Transfer Impact Assessments for SAS Hosted Managed Services Customers

This document assists SAS Customers by providing them with information regarding Transfer Impact Assessments concerning SAS Hosted Managed Services ("**HMS**") products and services. Please note that the responsibilities and liabilities of SAS to its Customers are controlled by the applicable agreements between SAS and its Customers including the Data Processing Agreement ("DPA") as applicable, collectively (the "Agreement"). This document is not part of, nor does it modify, any agreement between SAS and its Customers.

Capitalised terms used but not defined in this document will have the meanings provided in the Agreement.

The steps listed below reflect those identified by the European Data Protection Board ("EDPB") in the **EDPB Recommendations 01/2020 Version 2.0 adopted 18 June 2021**, ("EDPB Recommendations"). The EDPB Recommendations provide guidance on how to conduct Transfer Impact Assessments to evaluate whether there is an essentially equivalent level of protection for data transfers to locations outside of the European Economic Area ("EEA"), following the July 2020 judgment of the European Court of Justice in *Schrems II.* Additionally, in a Transfer Impact Assessment, SAS and Customers must consider the EU-US, Swiss-US Data Privacy Framework with UK Extension (the "DPF"). SAS completed its DPF certification in October 2023.

Step 1: Know your transfers.

For HMS products and services, SAS and its affiliated sub-processors may potentially process Customer personal data in the following non-EEA countries: India, United Kingdom, and the United States.

Step 2: Identify the transfer tools you are relying on.

In connection with HMS products and services, SAS transfers Customer personal data to its partners and affiliates in the following countries found to be adequate by the European Commission for transfers of EU personal data: United Kingdom. Following its withdrawal from the European Union, the United Kingdom has found Canada, Japan, and the European Union to be adequate for transfer of UK personal data. Where a country has been found to be adequate, international transfer safeguards and transfer risk assessments are not required.

For transfers of EU personal data to affiliates within the SAS corporate member group, where the recipients are located in non-adequate countries, SAS relies on its Intra-group Data Transfer Agreement ("IGDTA") which contains the EU Standard Contractual Clauses ("SCCs") and the UK Addendum to such SCCs.

In some cases, SAS and its sub-processors rely on the Standard Contractual Clauses ("SCCs") to transfer data to non-adequate countries, as provided in our DPA. SAS has committed to implement supplementary measures to safeguard EU and UK personal data following the *Schrems II* judgment. These supplementary measures can be found in Schedule 2 of the SAS DPA. Further details on supplemental security measures for HMS are documented in the SAS Security Governance Manual, available on reasonable customer request and upon customer's execution of a non-disclosure agreement with SAS. Details about our sub-processors can be found at this link on the SAS Trust Center page.

Step 3: Assess whether the Article 46 GDPR transfer tool relied upon is effective in light of all circumstances of the transfer.

SAS has assessed the laws or practices of third countries to which EU or UK personal data will be transferred in order to evaluate whether these laws could impinge upon the effectiveness of the relevant transfer tools.

Provided below are overviews of relevant legislation in key non-adequate jurisdictions where SAS operates for the provision of HMS.

India: India has two laws that could permit electronic surveillance of personal data:

- Section 5(2) of the Telegraph Act (1885) allows the Indian government to intercept and disclose electronic or telephonic messages on the occurrence of any public emergency or in the interest of public safety.

- Section 69 of the Information Technology Act (2000) allows the Indian government to intercept, monitor, or decrypt any information received or stored through any computer resource if such activity is "necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence."

The Supreme Court of India has recognized the right to privacy as a fundamental right under the Indian Constitution, which limits the scope of application of these Indian surveillance laws. In particular, under applicable rules, any interception, monitoring, or decryption of electronic information by the Indian government must be approved by a competent authority (e.g., the Union Home Secretary), and such approval is subject to mandatory periodic reviews.

Taking into account the practices of the Indian public authorities, and the fact that SAS has never been subject to an Indian government request for access to customer personal data, SAS concludes that:

- India surveillance laws and regulations that are potentially applicable to SAS' processing of personal data are unlikely to be applied in practice to customer data processed by SAS; and
- Consequently, SAS has no reason to believe that such laws and regulations will prevent SAS from fulfilling its obligations under the SCCs.

United States:

The Schrems II decision invalidated the prior US adequacy decision provided through the EU-US Privacy Shield. After this CJEU decision, the EU Commission and the US government worked to develop a new privacy and security framework that would provide an adequate level of protection for data accessed by those in the United States.

The Executive Order on Enhancing Safeguards for US Signals Intelligence Activity was issued on October 7, 2022. The Executive Order follows the March 2022 announcement of President Biden and European Commission President Ursula von der Leyen of an agreement on a new framework for transatlantic data

flows, known as the EU-US Data Privacy Framework ("DPF"). The Executive Order addresses concerns that were highlighted by the 2020 CJEU *Schrems II* case, including the establishment of the Data Protection Review Court, which will allow EU citizens redress. Additionally, the Executive Order provides additional safeguards on U.S. intelligence activities to ensure such activities are necessary and proportionate. The steps in the Executive Order provided the European Commission with a basis to adopt a new U.S. adequacy decision in 2023.

On 10 July 2023, the European Commission has adopted an adequacy decision for the United States, for those companies that participate in the EU-U.S. Data Privacy Framework ("DPF"). **The United States ensures an adequate level of protection for personal data transferred from the EU to US companies under the new framework.**

The framework includes important safeguards and limitations intended to address concerns about such access to data by the U.S. government. Key points regarding government access under the DPF include:

1. The U.S. government has committed that any access to personal data for national security purposes will be conducted in a manner that is necessary and proportionate. This means that data access should be limited to what is strictly required and should not involve excessive or indiscriminate data collection.

2. The framework includes mechanisms to ensure that individuals can seek redress if they believe their data has been improperly accessed by U.S. authorities. This includes the creation of an independent Data Protection Review Court (DPRC) that allows individuals to file complaints and seek remedies regarding government access.

3. The U.S. government issued in 2022 Executive Order 14086, as part of its effort to address concerns raised by the Court of Justice of the European Union (CJEU) in the Schrems II decision. It sets out additional safeguards, including stricter oversight and accountability for U.S. intelligence agencies, and reinforces the commitment to limit access to data to what is necessary and proportionate.

SAS is certified under the DPF. SAS is officially listed and on the active list of DPF in the following link, https://www.dataprivacyframework.gov/list.

Step 4: Adopt supplementary measures.

If a Customer's assessment finds that the transfer tool in Step 2 alone would not provide an essentially equivalent level of protection, then the Customer should identify supplemental contractual, technical and/or organisational measures to enhance the protection of the Personal Data.

SAS implements and maintains appropriate technical and organisational security measures, which are set out in Schedule 2 of the SAS DPA.

Step 5: Procedural steps if you have identified effective supplementary measures.

Customer should take any formal procedural steps that may be required in order to implement the supplementary measure(s).

SAS has concluded SCCs with its Customers and with its third-party vendors, which include supplementary measures that are permissible amendments to the SCCs. No additional procedural steps are required.

Step 6: Re-evaluate at appropriate intervals.

Customer should re-evaluate the level of protection afforded to personal data being transferred to third countries at appropriate intervals, including monitoring to assess whether there have been any relevant developments.

SAS reviews and, where necessary, adapts the supplementary measures it has implemented at least once per year to address data protection regulatory developments and risk environments.