personal data content into applications in our Cloud Products.

When is Qlik a data controller?

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

Please refer to Qlik Cloud’s Terms of Service: https://eu.qlikcloud.com/terms/latest
and privacy policy: https://www.qlik.com/us/legal/legal-policies

Data location:

Where are the data centres that operate Qlik Sense Cloud?

Qlik has 3 networked data centres: Dublin, Ireland; North Virginia, USA; and Sydney, Australia. Qlik uses Amazon Web Services ("AWS") architecture to operate Qlik's Cloud service.

Can I choose to keep my Qlik Sense Cloud data in my region?
(for example, can EU users ensure their data does not leave the EU)?

Yes, when you create a new Qlik Sense Cloud Business workspace, you can select any of the above 3 data centres to store your "at-rest" data. However, if you choose to share that application with someone outside of that region (e.g. a French user sharing it with a US user) or if you travel and access the app in a different region (e.g. a French user travels to USA and accesses the app from the USA), then the data will leave that region (in the foregoing examples, leave the EU). This is because it will be viewable from "in-memory" data on a server in our cloud from the new region and also be transported to the data centre closest to the user. The reason for this is for performance experience of the user/recipient. The user maintains full control over who they choose to share their apps with, through permissions and access granting.

Currently, this region-preference server feature is only available for Qlik Sense Cloud Business. Qlik Sense Cloud Basic does not have this feature and users' content (regardless of region) is stored in our data centres in the USA. If you are an EU user and wish for your data to be stored in the EU only, you should:

(i) Have a Qlik Sense Cloud Business account;
(ii) Select our EU data centre (Dublin) as your preference for storing at-rest data;
(iii) Access the content from the EU only; and
(iv) Not share the content with any others based outside of the EU.

Data Access & Use by Qlik:

Does Qlik have access to my data that I choose to put into a Qlik Sense Cloud app?

Qlik employees do not access a user's cloud content unless (a) the user actively shares it with someone at Qlik (e.g. in a Consulting Services context), or (b) Qlik is prompted by a trouble-shooting issue to access the individual content. Only a closed group of Qlik employees can access individual user content to trouble-shoot and only under strict controls.

Does Qlik use data related to my use of Qlik Sense Cloud?

Like all Cloud providers, Qlik does monitor usage data of our service. An example would be frequency of log-on, usage per day, and traffic/usage per country, etc. which could then enable us to allocate resources better (e.g. server space) to better serve our customers and/or improve our services.

Architecture & Security:

Where are Qlik Sense Cloud products hosted?

As you will see from our terms of service, Qlik Sense Cloud products are hosted by Amazon Web Services ("AWS"). You can find the AWS Privacy Policy here: https://aws.amazon.com/privacy/ and Qlik's Privacy Policy here. Qlik Sense Cloud prides itself on its security features. A fuller description of can be found here in our Qlik Sense Cloud Security White Paper.

Data Retention

How long does Qlik keep data in Qlik Sense Cloud?

Users may at any time delete their applications. Once deleted by the user, all information hosted by Qlik in that application is deleted, and no back-up exists. For dormant applications (i.e. applications within accounts that have been inactive for over 12 months), Qlik may delete these applications. Regarding user account details, if a user has not used their Qlik Sense Cloud account in 12 months, Qlik reserves the right to deactivate the account.

Privacy-By Design and Privacy-By-Default

Does Qlik utlise Privacy-By Design and Privacy-By-Default in Qlik Sense Cloud?

Qlik has implemented within its R&D/Product development process a Privacy-By-Design step, and within its product Privacy-By-Default features. For example, unless the app creator or Administrator pro-actively gives access to an app or stream to a user, by default, the user will be unable to access it unless they created the app.

Features to help users comply with Privacy laws

How to anonymise / pseudoanonymise / delete personal data:

Qlik Sense Cloud does not have any specific anonymizing functionality. Instead, the built-in scripting language can be utilized to encrypt, hash and scramble 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 before uploading to the Cloud.

How to 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:

All of Qlik's Products have in-built search tools; for example, Qlik Sense Cloud has the "Smart Search" function. You can find more information on these search tools at https://help.qlik.com/ . In addition, Qlik Sense Cloud is built around the ability of accessing and analysing the data that is entered into it. As well as by using the search function, the data relating to a particular data subject should be easy to retrieve using already configured visualizations.

Sharing / restricting personal data access within an app:

For all types of Qlik Sense Cloud users, the app will only be available to others if the user shares it. Access is controlled by the Qlik Authentication system, which prompts for usernames and passwords at the beginning of each 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 is different from authorization.
Authorization defines what the user, after successfully passing authentication, can do in the system (e.g. what apps they can access in a deployment). It can be adjusted to allow or restrict access by an Administrator.

For Qlik Sense Cloud subscriptions, all users have control over who has access to apps shared through their personal streams, and group owners can control who has access to apps created and shared as part of a work group.

For Qlik Sense Cloud Basic and Qlik Sense Cloud Plus, apps aren't visible to other users until the app creator publishes the app to their stream. Users control who is invited to view the apps in their stream.

For Qlik Sense Cloud Business, users can only see an app if they have access to the group workspace, and/or if they have access to the stream to which an app is published. The group owner can control these access rules from the Qlik Cloud Hub, available within the software.

Resources

Further GDPR information related to Qlik can be found at www.qlik.com/us/gdpr.

For IT Security related questions (e.g. encryption) you can find information resources on Qlik.com : https://www.qlik.com/us/products/qlik-sense/qlik-sense-cloud

Full list of links used in this document:

Qlik Cloud's Terms of Service: https://eu.qlikcloud.com/terms/latest
Qlik's Privacy Policy: https://www.qlik.com/us/legal/cookies-and-privacy-policy
AWS Privacy Policy: https://aws.amazon.com/privacy/
Qlik Sense Cloud Security White Paper:
https://www.qlik.com/us/-/media/files/resource-library/global-us/register/whitepapers/wp-qlik-sense-cloud-security-en.pdf?la=en

For questions related to the information in this document, please contact your usual Qlik contact.

The information in this document is accurate as of 10th May 2018. 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