Qlik® and the Schrems II Judgment (International Transfers of Personal Data)

Qlik recognizes that privacy and security of customer data is of paramount importance. This note provides information relating to transfers to the USA of European customer personal data which Qlik may process on customers' behalf ("Customer Data"), in light of the Schrems II Judgment of the CJEU ("Schrems II"). The terms "adequate country", "data controller", "data processor", "personal data", "processing" (and its derivates), "subprocessors" and "third country" have the meanings in this note as under the EU General Data Protection Regulation ("GDPR").

1. Qlik's privacy compliance model

Qlik has a robust, global privacy and security compliance program. Our global 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 Privacy Trust resources.

2. Processing by Qlik of European Customer Data in the USA

2.1. *When is Qlik a data processor of Customer Data?*

As set out in our Product Privacy Notice, Qlik may be a data processor of Customer Data in two scenarios:

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

2.1.2. Qlik services: If in the context of Qlik providing consulting and/or customer support services to a customer, the customer provides to Qlik their Customer Data (containing personal data), e.g., uploads to the support page of the Qlik Community portal a support attachment, which contains personal data.

Customers have full control over their Customer Data content, which may contain personal data if a customer chooses, however most Customer Data 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. For client-managed deployments of Qlik software, as this software and any customer content in it are on-premise, Qlik would not be a data processor of that data unless it is sent to Qlik under the scenarios above. Given this, the circumstances in which Qlik may be a data processor for customers are narrow.

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

If Qlik does process European Customer Data, it is unlikely that such data is sent to the USA.

2.2.1. Qlik Cloud: Qlik Cloud customers can choose our EMEA tenant, which hosts data in the EU only (including back-ups). Tenant access is controlled by the customer, and unless access is shared by the customer with someone outside the EU or an adequate country (internally or, for example, with a Qlik support engineer), the Customer Data is not exported, for example to the USA. As such, Schrems II is likely not applicable to European Customer Data in Qlik Cloud. Qlik Forts also gives customers the flexibility to keep certain Qlik Cloud applications on-premise, if they wish. For more information on Qlik Forts, please visit our website information on Qlik Forts.

2.2.2. Qlik services: Although Qlik is a U.S.-headquarted, global company, Qlik's operations (and by extension, any data processing that Qlik may undertake on behalf European customers) are European-centric. This

is because of our European (Swedish) origin and our large European presence. For example, while support Customer Data may be transferred outside the EU so that customers may avail of our 24/7/365 customer support, our EMEA support services are primarily carried out by our employees in the EU (Sweden and Spain) and our at-rest hosting locations for the vast majority of support Customer Data are in the UK and Germany.

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

3. Customer Data protections

3.1. *Application of Schrems II to Qlik*

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. 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]. To date, Qlik has never received a request from a government or law enforcement agency (in the USA or otherwise) to surrender Customer Data 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 Data, given Qlik's minimal processing of European Customer Data in the USA, the nature of the Customer Data processed and the B2B nature of our business. Qlik also has a process in place to monitor for relevant legal updates and guidance, such as those from the EDPB. Our customers also benefit from our robust legal and technical protections, outlined below.

3.2. *Contractual measures*

For Qlik customers, Qlik provides in our customer Data Processing Addendum ("DPA") the 2021 EU Standard Contractual Clauses ("SCCs"), approved by the EU Commission for transfers of EU personal data to third countries, as well as the 2022 UK Addendum in respect of UK personal data. Clause 15 of the SCCs describes the contractual assurances we provide in relation to European Customer Data transferred to the USA, if transferred. Qlik also reenforces these obligations in Section 5.5 of our DPA. These include assurances such as requesting the authority 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. Qlik's goal is to always protect Customer Data while also complying with relevant laws.

3.3. Technical and organizational measures

Qlik has in place the technical and organizational measures outlined in our DPA. These are supplemented by the stringent policies and procedures of our global privacy program discussed at 1 above. Qlik is already EU-centric in our operations for European customers, enabling Qlik Cloud customers to host their data in the EU. Qlik Cloud

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

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

Customer Data is protected by encryption. While Qlik uses subprocessors in relation to Qlik Cloud, such subprocessors cannot, even from a technical perspective, access Qlik Cloud Customer Data due to encryption and security controls. Customers have ownership and control over their data 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 Data.

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.

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/products/qlik-sense/qlik-forts
https://www.qlik.com/us/legal/legal-agreements