Data Transfer Impact Assessment Statement

Last updated on: 15 November 2022

Overview

This document provides information to help Certinia customers conduct data transfer impact assessments in connection with their use of Certinia Services, in light of the “Schrems II” ruling of the Court of Justice for the European Union and the recommendations from the European Data Protection Board.

In particular, this document describes the legal regimes applicable to Certinia in the US, the safeguards Certinia puts in place in connection with transfers of customer personal data from the European Economic Area, United Kingdom or Switzerland ("Europe"), and Certinia's ability to comply with its obligations as "data importer" under the Standard Contractual Clauses ("SCCs").

For more details about Certinia’s GDPR compliance program please visit this page.

Step 1: Know your transfer

Where Certinia processes personal data governed by European data protection laws as a data processor (on behalf of our customers), Certinia complies with its obligations under its Data Processing Addendum available at Data Processing Addendum ("DPA"). The Certinia DPA incorporates the SCCs and provides the following information:

- description of Certinia’s processing of customer personal data (Exhibit A); and

- description of Certinia’s security measures (Exhibit B)

Please refer to Exhibit A to the DPA for information on the nature of Certinia's processing activities in connection with the provision of the Services, the types of customer personal data we process and transfer, and the categories of data subjects.

A list of all of our data subprocessors and an RSS feed subscription where you can stay up-to-date on changes is available at subprocessors.

Step 2: Identify the transfer tool relied upon

Where personal data originating from Europe is transferred to Certinia, Certinia relies upon the European Commission's SCCs to provide an appropriate safeguard for the transfer. To review Certinia’s Data Processing Addendum (which incorporates the SCCs) please visit Data Processing Addendum.

Where customer personal data originating from Europe is transferred between Certinia group companies or transferred by Certinia to third-party subprocessors, Certinia enters into SCCs with those parties.

Step 3: Assess whether the transfer tool relied upon is effective in light of the circumstances of the transfer

U.S. Surveillance Laws

Information about these US surveillance laws can be found in the U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S.Data Transfers after Schrems II whitepaper from September 2020. This whitepaper details the limits

and safeguards pertaining to US public authority access to data and was issued in response to the Schrems II ruling.

Is Certinia subject to FISA 702 or EO 12333?

Certinia, like most US-based SaaS companies, could technically be subject to FISA 702 where it is deemed to be a RCSP. However, Certinia does not process personal data that is likely to be of interest to US intelligence agencies.

Furthermore, Certinia is not likely to be subject to upstream surveillance orders under FISA 702, the type of order principally addressed in, and deemed problematic by, the Schrems II decision. Certinia does not provide internet backbone services, but instead only carries traffic involving its own customers. To date, the U.S. Government has interpreted and applied FISA 702 upstream orders to only target market providers that have traffic flowing through their internet backbone and that carry traffic for third parties (i.e., telecommunications carriers).

EO 12333 contains no authorization to compel private companies (such as Certinia) to disclose personal data to US authorities and FISA 702 requires an independent court to authorize a specific type of foreign intelligence data acquisition which is generally unrelated to commercial information. In the event that US intelligence agencies were interested in the type of data that Certinia processes, safeguards such as the requirement for authorization by an independent court and the necessity and proportionality requirements would protect data from excessive surveillance.

Indian Surveillance laws

The basic law underpinning electronic surveillance is section 5(2) of the Telegraph Act, 1885, this allows for the interception and disclosure of messages in the event of a public emergency or in the interest of public safety. In addition to matters like state security

and public order, the Government can also order this for preventing incitement to the commission of an offence.

Rule 419A was added to the Telegraph Rules, 1951 states that an interception order can be issued only when there is no other reasonable means of acquiring such information.

Section 69 of the Information technology Act, 2000 (IT Act) tracks Section 5(2) of the Telegraph Act and allows the Government to intercept, monitor, or decrypt any information received or stored through any computer resource provided that a degree of specificity is disclosed to allow access and is orders can only be issued similarly to Rule 419A.

What is Certinia's practical experience dealing with government access requests?

To date, Certinia has never received a US National Security Request (including requests for access under FISA 702 or direct access under EO 12333) in connection with customer personal data or a request from the Indian Government.

Therefore, while Certinia may technically be subject to surveillance laws identified in Schrems II we have not been subject to these types of requests in our day-to-day business operations.

Step 4: Identify the supplementary measures applied to protect the transferred data

Certinia provides the following technical measures to secure customer data:

- All data is encrypted in transit using, at a minimum, 128-bit TLS Certificates and 2048-bit RSA public keys

- Additional information about Certinia's security practices and certifications are available in Annex II of the Data Processing Addendum, and on our Trust and Compliance site and our Security site.

Certinia's contractual measures are set out in our Data Processing Addendum which incorporates the SCCs. In particular, we are subject to the following requirements:

- Certinia is contractually obligated to have in place appropriate technical and organizational measures to safeguard personal data (both under the Data Processing Addendum as well as the SCCs we enter into with customers, service providers, and between entities with the Certinia group).
- Certinia is obligated under the SCCs to notify its customers in the event it is made subject to a request for government access to customer personal data from a government authority. In the event that Certinia is legally prohibited from making such a disclosure, Certinia is contractually obligated to challenge such prohibition and seek a waiver.
- Under the SCCs, Certinia is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.

Certinia's organizational measures to secure customer data include:

- Certinia remain accountable to you for how your data is used when transferred to third parties. We review the data Certinia plans to share with a service provider and the associated level of risk, the supplier's security policies, measures, and third party audits, and whether the supplier has a mature privacy program that respects the rights of data subjects. We provide

a list of our sub-processors here and you can sign up for updates to our subprocessors here.

- Certinia provides data protection training to all Certinia staff.

Step 5: Procedural steps necessary to implement effective supplementary measures

In light of the information provided in this document, including Certinia's practical experience and the technical, contractual, and organizational measures Certinia has implemented to protect customer personal data, Certinia considers that the risks involved in transferring and processing European personal data in/to the US and/or India do not impinge on our ability to comply with our obligations under the SCCs (as "data importer") or to ensure that individuals' rights remain protected. Therefore, no additional supplementary measures are necessary at this time.

Step 6: Re-evaluate at appropriate intervals

Certinia will review and, if necessary, reconsider the risks involved and the measures it has implemented to address changing data privacy regulations and risk environments associated with transfers of personal data outside of Europe.

Legal Notice: Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, and (b) does not create any commitments or assurances from Certinia and its affiliates, suppliers or licensors. The responsibilities and liabilities of Certinia to its customers are controlled by Certinia agreements, and this document is not part of, nor does it modify, any agreement between Certinia and its customers.