International Transfers of Personal Data FAQs

Contents

Introduction

At SAS, we are committed to enabling our customers to use our offerings in compliance with applicable data protection regulations, including the European Union's General Data Protection Regulation (GDPR).

We know that the judgment of the Court of Justice of the European Union (CJEU) in *Schrems II* and the subsequent recommendations released by the European Data Protection Board (EDPB) may present challenges to our customers with respect to the international transfer of personal data. This document describes the steps we have taken to help our customers address those challenges when they use our offerings, and answers frequently asked questions in relation to the impact of *Schrems II* and the EDPB's recommendations on those offerings.

Overview of *Schrems II* ruling and European Data Protection Board recommendations

On July 16, 2020, the CJEU issued the *Schrems II* decision, which held that the EU-US Privacy Shield could no longer serve as a valid mechanism under GDPR to transfer personal data from the European Economic Area (EEA) to the United States. This decision was based on the CJEU's opinion that neither Privacy Shield nor US law generally provided "effective administrative and judicial redress" for US government intelligence and surveillance activities that could affect personal data transferred under the Privacy Shield. The decision also confirmed, however, that organizations could continue to rely on Standard Contractual Clauses (SCCs) as a valid transfer mechanism, subject to certain conditions.

To that end, the CJEU held that organizations transferring personal data outside the EEA under the SCCs must assess, case-by-case, whether the law and practices of the third country, especially as regards any access by the public authorities to the personal data transferred, offer an "essentially equivalent" level of protection for personal data as guaranteed in the EU by GDPR. This additional review of the transfer, known as a Transfer Impact Assessment or TIA, must consider, among other aspects, the circumstances of the transfer, the nature of the data at issue, and the availability and implementation of supplementary safeguards ("Supplementary Measures") to ensure compliance with that "essentially equivalent" level of protection for the personal data.

In June 2021, in response to the *Schrems II* ruling, the EDPB – a body that includes representatives from EU member state data protection authorities – published **recommendations** on how data exporters in the EEA can ensure an essentially equivalent level of protection with respect to their transfers of personal data to third countries. The recommendations describe how to perform a TIA, and suggest technical, organizational, and contractual Supplementary Measures that may be used to ensure an essentially equivalent level of protection. For more details on the EDPB's recommendations, please see our **FAQ on Transfer Impact Assessments**.

FAQs on International Data Transfers

What are SCCs and why are they used?

The GPDR requires that any personal data transferred outside the EU must be provided with an "adequate level of protection" in the receiving country. Some countries outside the EU have obtained an "adequacy" finding from the European Commission that confirms their laws provide an adequate level of protection for EU personal data transferred to those countries.

When the recipient of a transfer of personal data is located in a country that has **not** obtained an adequacy finding, however, the data exporter must implement other mechanisms to legitimize the transfer, referred to in GDPR as "appropriate safeguards." One GDPR-approved method of providing appropriate safeguards is the execution of SCCs – form data transfer agreements that have been pre-approved by the European Commission and include terms meant to ensure an adequate level of protection for personal data – between the data exporter and the data importer.

What are the New SCCs?

Partly in response to the *Schrems II* ruling, in June 2021 the EU Commission released an **updated set of SCCs** (the "New SCCs"), which are intended to replace previous version of the SCCs that had been adopted under the GDPR's predecessor, the European Data Protection Directive (the "Old SCCs").

Among other changes, the New SCCs require the parties to conduct and document a TIA, and incorporate certain Supplementary Measures, such as procedures to be followed if the data importer receives a request for any transferred personal data from government authorities, or becomes aware of direct access to that personal data by those authorities.

The New SCCs have one set of clauses with four different numbered "modules" that can be used depending on the role played by the data importer and data exporter: controller or processor. Under this modular approach, some of the clauses in the New SCCs apply to all transfers, while other clauses include different provisions that vary according to the character of the transfer. This approach requires parties to select which module applies to their transfer, but allows for more flexibility, in terms of the types of transfers that can be accommodated, than the Old SCCs.

Are there any deadlines for implementing the New SCCs?

In its **decision** implementing the New SCCs, the European Commission required that for any contract concluded **after** Sept. 27, 2021, parties relying on SCCs to provide appropriate safeguards for transfers of personal data to third countries must use the New SCCs.

In that same decision, the Commission concluded that for any contract concluded **before** Sept. 27, 2021, that relied on the Old SCCs to provide appropriate safeguards for transfers of personal data to third countries, the parties could continue to rely on the Old SCCs until Dec. 27, 2022, provided that the processing operations that are the subject matter of the contract remain unchanged. If, however, the transfer of personal data under the contract will continue after that date, the Old SCCs must be replaced with the New SCCs or another valid transfer mechanism.

How do the rules of international transfers apply to personal data from the UK and Switzerland?

Although Switzerland and the UK generally follow the EEA's lead in data protection matters, because those countries are not part of the EEA, the New SCCs, standing alone, do not cover transfers of personal data from those countries to non-adequate third countries.

To address that issue, the Swiss Federal Data Protection and Information Commissioner issued **guidance** in August 2021 on the use of the New SCCs for transfers of personal data from Switzerland to non-adequate third countries. That guidance confirmed that the New SCCs can be used for those transfers as long as the parties add a short annex to the New SCCs to align certain of their provisions with Swiss data protection law.

The UK, for its part, has **approved** two new data transfer tools to address the transfer of personal data from the UK to third countries: a UK-specific "International Data Transfer Agreement," and a "UK Addendum" to the New SCCs that can be added to the New SCCs and allows for the New SCCs to be used to provide appropriate safeguards for transfers of personal data from the UK to inadequate jurisdictions.

How does SAS use the New SCCs?

As a global corporation with subsidiaries, affiliates, business partners, and customers in many countries,SAS understands that the delivery and use of its offerings often result in transfers of personal data from the EEA, Switzerland, and the United Kingdom to the United States and other third countries that have not obtained an adequacy finding.

To help customers comply with their obligations under GDPR with respect to those transfers, SAS' **Universal Terms** incorporate a Data Processing Addendum ("DPA") that includes, by default, the New SCCs and the corresponding Swiss annex and UK Addendum. Under the terms of SAS' DPA, those mechanisms apply to transfers of personal data originating in the EEA, Switzerland, and/or the UK from the customer, as the data exporter, to SAS and its affiliates that are located in third countries, as the data importers.

Where necessary to comply with GDPR and its contractual commitments to customers and business partners, SAS also relies on the New SCCs and the corresponding Swiss annex and UK Addendum for intercompany transfers of personal data between and among its global affiliates, and to its third-party suppliers and subcontractors.

My company has an existing DPA with SAS that relies on the Old SCCs. Can I update the DPA to include the New SCCs?

Yes – SAS stands ready to amend its DPAs with customers to bring those DPAs up to date with the latest requirements of applicable data protection laws and regulations, including the incorporation of the New SCCs. If you would like to request such an amendment, please contact your SAS representative.

What else has SAS done to address the *Schrems II* ruling and the EDPB's recommendations?

In addition to updating its DPA to include the New SCCs and the corresponding Swiss annex and UK Addendum, SAS has taken two other key steps to address the *Schrems II* ruling, both of which are outlined in our **FAQ on Transfer Impact Assessments**.

First, SAS has assessed the practical application of the surveillance laws and practices in the United States that were at issue in *Schrems II* to SAS' business and offerings. As a result of that assessment, SAS has concluded that it can provide an essentially equivalent level of protection for personal data it receives from customers in the EEA, Switzerland, and the UK when they use SAS' offerings, despite the existence of those laws and practices.

Second, SAS has implemented and continues to maintain various Supplementary Measures, including contractual, organizational, and technical measures, to provide customers with additional assurances regarding the protection of personal data that SAS processes on their behalf. Those measures are detailed in our **FAQ on Transfer Impact Assessments**.

Where can I find the latest version of the SAS DPA?

The latest version of SAS' Customer DPA is available in English language for download on our **SAS Trust Center** website and also on **SAS Agreements**.

Does SAS also rely on transfer mechanisms other than the SCCs?

No, SAS currently relies exclusively on the New SCCs to ensure an adequate level of protection when SAS processes EEA and UK personal data on behalf of its customers. SAS does, however, actively monitor legal and regulatory developments that could impact how it conducts international transfers, and could in the future adopt additional or different transfer mechanisms if it determines doing so will be beneficial to our customers and their use of our offerings.

What kinds of personal data does SAS process on customers' behalf?

The personal data SAS processes on behalf of a particular customer depends on the SAS offerings that customer uses, and the data the customer chooses to process through those offerings. In general, however, customers commonly process the following categories of personal data:

- Business contact details.
- Personal contact details.
- Human resources data.
- System access / usage / authorization data.
- Contract and invoice data.

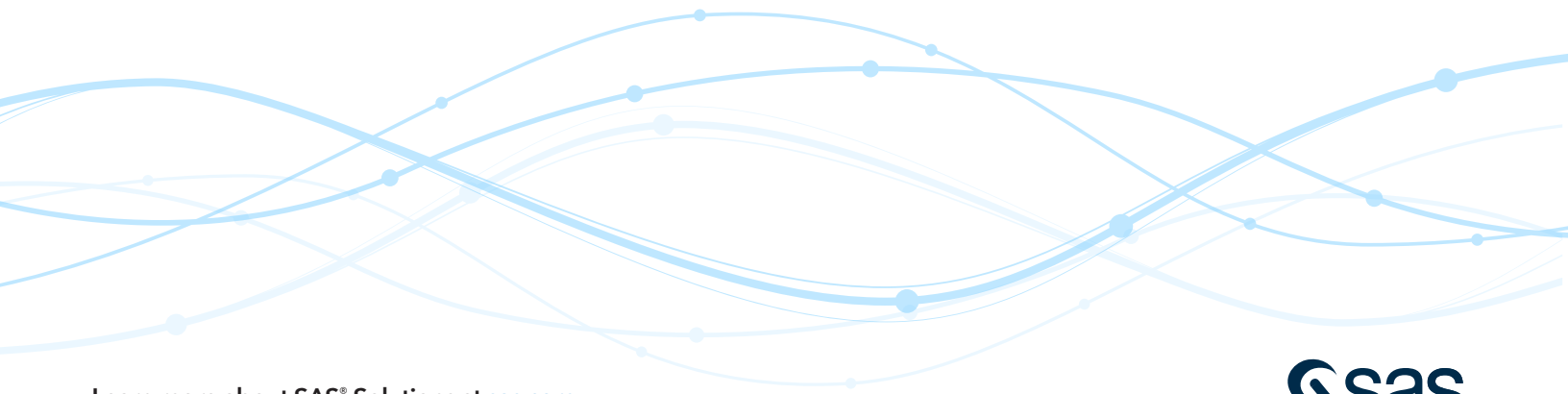
Does SAS process any special categories of personal data?

SAS does typically not process special categories of personal data on behalf of its customers, and SAS' DPA prohibits customers from providing these categories of personal data to SAS unless the parties have specifically agreed otherwise.

In some cases, however, where the processing of special categories of personal data is necessary for a customer to effectively use SAS' offerings, SAS can agree to process special categories of personal data on the customer's behalf, subject to terms specifically agreed upon between SAS and the customer.

Where can I get more information on the processing and transfer of personal data by SAS?

For more information on the processing and international transfers of personal data in connection with SAS' offerings, please visit our **Trust Center**. For specific questions that aren't answered in the Trust Center, please contact your SAS representative.



Learn more about SAS® Solutions at sas.com.