

SAS Institute Inc.
March 2022 Update: EU Data Processing for EU Customers

SAS Institute Inc. (together with its subsidiaries and affiliates, “SAS”) is providing an update to the November 2021 announcement of our commitment to invest in technical and operational measures to further limit processing of EU/UK Customer Data from outside the EU. This update will assist customers in data privacy risk assessments in the context of non-EU access to Customer Data.

SAS recognizes the critical importance of privacy regulations, including the General Data Protection Regulation and the UK GDPR (together “GDPR”), which are designed to protect data privacy within a technology solution using a risk-based approach. In the months since our November 2021 announcement, SAS has gathered and analyzed feedback from customers and regulatory resources in the EU to better understand customer needs and priorities.

These discussions confirmed the importance of data governance and access controls and SAS’ associated responsibilities as data processor. Many customer Transfer Impact Assessment (“TIA”) questionnaires under GDPR/Schrems II focus on SAS’ specific data governance practices. Here is a summary of our current practices and our progress towards our EU processing goal:

- 1. Cloud Infrastructure within EU:** SAS’ customers have the option to use cloud environments based on a “within-EU principle.” This means, upon Customer’s request, the cloud environments (physical and logical IT infrastructure) SAS provides for Hosted Managed Services resides within the EU. Our standard setup (depending on the cloud infrastructure provider deployed) is an Availability Zone (“AZ”) in Frankfurt (Germany) or Dublin (Ireland) drawing on infrastructure physically located around these cities.
- 2. No movement or storage of data outside of the EU:** Currently, when SAS operates customer cloud services for EU-only customers (those customers who request “EU-only” resources), SAS does not move or store customer data outside the EU and agreed-to AZ. Backup facilities associated with the AZ also reside within the EU.
- 3. Cloud personnel with least privilege “need to know” data access to be based in EU to the greatest extent possible:** Currently, SAS leverages EU-based resources for service delivery activities to EU-only customers. SAS is investing heavily in this area; we are hiring additional EU resources in order to support EU-only customers with a 24x7 service. In addition, SAS is further limiting the number of individuals with access from outside of EU. In certain situations, some non-EU roles may be needed, such as for emergency support. Other roles may have access to the solution for initial architecture design, software install in advance of data transfer, or other support reasons but will not have access to customer data. In all cases, access will be requested and approved, and actions will be logged and monitored.
- 4. Role Based Access:** In alignment with security best practices, any access, whether in a system that houses customer data or an internal support tool, is limited only to the resources that have a need for access with the minimally-required permissions to complete the job functions. For every individual and role involved in Hosted Managed Services, SAS uses role-based access controls to design, assign, and audit access based on job function and associated responsibilities.
- 5. Privileged access management and monitoring:** SAS is improving its capability related to privileged access management. Combining these capabilities with role-based access control, SAS will have better auditing and control capabilities for interactive administrative users.
- 6. Updated Standard Contractual Clauses (SCCs) for data transfers:** SAS has entered into an intra-company (among SAS and its subsidiaries) Data Processing Agreement (DPA) using the updated (June 2021) SCCs to



help provide assurances of appropriate data protection safeguards. This supports the data transfer compliance between the contracting SAS entity as data exporter and the subcontracted SAS entities as data importer. With respect to new customer agreements, SAS has begun using DPAs based on the updated SCCs. In accordance with the European Commission's schedule, SAS will be entering into updated SCCs for existing customers and processing by 27 December 2022, as required.

SAS continues our commitment to meet the requirements of EU data protection laws and to deliver processing environments to meet customer demands.