International Transfers of Personal Data FAQ

Qlik recognizes that privacy and security of customer data is of paramount importance. This FAQ provides information relating to international transfers (e.g., to the USA) of European customer personal data which Qlik may process on customers' behalf ("Customer Content"), in particular in light of the Schrems II Judgment of the CJEU ("Schrems II"). The terms "processor", "personal data" and "processing" (and its derivates) have the same meaning in this note as under the EU General Data Protection Regulation ("GDPR"). This FAQ applies to both Qlik and Talend offerings; Qlik Cloud, for the purpose of this FAQ, includes Talend cloud offerings. Unless otherwise specified, "Qlik" includes both Qlik and Talend affiliates.

1. Qlik's privacy compliance model

Qlik has a robust, global privacy and security compliance program. Our approach to privacy compliance is to apply GDPR standards globally including in the USA, where possible. For example, our data retention procedures and security controls apply globally to meet EU standards, regardless of location of data/customer. For further information on Qlik's privacy program, please see Qlik's Trust & Privacy resources.

2. Processing and Transfer Scenarios

2.1. When is Qlik a processor of Customer Content?

Qlik may be a processor of Customer Content in two scenarios:

A. Qlik Cloud: If the customer uploads Customer Content into Qlik Cloud e.g., creates a Qlik Sense app containing personal data, such as a non-anonymized HR data app; and/or

B. Qlik professional services: If the customer provides Customer Content to Qlik in the context of a consulting engagement (e.g., to build a Qlik application for the customer, which contains personal data) or for technical support (e.g., uploads to the support page of the Qlik Community portal a support attachment which contains personal data or invites a Qlik support engineer into their Qlik Cloud tenant and shares with the engineer personal data therein).

Customers have full control over their Customer Content, which may contain personal data if a customer chooses, however most Customer Content is not personal in nature. For example, customer support attachments that Qlik receives are typically technical in nature, with customers encouraged to follow data-minimization best practices to remove any personal data prior to submitting it to the Qlik Community portal or Talend Support Ticket Portal. For client-managed deployments of Qlik software, as this software and any Customer Content in it are on-premise, Qlik would not be a processor of that data unless it is sent to Qlik under the scenarios above. Given the above scenarios, the circumstances in which Qlik may be a processor for customers are narrow. For further information, see our Product Privacy Notice,

2.2. When would European Customer Content be transferred to the USA?

A. Qlik Cloud:

- If Qlik does in fact process European Customer Content within Qlik Cloud, it is unlikely that it is sent to/accessed from the USA.
- Qlik Cloud customers can choose an EU tenant (including back-ups). We will only host your Qlik Cloud Customer Content in the region you select.

- Tenant access (and to Customer Content therein) is controlled by the customer. Unless access is shared by the customer (e.g., with a user outside the EU), there is no 'transfer' by Qlik. It is the customer's determination to make on who to invite into their tenant.
- While Qlik uses third party subprocessors for Qlik Cloud, these subprocessors also host Customer Content in the EU only for our EU tenants. Please note that Qlik Cloud subprocessors do not have access to any Qlik Cloud Customer Content and could not access it as they do not have access to the encryption key.
- Customers may also use Qlik's Cloud's Customer-Managed-Key ("CMK") function to manage their own encryption key, where available.
- As such, Schrems II is likely not applicable to European Customer Content in Qlik Cloud, as Qlik does not transfer such Customer Content outside of the EU, unless a customer selects to invite a Qlik employee into their tenant (see below – Qlik professional services for more detail on this).

B. Qlik professional services:

- Although Qlik is a U.S.-headquartered, global company, Qlik's operations (and by extension, any data processing that Qlik may undertake on behalf European customers) are Europe-centric. This is because of our European (Swedish for Qlik, French for Talend) origins and our large European presence.
- Technical support data received in relation to Qlik offerings is hosted at-rest in Europe only (UK & Germany), while technical support data received in relation to Talend offerings is hosted at-rest in the United States and France. In terms of access by Qlik team members, while technical support Customer Content (e.g., attachments to support tickets) may be accessed by our technical support engineers outside Europe so that customers may avail of our 24/7/365 customer support, our EMEA support services are primarily carried out by our employees in Europe (predominantly in Sweden and Spain for Qlik, and France for Talend).
- For Qlik Cloud-related services/support, Qlik does not have direct access to Qlik Cloud Customer Content. In the unlikely event that a customer would need to give access to Qlik to Customer Content within their tenant (this is extremely rare as most issues can be resolved without tenant access), under our controls, a customer would have to explicitly invite a technical support engineer into their tenant for Customer Content therein to be accessible by a Qlik technical support engineer.
- For consulting services, our services can be carried out using Customer Content hosted on customer systems only (with no hosting by Qlik) or by inviting the Qlik Consultant into your Qlik Cloud tenant (e.g., in the EU) with access controlled by the customer. This means that customers can host their consulting Customer Content in the EU only. In terms of access by Qlik team members, Consulting engagements are in the vast majority performed by in-region resources. This means that not only is the data hosted in Europe, but access to it is extremely likely to be by Europe-based persons too for European customers.
- In terms of transfer destinations, as above, transfer by Qlik (e.g., access by a non—Europe-based Qlik team member of European Customer Content) is extremely unlikely (and it is similarly unlikely that such data transferred would contain personal data). However, Qlik's main hubs outside of the EU for our services include the UK, Canada and Israel, where we have support/R&D resources (all adequate countries under GDPR), as well as the USA and India. Qlik has in place relevant transfer measures for these jurisdictions, such as the EU-US Data Privacy Framework ("DPF") for transfers to the USA and the latest EU & UK Standard Contractual Clauses for India.

To summarize, while it is possible that Qlik may process European Customer Content outside Europe (e.g., in/from the USA), it would only occur if (a) the customer gave Qlik Customer Content to process on the customer's behalf, (b) that Customer Content contained European personal data, and (c) the Customer Content was actually transferred to/accessed from a destination such as the USA. As above, this is very unlikely, in particular in relation to Qlik Cloud Customer Content, with the sharing of Qlik Cloud Customer Content controlled by the customer. Even if

such a transfer did occur, the personal data within the Customer Content is likely to be very limited (e.g., B2B contact details, or IP addresses in a log file).

3. Customer Content Protections

As per our Data Processing Agreement ("DPA"), our obligations under the EU & UK Standard Contractual Clauses ("SCCs") and DPF Principles, we are committed to cooperating with customers to provide the relevant information they need so that they can use our offerings with confidence. We transfer any European personal data (if any) to our U.S. operating affiliates under the DPF Principles. The DPF was granted an adequacy decision by relevant European authorities, such as the EU Commission. To view our DPF Policy, please see https://www.qlik.com/us/legal/legalpolicies. While a transfer impact assessment is not required under the DPF, Qlik has previously made available the information below information to customers to for the purpose of their own due diligence / transfer impact assessments, if they wish.

3.1. Relevance of the laws addressed in Schrems II to Qlik

A. Qlik is a B2B software company and most of our products and services do not result in us processing personal data on behalf of customers. As indicated by this USA Government Paper[1], most companies, including Qlik, do not store or hold data that would be of interest to U.S. intelligence agencies.
B. The U.S. Department of Justice[2] also recognizes that data owners, rather than their cloud service providers, should typically be contacted regarding any U.S. law enforcement request, stating that "prosecutors should seek data directly from the enterprise, if practical, and if doing so will not compromise the investigation. If an investigation requires only a subset of data for example, the email accounts of a small group of employees, or data relating to a particular group of transactions approaching the enterprise will often be the best way to get the information or data sought, while avoiding over-collection. This approach also gives the counsel the opportunity to interpose privilege and other objections to disclosure for appropriate resolution, and parallels the approach that would be employed if the enterprise maintained data on its own servers, rather than in the cloud."[2].
C. To date, Qlik has never received a request from a government or law enforcement agency (in the USA or otherwise) to surrender Customer Content under the laws addressed in Schrems II or similar laws. We believe it is unlikely that Qlik would ever receive such a request impacting European personal data rights of data subjects of Customer Content, given Qlik's minimal processing of European Customer Content in the USA, the nature of the Customer Content processed and the B2B nature of our business.
D. Qlik also has a process in place to monitor for relevant legal updates and guidance, such as those from the EDPB. Qlik's goal is to always protect Customer Content while also complying with relevant laws.

3.2. Contractual measures

A. Qlik provides commitments to customers, in its DPA as well as in the DPF Principles, to protect any transferred European Customer Content, as set out below.
B. Qlik also reenforces our obligations under the DPF Principles/SCCs in Section 5.5 of our DPA. These include assurances such as requesting the authority making any law enforcement request to address their request instead to the customer directly and seeking to inform the customer of the request where it is lawful to do so.

[1] https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

[2] https://www.justice.gov/criminal-ccips/file/1017511/download

C. Qlik also commits in Qlik's DPA to undertakings regarding the engagement of any subprocessors. Qlik's subprocessor list may be found here.

3.3. Technical and organizational measures

A. Qlik provides the technical and organizational measures outlined in our DPA. For Qlik Cloud, Qlik also offers the security measures provided in our Qlik Cloud Security Addendum. These are supplemented by the stringent policies and procedures of our global privacy program discussed at 1 above.

B. Qlik is already EU-centric in our operations for European customers, enabling Qlik Cloud customers to host their Customer Content in the EU.

C. Qlik Cloud Customer Content is protected by encryption. Where available, customers are also able to deploy our CMK feature, which **enables customers to manage their own tenant encryption keys** (further information on CMK may be found here).

D. While Qlik uses subprocessors in relation to Qlik Cloud, such subprocessors cannot, even from a technical perspective, access Qlik Cloud Customer Content due to encryption and security controls. Customers have ownership and control over their Customer Content at all times and user access is managed by the customer, with customers able to deploy their own IDP controls to further regulate access to their own Customer Content. Customers also control what Customer Content they choose to input into Qlik Cloud, as well as the deletion of that Customer Content.

E. For Qlik professional services, any onward transfer outside of Europe is limited (see 2 above). Nonetheless, Qlik has relevant technical and organizational protections in place, such as encryption, least-privilege access, logging, and data retention controls, with Customer Content typically deleted by Qlik within 180 days after closure of the relevant technical support case or within 30 days after the termination of the Consulting engagement, as relevant.

Qlik is confident that our business and customer offerings continue to meet GDPR and Schrems II standards and that European customers can continue to use our products and services with confidence. In addition to the information above, customers may submit transfer risk assessment questionnaires to privacy@qlik.com if they require further information.

This note is provided for information purposes only and is not legal advice to your organization. Qlik encourages customers to consult with their own legal counsel to keep abreast of relevant requirements. This document is accurate at the date of publication. For changes or further information, customers should visit Qlik's Privacy Trust resources.

Qlik resources:
https://www.qlik.com/us/trust/privacy https://www.qlik.com/us/legal/product-privacy-notice
https://www.qlik.com/us/legal/legal-agreements https://www.qlik.com/us/legal/product-terms