



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 on 16 July 2020 the European Commission’s Privacy Shield Decision invalid on account of invasive United States (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.

On 10 July 2023, the European Commission adopted its [Adequacy Decision](#) for the EU- U.S. Data Privacy Framework. The European Commission concludes that the United States ensures an adequate level of protection, compared to that of the European Union (EU), for personal data transferred from the EU to US companies participating in the EU-U.S. Data Privacy Framework.

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 are 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.

Siemens 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 (EDPB) 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..

With regards to the transfer of personal data of EU citizens to the US: On 7 October 2022 President Biden signed the [Executive Order on 'Enhancing Safeguards for United States Signals Intelligence Activities'](#). This Executive Order introduces new binding safeguards to address all the points raised by the Court of Justice of the EU, limiting access to EU data by US intelligence services and establishing a Data Protection Review Court.

The EDPB concluded¹:

“ that all the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transferred to the US, regardless of the transfer tool used. Therefore, when assessing the effectiveness of the Article 46 GDPR transfer tool chosen, data exporters should take into account the assessment conducted by the Commission in the Adequacy Decision”.

For Europeans whose personal data is transferred to the US, the following safeguards have been put in place by the US government:

1. Binding safeguards that limit access to data by US intelligence authorities to what is necessary and proportionate to protect national security;
2. Enhanced oversight of activities by US intelligence services to ensure compliance with limitations on surveillance activities; and
3. The establishment of an independent and impartial redress mechanism, which includes a new Data Protection Review Court to investigate and resolve complaints regarding access to their data by US national security authorities.

In light of the above, Siemens concludes Siemens can fulfill its obligations under the SCCs in the specific circumstances of the transfers related to Siemens' provision of services to its customers.

¹ See the Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023 of the EDPB: https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf