SAS Institute Inc.
EU/UK-US Transfers: Adequacy, Supplementary Measures and Response to Government Data Access Requests

Last Updated October 2022

SAS Institute Inc. (together with its subsidiaries and affiliates, "SAS") provides this statement to assist its customers in determining that there is an adequate level of protection for personal data transferred to or accessed by SAS, taking into account the July 16, 2020 judgment of the EU Court of Justice (CJEU) in Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems ("Schrems II").

Background: In Schrems II, the CJEU invalidated the EU-US Privacy Shield based in part on the potential harm to data subject rights caused by US government surveillance carried out under Section 702 of FISA and Executive Order 12333. The CJEU also referred to PRISM and UPSTREAM, two US surveillance programs revealed by the Edward Snowden leaks.

Importantly, the CJEU stated that Standard Contractual Clauses ("SCCs") ***may be used*** for transfers of personal data to the United States where the SCCs, together with any other safeguards that may be added, provide adequate protection for the personal data in light of EO 12333 and FISA § 702.

This statement outlines (i) the absence of any US government data request to any SAS entity to date and the low risk of a data request in the future, and (ii) the supplemental measures (contractual, organisational and technical) SAS uses, together with the June 2021 SCCs, in order to help data controllers ensure that transfers are compliant with the Schrems II ruling.

In summary, the risks posed by US legal provisions either do not apply to SAS's processing of personal data or can be sufficiently mitigated by supplemental contractual, technical and organisational safeguards that SAS offers.

1. **Low Risk of Government Access Request**
   The European Commission in its June 2021 Implementing Decision for the new SCCs, and the EDPB Final Guidelines released June 21, 2021 confirm that controllers are permitted to take into account how the US laws are applied *in practice.* SAS has never received a government request in the past and is unlikely to ever receive such a request.

a. Because SAS is not a public communications carrier, it is highly unlikely that SAS would ever be subject to a government request for data.

To date, *no SAS entity worldwide* has received an access request for customer data from a law enforcement authority or state security body. This includes access requests and known surveillance under any of the programs listed by the CJEU in the Schrems II ruling. The nature of SAS's business hosting data and providing analytics solutions to *commercial* customers makes SAS an unlikely candidate for such surveillance. The US Department of Commerce has confirmed this low risk as stated in its recent whitepaper on this topic, according to which most EU companies "do not, and have no grounds to believe they do, deal in any data that is of any interest to intelligence agencies." [page 2].

Moreover, in the event any such personal data processed by SAS were relevant to such an investigation, the government is more likely to seek such data through other forms of legal process (such as a search warrant approved by a judge) that do satisfy the high standards for government access to data described in the Schrems II decision. This is because it would be much faster and easier for the government to seek an order or warrant under something other than FISA § 702 than to put in place the mechanisms required for the government to serve directives on SAS under FISA § 702. For any such request SAS would follow the clearly defined legal process as described below.

b. *SAS is not eligible to receive "upstream" or bulk surveillance orders under FISA § 702*

SAS acts, in part, as an electronic communications service ("ECS") in connection with certain services or product features we provide to customers. SAS thus is among the large group of companies upon which the US government could serve a targeted directive under FISA § 702. However, as the U.S. government has interpreted and applied FISA § 702, SAS is <u>not</u> eligible to receive the type of order that was of principal concern to the CJEU in the Schrems II decision—i.e., a FISA § 702 order for "upstream" surveillance. As the U.S. government has applied FISA § 702, it uses upstream orders *only* to target traffic flowing through internet backbone providers that carry Internet traffic for third parties (i.e., telecommunications carriers).

SAS does not provide such Internet backbone services, as we only carry traffic involving our own customers. As a result, we are not eligible to receive the type of order principally addressed in, and deemed problematic by, the Schrems II decision.

c. *SAS does not assist — and cannot be ordered to assist — U.S. authorities in their collection of information under Executive Order 12333.*

SAS does not and will not provide any assistance to U.S. authorities conducting surveillance under EO 12333. EO 12333 does not provide the U.S. government the ability to compel companies to provide assistance with those activities, and SAS will not do so voluntarily. As a result, SAS does not, and cannot be ordered to, take any action to facilitate the type of bulk surveillance under EO 12333 which the Schrems II decision deemed problematic.

2. <u>Supplemental Measures</u>

a. <u>*Contractual Measures*</u>

SAS agrees to be bound by the SCCs. If you have entered into an agreement with or are otherwise obtaining services from SAS that will require SAS to process your personal data in the UK or European Economic Area ("European Data") from territories outside the EEA or UK, SAS will agree to be bound by the SCCs and certain supplemental clauses outlining the organizational and technical measures SAS has in place to protect your European or UK Data.

b. <u>*Organisational Measures*</u>

- <u>Process for responding to any access request</u>

  If a SAS entity may receive an access request for hosted data in the future, SAS would follow the required legal process for the country and jurisdiction in question, including any applicable privacy safeguards. SAS policy requires any such requests to be forwarded to the SAS Legal Division for immediate review. SAS also would involve experienced outside legal counsel as needed to assist with any such requests.

  SAS would challenge a request to the fullest extent possible. SAS would first seek to determine that the related legal process is valid and appropriate. Importantly, SAS would ensure that the request does not prevent SAS from fulfilling our commitments towards our customers, including our obligations under the EU SCCs when these are in place. SAS would aim to deliver only data that are necessary and proportionate in response to a specific request.

SAS also commits to using all applicable legal processes and tools in place in order to assess or respond to a request. When necessary and permissible, SAS will consult with the competent data protection authorities in each jurisdiction. SAS will also strive to obtain the right to waive any communication prohibition in order to be able to communicate with the competent data protection authority regarding the request.

If SAS did not manage to resolve the request, SAS would use its best efforts to put the access request on hold for a reasonable delay in order to consult with competent EU data protection authorities on how to resolve it, unless such consultation is otherwise prohibited by applicable law. SAS would use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible to the competent data protection authority, and be able to demonstrate that it did so.

In addition to the above, where SAS acts as Data Processor, SAS would notify the Data Controller when local laws prevent SAS (i) from fulfilling its obligations under the Standard Contractual Clauses and such laws have a substantial adverse effect on the guarantees provided by the Standard Contractual Clauses, and (ii) from complying with the instructions received from the Data Controller via the data processing agreement between SAS and the Data Controller. SAS would not notify Data Controllers if such disclosure is prohibited by applicable law.

- Transparency

  SAS commits to publishing an annual transparency report detailing the numbers of accepted and rejected government national security demands for data, if any such requests have been received.

c. *Technical Measures*

- Access Control

  SAS also maintains strict administrative, technical, and physical procedures to protect information stored on its servers. Access to personal information is limited through login credentials to those employees who require it to perform their job functions. In addition, SAS uses access controls such as multi-factor authentication, Single Sign On, access on an as-needed basis, strong password controls, and restricted access to administrative accounts.

- Data Protection and Security Standards

  - Data protection and security are of paramount importance to SAS. These controls are key to protecting customer data from unauthorized access. With respect to SAS's hosted solutions, SAS holds several certifications, including ISO 27001, ISO27017 and ISO27018, with SOC 2, and SOC 3 planned availability by Q1 2022. Please see the following SAS Cloud Whitepaper which outlines in detail SAS's commitment to physical, logical and personnel security.

  - SAS's software solutions are also subject to rigorous security and quality processes. For details on SAS product security, please see the following SAS Product Quality Whitepaper which outlines the security controls present in SAS software development.

For more information regarding these principles and the additional supplemental principles, please see the Full Text of the Principles.

- Encryption

  Encryption is an important technical measure that can prevent surveillance wiretapping by government authorities, including the PRISM and UPSTREAM surveillance programs cited by the CJEU. Customer data is encrypted in transit to prevent this access.

- Pseudonymisation

  SAS policy encourages all customers to pseudonymize data processed by SAS. The pseudonymization key should be held only by the data controller. For products or services where data must be in the clear (for example, CI360 Email), data is encrypted in transit and at rest and data is in the clear for the minimum time period necessary.