Transfer Impact Assessments for SAS CI-360 Customers

This document assists SAS Customers by providing them with information regarding Transfer Risk Assessments concerning SAS CI-360 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*.

Step 1: Know your transfers.

For CI-360 products and services, SAS and its sub-processors may potentially process Customer personal data in the following non-EEA countries: Argentina, Australia, Brazil, Canada, India, Japan, New Zealand, Philippines, South Korea, United Kingdom, and the United States.

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

In connection with CI 360 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: Argentina, Canada, New Zealand, Japan, South Korea and the 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").

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 CI 360 services 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 CI 360 services.

Australia: Australia has conditions on the access to and use of personal information by public authorities, such as requiring warrants issued by certain judges, the Attorney General or the Director General of Security. The Privacy Commissioner is responsible for oversight and enforcement of the Privacy Act and the 13 Australian Privacy Principles ("APPs"), which includes complaints made by individuals about invasions of their privacy and/or breaches of the APPs.

Australia's Telecommunications (Interception and Access) Act 1979 (TIA Act) limits government surveillance by prohibiting interception of communications and access to stored communications. Privacy is also protected by the Telecommunications Act 1997, which prohibits telecommunications service providers from disclosing information about their customers' use of telecommunications services.

The TIA Act sets out certain exceptions to these prohibitions to permit eligible Australian law enforcement and security agencies to (1) obtain warrants to intercept communications, (2) obtain warrants to access stored communications, and (3) authorize the disclosure of data. Such agencies can only obtain warrants or give authorizations for national security or law enforcement purposes set out in the TIA Act.

Australia's Surveillance Devices Act 2004 (SD Act) governs the use of surveillance devices by law enforcement and security agencies. Under the SD Act, an eligible agency can apply for a warrant to use a surveillance device to investigate a relevant criminal offense.

The Attorney General's Department of Australia administers both the TIA Act and the SD Act. Neither law has been used to access the kinds of commercial information collected and processed by SAS.

Australia's electronic surveillance laws are in the process of being reconsidered and may change in the coming years. The Australian government recently completed a consultation on a discussion paper on the reform of Australia's electronic surveillance framework that recommended updating existing laws.

Australia has signed and adopted the following privacy related commitments: International Covenant on Civil and Political Rights; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Asia-Pacific Economic Cooperation Privacy Framework; and APEC Cross Border Privacy Rules.

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

- Australian 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.

Brazil: In the same path as the GDPR and the Data Protection Directive with respect to Law Enforcement (Directive (EU) 2016/680), Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.873 of 8 July 2019) ("LGPD") excludes from its application the processing of personal data for the exclusive purposes of public security, national defense, state security or activities of investigation or prosecution of criminal offenses. Public authorities can only process personal data to achieve its public purpose, in pursuit of the public interest, and for the purpose of performing the legal duties. The Brazilian data protection authority ("ANPD") was established by Articles 55-A to 55-L of the LGPD and is an independent supervisory authority. The Brazilian Constitution provides a right to any individual to submit any injury or threat for judicial review and the LGPD expressly allows the defense of interests and rights of data subjects within court.

Brazil's Wiretap Act (Law No. 9.296/1996) regulates the right of police authorities and the public prosecutor office to intercept telecommunications. A court order is required, and the interception must satisfy several high standards, including (1) there is reasonable evidence of participation in a criminal offense, (2) there are no other available means of obtaining the additional evidence that interception of telecommunications will provide, and (3) the crime being investigated constitutes an offense punishable with a prison sentence. Furthermore, the court issuing the order continues to be involved, requiring a transcript and report regarding the intercepted communications.

In addition, Brazil's Civil Rights Framework for the Internet (Law No. 12.965/2014) requires prior judicial authorization to access metadata and communications content. Authorities can also access the stored content of seized devices, provided that the search and seizure procedure was authorized by a judge.

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

- Brazilian 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.

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.

Philippines: The Constitution of the Republic of the Philippines (1987), Article III, Section 2 of the Constitution provides that a search warrant or warrant of arrest may be issued upon probable cause, personally determined by the judge after examination under oath or affirmation of the complainant and the witnesses (as applicable), and particularly describing the place to be searched and the persons or things to be seized. Article III, Section 3 of the Constitution provides that the privacy of communication and correspondence are inviolable, except with lawful order of

the court, or when public safety or order requires otherwise as prescribed by law. The Data Privacy Act provides that the processing of personal information shall be lawful where it is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data. The National Privacy Commission is an independent supervisory authority to monitor and validate compliance with the Data Privacy Act. Data subjects may lodge a complaint with the National Privacy Commission, file a civil case under Article 32 of the Civil Code for damages or lodge a criminal complaint under Sections 25-32 of the Data Privacy Act.

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

- Philippine 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: SAS is a United States corporation formed and registered in the State of North Carolina, subject to United States law. Under existing case law, SAS is a remote computing service ("RCS") as defined in the Electronic Communications Privacy Act ("ECPA"), Section 2711 of Title 18 U.S.C. when it provides Services to Customers. ECPA does not permit law enforcement authorities to access data stored with an RCS provider unless they first obtain a warrant, subpoena, or court order. Providers of remote computing services may also be subject to Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702") if they store electronic communications.

Consistent with the EDPB Recommendations, SAS Customers should consider not only the legal framework of the jurisdiction of the data importer but also practical experience "with relevant prior instances of requests for access received from public authorities outside the EEA."

SAS does not provide assistance to U.S. authorities conducting surveillance under Executive Order 12333 ("EO 12333"). EO 12333 does not authorise the U.S. Government to require companies to provide assistance in collecting foreign intelligence information, and SAS will not voluntarily do so. To date, SAS has not received **any** government requests for customer data anywhere in the world.

Helpful context in relation to U.S. surveillance laws is provided in a White Paper entitled, "**U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II**" ("White Paper"), which was issued jointly by the U.S. Department of Commerce, the Department of Justice, and the Office of the Director of National Intelligence in September 2020. The White Paper clarifies that:

- "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*."
- "There is a wealth of public information about privacy protections in U.S. law concerning government access to data for national security purposes, including information not recorded in Decision 2016/1250, new developments that have occurred since 2016, and information the ECJ neither considered nor addressed. Companies may wish to take this information into account in any assessment of U.S. law post-*Schrems II*."
- "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."
- "The theoretical possibility that a U.S. intelligence agency could unilaterally access data being transferred from the EU without the company's knowledge is no different than the theoretical possibility that other governments' intelligence agencies, including those of EU Member States, or a private entity acting illicitly, might access the data. Moreover, this theoretical possibility exists with respect to data held anywhere in the world, so the transfer of data from the EU to the United States in particular does not increase the risk of such unilateral access to EU citizens'

data. In summary, as a practical matter, companies that fall in this category have no reason to believe their data transfers present the type of data protection risks that concerned the ECJ in *Schrems II*."

- In Schrems II, the ECJ voiced concern about whether U.S. law provides individual redress for violations of the FISA 702 program. "A review of applicable U.S. law demonstrates that several U.S. statutes authorize individuals of any nationality (including EU citizens) to seek redress in U.S. courts through civil lawsuits for violations of FISA, including violations of Section 702. This information was not addressed by the ECJ in *Schrems II*. For example, the FISA statute itself empowers a person who has been subject to FISA surveillance and

  whose communications are used or disclosed unlawfully to seek compensatory damages, punitive damages, and attorney's fees against the individual who committed the violation. The Electronic Communications Privacy Act provides a separate cause of action for compensatory damages and attorney's fees against the government for willful violations of various FISA provisions. Individuals may also challenge unlawful government access to personal data, including under FISA, through civil actions under the Administrative Procedure Act ("APA"), which allows persons 'suffering legal wrong because of' certain government conduct to seek a court order enjoining that conduct."

  - "The following statutes establish means of individual redress for violations of FISA 702:

    Section 1810 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1810 (2018)

    Section 2712 of the Electronic Communications Privacy Act, 18 U.S.C. § 2712 (2018)

    Section 702 of the Administrative Procedure Act, 5 U.S.C. § 702 (2018)."

  - "...[I]n early 2018, the U.S. Congress passed, and the President signed into law, additional privacy protections and safeguards relating to FISA 702 through amendments to FISA and other statutes. These amendments included (1) requiring that with each annual FISA 702 certification, the government must submit and the FISC [Foreign Intelligence Surveillance Court] must approve querying procedures, in addition to targeting procedures and minimization procedures; (2) requiring additional steps including notification to Congress before the government may resume acquisition of 'about' collection under FISA 702; (3) amending the enabling statute for the PCLOB [U.S. Privacy and Civil Liberties Oversight Board] to allow it to better exercise its advisory and oversight functions; (4) adding the Federal Bureau of Investigation and NSA to the list of agencies required to maintain their own Privacy and Civil Liberties Officers, instead of being subject only to their parent department-level officers, to advise their agencies on privacy issues and ensure there are adequate procedures to receive, investigate, and redress complaints from individuals who allege that the agency violated their privacy or civil liberties; (5) extending whistleblower protections to contract employees at intelligence agencies; and (6) imposing several additional disclosure and reporting requirements on the government, including provide annual good faith estimates of the number of FISA 702 targets. The ECJ's basis in *Schrems II* for invalidating Decision 2016/1250 obviously could not have taken into account these additional FISA 702 privacy safeguards, which were introduced after Decision 2016/1250 was issued.

> Companies, however, may take into consideration these additional FISA 702 privacy safeguards in their own independent reviews of current U.S. law for purposes of SCC transfers."

The Executive Order On Enhancing Safeguards for United States Signals Intelligence Activities 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. For more details, please see The White House Fact Sheet. 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. 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/s/participant-search.

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.