Transfer Impact Assessments FAQs

Contents

1. What is the purpose of these FAQs?

These FAQs are intended to provide support for our customers in their transfer impact assessments ("TIAs") when they use the SAS® Cloud. The FAQs track the **recommendations** published by the European Data Protection Board ("EDPB recommendations") following the Court of Justice of the European Union's decision in Schrems II. For an overview of Schrems II and the EDPB Recommendations, please visit our **FAQs on International Transfers of Personal Data**.

Please note that the information below is intended to help SAS Cloud customers conduct their own independent assessments in consultation with their legal counsel and compliance teams. It is provided "as is," for informational purposes only, and does not constitute legal advice.

2. What is the purpose of a TIA?

A TIA is meant to determine whether personal data transferred outside the EU or countries deemed by the European Commission to provide "adequate protection" for personal data will be subject to a level of protection that is "essentially equivalent" to that guaranteed within the EU.

In conducting TIAs, data exporters must evaluate, among other things, the transfer tool used, the circumstances of the transfer, the laws and practices in the receiving jurisdiction that might allow government authorities to access or obtain the transferred personal data, the likelihood that transferred personal data would be subject to governmental requests or direct access, and any "supplementary measures" that the parties have implemented to ensure an essentially equivalent level of protection.

3. What is a transfer tool?

Under the European Union's General Data Protection Regulation ("GDPR"), personal data cannot be transferred outside of the EU unless an appropriate transfer tool is in place. Under GDPR, these transfer tools include:

- (i) a decision by the European Commission under Article 45 of GDPR that the importing country ensures an "adequate level of protection" for personal data;
- (ii) the implementation by the data exporter of "appropriate safeguards" described in Article 46 of GDPR, such as Standard Contractual Clauses ("SCCs") or binding corporate rules, that serve to ensure that the Personal Data transferred is subject to an adequate level of data protection in the importing country; or
- (iii) derogations under Article 49 of GDPR, which can be used in limited circumstances when the other transfer tools do not apply.

4. Why is reliance on a transfer tool identified in GDPR Article 46 (such as the SCCs) not sufficient, and why is a TIA needed?

In its recommendations, the EDPB explained that SCCs and other transfer tools described in Article 46 of GDPR "do not operate in a vacuum," and that under the decision in Schrems II, data exporters relying on those tools to transfer personal data to a third country must still verify, on a case-by-case basis, if the law or practices in that third country "impinge on the effectiveness of the appropriate safeguards contained in the . . . transfer tools."

As a result, even when a data exporter relies on a transfer tool described in Article 46 of GDPR (such as the SCCs), the data exporter must still assess whether the law and practices in the third country – especially with respect to public authorities' ability to request and obtain personal data – could undermine the protections offered by that transfer tool, and if so whether supplementary measures can be implemented to address any gaps.

In addition, the updated SCCs issued by the EU Commission pursuant to Article 46 of GDPR in June 2021 impose a separate and independent obligation to conduct a TIA on exporters that rely on that tool for transfers of personal data to third countries.

5. What are the EDPB's recommendations for conducting a TIA?

The EDPB Recommendations outline six steps for data exporters to take when conducting a TIA:

- **Step 1:** Know your transfers – perform a mapping of all transfers of personal data to third countries, to identify where personal data may be located or processed.
- **Step 2:** Identify the transfer tool(s) that will be used, such as an adequacy decision under Article 45 of GDPR or a transfer tool listed in Article 46 of GDPR.
- **Step 3:** If relying on a transfer tool listed in Article 46 of GDPR, such as the SCCs, assess whether the tool is effective in light of all circumstances of the transfer, taking into account the laws or practices of the importing country.
- **Step 4:** If necessary in light of the assessment undertaken in Step 3, identify and adopt supplementary measures to bring the level of protection for the data transferred up to the standard of "essential equivalence."
- **Step 5:** Take any formal procedural steps that the adoption of the supplementary measures may require.
- **Step 6:** Re-evaluate, when appropriate, the level of protection for personal data transferred to third countries and monitor any developments that may affect the transfers.

6. What information does SAS provide to help customers carry out TIAs?

To help its customers conduct the required TIA when they act as data exporters in transferring EU personal data to SAS, SAS is providing the information below with respect to each of the EDPB recommended steps.

Step 1: Know your transfers

The first step in the EDPB recommendations requires data exporters to identify the locations to which the personal data may be transferred.

SAS Cloud customers located in the EU have the option to use hosting environments located within the EU based on the "EU only" principle. When a customer selects that option:

- The physical and logical infrastructure used to provide the SAS Cloud offerings will reside within the EU, as will the associated backup facilities.
- SAS will not store customer data outside the EU.
- SAS will rely primarily on personnel located within the EU for the delivery of its services, will limit the number of individuals with remote access to customer data from outside of the EU, and will only allow remote access to customer data by personnel outside the EU where necessary, such as for emergency support. In those cases, the non-EU personnel may be located in the United States or other countries in which SAS support personnel are located, and their access will be logged and monitored.

For customers that do not select the "EU only" option with respect to their use of SAS Cloud offerings, personal data processed through those offerings may be stored in, or regularly accessed by, SAS personnel or subprocessors in countries outside the EU. The specific countries will vary based on the particular offering and the customer's location, among other factors. For information that about the locations to which personal data processed by SAS in connection with a particular SAS Cloud engagement may be transferred, please contact your SAS representative.

Step 2: Identify the transfer tool you are relying on

Step 2 requires that data exporters identify the transfer tool that it is relying on for transfers of personal data to third countries.

For its processing of EU personal data in connection with SAS Cloud offerings, SAS relies on the standard contractual clauses annexed to Commission Implementing Decision (EU) (2021/914) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/279 of the European Parliament and of the Council (the "EU SCCs").

Under SAS' standard **Customer Data Processing Addendum**, SAS agrees to enter into the EU SCCs with the customer when the customer acts as the data exporter in a transfer of personal data originating in EU and SAS is located in a third country and acts as the data importer.

Step 3: Assess the laws or practices of the recipient country and their impact on the effectiveness of the transfer tool

The EDPB Recommendations provide that, in Step 3, data exporters relying on a transfer tool under Article 46 of GDPR must consider whether the "practices in force in the third country" could undermine the protections offered by that transfer tool.

SAS has assessed the publicly available information related to the laws and practices of the United States and other countries outside the EU to which personal data may be transferred in connection with its customers' use of the SAS Cloud. Based on this assessment, SAS has concluded that these laws and practices do not prevent it from fulfilling its obligations under the EU SCCs in regard to transfers of personal data outside of the EU and are compatible with commitments made by SAS in the EU SCCs.

Given the focus of the Schrems II judgement on US law, and SAS' status as a US-headquartered company, US law is particularly relevant. To that end, SAS has conducted a review of the potential impact of the laws at issue in Schrems II – Section 702 of FISA and Executive Order 12333 – on SAS, taking into account the circumstances of the transfers that occur between SAS and its customers when they use the SAS Cloud. Based on that review, and taking into account SAS' practical experience (including the absence of any US government requests for personal data to any SAS entity to date), SAS has concluded that the risks posed by those provisions either do not apply to SAS' processing of personal data on its customers' behalf, or can be sufficiently mitigated by supplemental contractual, technical, and organizational measures that SAS offers in connection with the SAS Cloud. For more information, please see SAS' **Statement on Adequacy, Supplementary Measures and Response to Government Data Access Requests**.

SAS has made similar assessments of the laws and practices in other countries in which it processes personal data on behalf of SAS Cloud customers, and before opening a data center in a new country, SAS conducts a rigorous assessment of local laws to validate the data in the country will be hosted in a manner consistent with SAS obligations to its customers.

Step 4: Identify and implement supplementary measures

Step 4 of the EDPB Recommendations requires data exporters to identify supplementary measures that may be used bring the level of protection of the personal data transferred up to the required standard of "essential equivalence." Data exporters need to take this step only if their assessment in Step 3 reveals that the laws or practices of the destination country could negatively impact the effectiveness of the transfer tool. These measures can fall into three categories: contractual, technical, and organizational.

This section summarizes the various contractual, technical, and organizational measures that SAS makes available to SAS Cloud customers to ensure that an equivalent level of protection exists for EU personal data that they process through their use of SAS Cloud offerings.

Contractual measures

SAS' Customer Data Processing Addendum includes several contractual measures suggested by the EDPB Recommendations, including:

- A commitment by SAS to implement specific technical and organizational security measures with respect to personal data processed through the SAS Cloud to protect that personal data against unauthorized access, including the encryption of personal data in transit and at rest.
- A commitment by SAS, pursuant to the EU SCCs between SAS and the customer, to provide the customer, at regular intervals, with information on requests received from public authorities for the disclosure of personal data transferred to SAS by the customer.
- A commitment by SAS to take steps to resist any binding order for compelled disclosure of personal data transferred to SAS by the customer, and to only disclose the minimum amount of personal data necessary to satisfy the order when SAS remains compelled to disclose personal data.
- A commitment by SAS to promptly inform the customer of any changes to the legislation applicable to SAS that could undermine the protections provided for personal data in the Data Processing Addendum.

Technical Measures

SAS relies on several technical measures to ensure the protection of personal data transferred to it by SAS Cloud customers which are described below.

Data Protection and Security Standards

Data protection and security are of paramount importance to SAS. With respect the SAS Cloud, SAS holds several certifications, including ISO 27001, ISO27017 and ISO27018, SOC 2 Type II, and SOC 3. For more information, please see our White Paper **Security in the SAS Cloud**.

SAS' software solutions are also subject to rigorous security and quality processes. For details on SAS product security, please see our white paper ***The Quality Imperative: SAS' Commitment to Quality***, which outlines the security controls that SAS uses in connection with the development of its software solutions.

Access Controls

SAS maintains strict administrative, technical, and physical measures to protect information processed through the SAS Cloud. Access to personal data is limited through login credentials to those employees who require it to perform their job functions. In addition, SAS uses controls such as multi-factor authentication, single sign-on, access on an as-needed basis, strong password controls, and restricted access to administrative accounts to prevent unauthorized access to personal data in the SAS Cloud.

Encryption

Encryption is an important technical measure that can prevent unauthorized direct access to personal data by public authorities, including as might arise in connection with government surveillance programs like those discussed in the *Schrems II* decision. SAS encrypts customer data in transit to prevent this access.

Pseudonymisation

SAS encourages all customers to pseudonymize personal data processed by SAS before transferring that personal data to SAS. The pseudonymization key should be held only by the customer. For products or services where data must be processed "in the clear," personal data is encrypted in transit and at rest, and kept in the clear for the minimum time period necessary.

Organizational measures

SAS has implements robust organizational measures to protect transferred personal data in the SAS Cloud, including internal policies, procedures, and standards for information security, asset management, human resources security, physical and environmental security, operations management, access control, security incident management, and business continuity management. These measures are regularly audited by third parties, including in connection with SAS' ISO 27001 certification and annual SOC 2 Type II and SOC 3 audits.

In addition, SAS has implemented data minimization measures that are designed to limit the possibility that personal data in the SAS Cloud will be subject to unauthorized access. To that end, when SAS operates cloud services for customers who have requested to use cloud environments hosted exclusively within the European Union, SAS does not store their personal data outside the European Union, and limits remote access to its personnel located within the European Union to the greatest extent possible.

Step 5: Formal procedural steps needed to adopt the supplementary measures

Step 5 under the EDPB recommendations is to take any formal procedural steps required to effectively implement any supplementary measures adopted under Step 4.

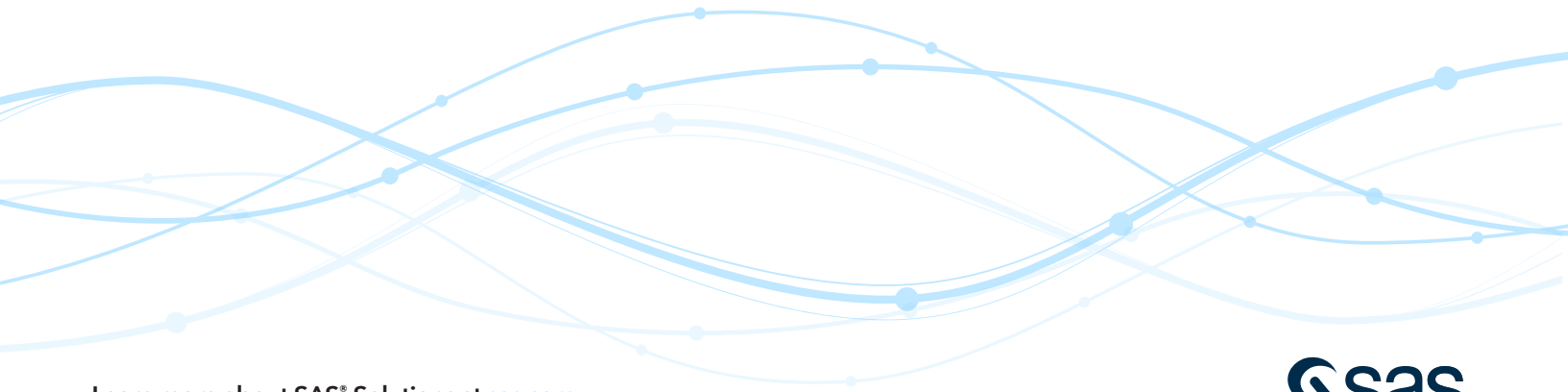
As noted above, many of the supplementary measures that SAS has implemented are incorporated into in SAS' Customer Data Processing Addendum, and thus are legally binding on SAS by virtue of the customer's agreement with SAS.

Step 6: Re-evaluate the level of protection at appropriate intervals

Step 6 under the EDPB recommendations requires the data exporter to re-evaluate, at appropriate intervals, the protection afforded to personal data in third countries to which the data exporter transfers personal data, and to monitor any developments that may affect the initial assessment of the level of protection in those countries.

SAS closely monitors developments in the laws and practices of the United States and other countries in which it processes personal data, and updates its agreements, policies, and procedures as necessary to address those developments.

To help customers carry out this step, SAS also commits, in its Customer Data Processing Addendum, to promptly notify its customers of any change in legislation applicable to SAS or its sub-processors that could have a substantial adverse effect on the commitments SAS makes in its Customer Data Processing Addendum with respect to the protection of personal data.



Learn more about SAS® Solutions at sas.com.