SAS Institute Inc.

November 2023 Update: EEA/UK Data Processing

SAS Institute Inc. (together with its subsidiaries and affiliates, "SAS") is providing an update to the 2022 statements on our commitment to invest in technical and organizational measures to further limit processing of European Economic Area/United Kingdom (EEA/UK) customers' personal data ("Customer Data") from outside the EEA/UK. This update will assist customers in data privacy risk assessments in the context of non-EEA/UK access to Customer Data. It focuses on the topics most relevant from a data protection perspective: storage of and access to personal data. These controls, both technical and procedural, provide an end-to end solution to limit SAS personnel who have the ability to access the EEA/UK customer environments.

In addition, as of 12 October 2023, SAS is certified to the EU-US, Swiss-US Data Privacy Framework with UK Extension (the "**DPF**"). On 17 July 2023, the EU granted adequacy status to US companies who certify to the DPF. SAS' DPF certification has been validated by our independent assessor, TRUSTe (TrustArc). Please view our certification status at https://www.dataprivacyframework.gov/s/participant-search.

Here is a summary of our current practice for EEA/UK processing:

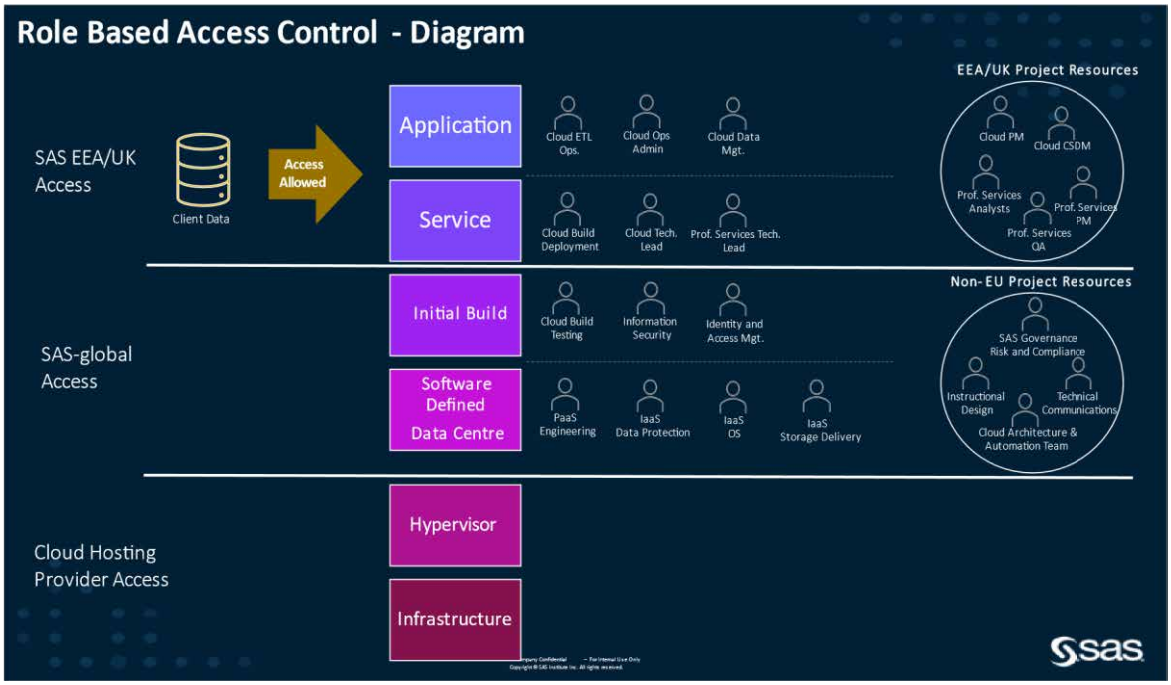
Part 1: STORAGE OF PERSONAL DATA

1. **Cloud Infrastructure within EEA/UK**: SAS' customers have the option to use cloud environments physically located in the EEA/UK. This means that, upon customer request, the cloud environments (physical and logical IT infrastructure) that SAS provides for Hosted Managed Services will reside within the EEA/UK. Our standard setup is an Availability Zone ("**AZ**") in Frankfurt (Germany), London (UK), Oslo (Norway) or Dublin (Ireland), drawing on infrastructure physically located around these cities. Personnel used to build and manage the underlying Cloud Infrastructure do not require access to Customer Data to perform their roles.

2. **No Storage of Data Outside of the EEA/UK**: When SAS operates cloud services for EEA/UK only customers (those customers who request "EEA/UK-only" resources), SAS will not move or store Customer Data outside the EEA/UK and agreed-to AZ. Backup facilities associated with the AZ also reside within the EEA/UK.

Part 2: ACCESS TO PERSONAL DATA

1. **Role-Based Access Controls (RBAC):** In alignment with security best practices, any access to Customer Data is limited to only the personnel that have a need for access. The access itself has only the minimum permissions required to perform the role. For every individual/role involved in Hosted Managed Services, SAS uses these role-based access controls to design, assign, and audit access based on job function and responsibilities. See the diagram below.



The role-based access control diagram (from bottom to top) separates the following roles/access levels:

a. Infrastructure and Hypervisor/Cloud Service Provider: These are the public cloud service providers (for example Microsoft or Amazon) who partner with SAS. These Infrastructure-as-a-Service providers offer essential compute, storage, and networking resources. Their responsibilities include the infrastructure that provides the computing hardware, network availability and the physical and environmental data center security.

b. Software Defined Data Center and Initial Build: These roles are for SAS technology and build engineering personnel. These resources ensure that the infrastructure and tooling are deployed to the standards set by SAS to deliver the platform. All these tasks are carried out *without* access to Customer Data.

c. Application and Service: These are roles providing the operational SAS Cloud services to deliver the application. These roles support the software implementation project to operational service. To deliver their services, access to Customer Data may be needed. Therefore, these personnel are placed within the EEA/UK.

2. **Privileged Access Management and Monitoring**: Effective 1 January 2023, SAS upgraded its privileged access management ("**PAM**") solution. SAS has enhanced auditing and control capabilities for individually assigned privileged accounts used by SAS staff with access to EEA/UK servers and Customer Data.
3. **SAS Personnel with Data Access Based in EU**: Effective 1 January 2023, SAS uses EEA/UK based personnel for service delivery activities with access to Customer Data and provide EEA/UK customers with 24x7 service. Non-EEA/UK roles do not have access to Customer Data. In extraordinary cases, a SAS expert for product development or IT configuration outside of the EEA/UK may need access to the system. This data access will be granted only upon the customer's prior approval and for a very limited period of time to fulfil a specific task. In all cases, access to data is requested and approved within the SAS RBAC structure, and actions **are** logged and monitored.

For example, SAS Cloud resources such as SAS Cloud Operational Administrators located in the EEA/UK access SAS Viya 4 using a privileged service account that is retrieved from a secure password vault. Extract Transform Load (ETL) Operations personnel would have access to the batch automation process but not privileged access.

SAS Cloud Operational Administrators' access to the Kubernetes console is controlled via Azure Active Directory authentication. Permissions for SAS Cloud Operational Administrators are based on business role and location, which are documented in the RBAC model. This access is reviewed regularly.

Hands-on tasks related to the Kubernetes cluster such as managing nodes and resources are performed by people within the EEA/UK. Administration of the Azure data centres, configuration of shared services and other data centre-wide operations may be performed by non-EEA/UK resources because no access to data is possible. (Please see diagram above).

SAS continues its commitment to meet the requirements of EEA/UK data protection laws and to deliver processing environments to meet customer demands. For more information on SAS' commitment to Privacy, please contact your SAS representative or see the SAS Trust Center-Privacy.