SIEMENS CLOUD SOLUTIONS TRUST CENTER

International **Data Processing** in light of Schrems II

SIEMENS

1. Introduction

In its so-called "Schrems II ruling" (case C-311/18), the European Court of Justice (CJEU) declared the European Commission's Privacy Shield Decision invalid on account of invasive US surveillance programs, thereby making transfers of personal data on the basis of the Privacy Shield Decision illegal. The court further stated that companies transferring personal data based on transfer tools contained in Art. 46 General Data Protection Regulation (GDPR), must check whether the law or practice of the third country, in which a data recipient is located, impinge on the effectiveness of such safeguards.

2. Legal Background

When it comes to international transfers of personal data, the main rule in GDPR is that transfers outside of the European Economic Area (EEA) are prohibited unless an adequate safeguard can be used. First and foremost, there are the EU Commission's adequacy decisions, where the EU Commission after thorough evolution of national laws have concluded that a country's data protection laws are essentially equally good as the GDPR. Then there a mechanisms for secure transfers outside of the EEA, the EU Standard Contractual Clauses and Binding Corporate Rules (only for intra-group transfers).

3. Schrems II ruling and EU Standard Contractual Clauses (SCC)

The European Court of Justice explicitly stated that the SCC are still valid as a transfer mechanism in principle but do not operate in a vacuum. It must be assessed on a case-by-case basis if the law or practice of the third country where the recipient is located impinges on the effectiveness of the SCC.
In response to the CJEU ruling, Siemens stopped any use of the EU-U.S. Privacy Shield and continued its use of SCC as basis for personal data transfers to recipients in non-EEA countries.
In light of the Schrems II ruling, the European Commission issued a set of modernized SCC to help companies lawfully transfer personal data from EU to non-EEA countries. These new SCC form an integral part of the Siemens Data Privacy Terms (DPT).

4. Transfer Impact Assessment and EEA – US Data Transfers

Following the Schrems II ruling, the European Data Protection Board issued its "Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" suggesting that companies must assess whether problematic law is interpreted and applied in practice as to cover the respective personal data transferred.
Additionally, Clause 14(a) of the SCC, requires both data exporters and importers to warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, prevent the data importer from fulfilling its obligations under these Clauses.

For the United States, the CJEU concluded the following US laws do not respect the minimum safeguards resulting from the principle of adequacy under EU law:

- Title 50 United States Code § 1881 a - Foreign Intelligence Surveillance Act, Section 702 (FISA 702)
- Executive Order 12333 (EO 12333)

To comply with its obligation under the SCC, Siemens has assessed whether it has reason to believe that Section 702 and/or EO 12333 would prevent Siemens from fulfilling its obligations under the SCC (either acting in its role as data

exporter or data importer). Having done this assessment, Siemens has determined that it does not have reason to believe that FISA 702 or EO 12333 when applied in practice would prevent Siemens from fulfilling its obligations under the SCC in the specific circumstances of the cloud solutions offered by Siemens.

a) FISA 702

The documentation reviewed by Siemens provides no reason to believe that, in practice FISA 702 is used to target private enterprises but rather involves the collection of data relating to the communications and actions of individuals and/or criminal groups (e.g., terrorist networks).

- In this context the US government has engaged in two foreign surveillance programs under FISA 702, both of which were raised as specific concerns by the CJEU when invalidating the EU-US Privacy Shield framework. According to the Privacy and Civil Liberties Oversight Board (PCLOB) "Report on the Surveillance Program Operated Pursuant to Sec 702 of the Foreign Intelligence Surveillance Act"[1], which played an important role in Schrems II – the CJEU's conclusions regarding US surveillance programs were based largely on the findings of the Irish High Court, which, in turn, drew heavily from the PCLOB report - both programs focused on the collection of **communications** as follows:
  - PRISM or downstream surveillance, which involves the direct 'downstream' collection of information from US online providers that provide individual accounts. Downstream collection acquires internet transactions that are "to," "from," or "about" a tasked selector. Effectively, the government sends a selector, such as an email address, to a US-based provider, and the provider is required to provide the government with all communications sent to or from that selector via that provider's systems.
  - Upstream surveillance, which involves the indirect 'upstream' collection of communications via US telecommunications providers that provide the backbone of the internet.
- The U.S. Department of Commerce (DOC), Department of Justice (DOJ), and Office of the Director of National Intelligence (ODNI)[2] released a joint white paper in September 2020 "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II". The whitepaper also describes and confirms the targeting practices described above and concludes:

> "Most U.S. companies do not deal in data that is of any interest to U.S. intelligence agencies and have no grounds to believe they do. They are not engaged in data transfers that present the type of risks to privacy that appear to have concerned the ECJ in Schrems II. (...) As a practical matter, for many companies the issues of national security data access that appear to have concerned the ECJ in Schrems II are unlikely to arise because the data they handle is of no interest to the U.S. intelligence community (...). Companies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data."[3]

- The Annual Statistical Transparency Report for 2020, published by ODNI, further support the scope of application of FISA 702 as described above.

[1] See pages 41 et seqq. (https://fas.org/irp/offdocs/pclob-702.pdf).
[2] https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF
[3] See pages 1 and 2 of the whitepaper "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II"

b) E.O. 12333

EO 12333 provides the basis for certain surveillance activities abroad that are in addition to the acts that are regulated by FISA. In essence, EO 12333 addresses the collection techniques of the U.S. in which the activities are undertaken abroad, i.e., outside the United States.
E.O. 12333 does not include any authorization to compel private companies such as Siemens to disclose data.

c) Conclusion

In light of the above, Siemens concludes that it has no reason to believe that FISA 702 or EO 12333 would prevent Siemens from fulfilling its obligations under the SCCs in the specific circumstances of the transfers related to Siemens' provision of services to its customers.