Attachment 1: Description of the data processing activities

This attachment describes the general data processing activities regarding services offered by Siemens for the Product (BMS as a Service, hosted by Desigo CC) as well as the affected persons and the categories of the processed personal data.

Product	Service	Explanation
BMS as a Service (hosted by Desigo CC)	User administration	Create/deactivate user-accounts (on behalf of the customer) andd assign user rights. A user name and password combination and an email address are necessary to access the product.
	Data Storage	A unique user name is created by Siemens employees from the operations team. For end-customers, a unique user name is formed from a combination of the user's actual Given and Family names.
Categories of affected persons • Employees of customers and / or employees of third parties operating or otherwise using the Product.		
Category of data • Personal master data (name, user name, office address, validity, user rights, employee number, access rights etc.) • Operating data within the Product • Logged activities (e. g. changes at the configuration of the system)		

Attachment 2: Technical and organizational measures pursuant to Art. 32 General Data Protection Regulation ("GDPR")

1. Physical Access Control

The following measures are implemented to protect against unauthorized physical access to premises, buildings or rooms where data processing systems are located which process and/or use Personal Data:

a) Physical components of the data center facilities, servers, networking equipment, and host software are housed in nondescript facilities.
b) Physical barrier controls are used to prevent unauthorized entrance to these facilities both at the perimeter (e.g., fencing, walls) and at building access points.
c) Physical access points to server locations are managed by electronic access control devices and are secured with intrusion detection devices that sound alarms if the door is forced open or held open.
d) Establishing access authorizations for employees and third parties, including the respective documentation.
e) All visitors are required to present identification and are signed in.
f) Use of video cameras (CCTV) to monitor individual physical access to data center facilities.
g) Data centers utilize security guards 24x7, who are stationed in and around the building.

2. System Access Control

The following measures are implemented to protect against the unauthorized access to and use of data processing systems used to provide the digital services:

a) User and administrator access to the data center facilities, servers, networking equipment, and host software is based on a role based access rights model. A unique ID is assigned to ensure proper user-authentication management for users and administrators on all system components.
b) The concept of least privilege is employed, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.
c) IT access privileges are reviewed on regular basis by appropriate personnel.
d) Access to systems is revoked within a reasonable timeframe of the employee record being terminated (deactivated).
e) First time passwords/passphrases are set to a unique value and changed immediately after first use.
f) User passwords/passphrases are changed periodically and only allow complex passwords.
g) Time stamped logging of security relevant actions is in place.
h) Automatic time-out of user terminal if left idle, with user identification and password required to reopen.
i) Assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection.
j) Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.
k) Firewall policies (configuration files) are pushed to firewall devices on regular basis.

3. Data Access Control

The following measures are implemented to control that persons entitled to use data processing systems gain access only to the Personal Data when they have a right to access, and Personal Data is not read, copied, modified or removed without authorization in the course of processing, use and storage.

a) User and administrator access to the data center facilities, servers, networking equipment, and host software is based on a role based access rights model. A unique ID is assigned to ensure proper user-authentication management for users and administrators on all system components.
b) The concept of least privilege is employed, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.
c) **IT** access privileges are reviewed on regular basis by appropriate personnel.
d) Time stamped logging of access to and modification of Personal Data is in place.
e) An incident response plan is in place to address the following at time of incident:
   - Roles, responsibilities, and communication and contact strategies in the event of a compromise.
   - Specific incident response procedures.
   - Coverage and responses of all critical system components

4. Data Transmission Control

The following measures are implemented to control that Personal Data is not read, copied, modified or removed without authorization during transfer:

a) Prevention of unauthorized copying: The measures taken to prevent unauthorized copying of the physical storage infrastructure as such (e.g. copying your data by transferring them to an external storage medium as a hard drive) are included in the measures described above.
b) Use of role based access rights model: described above.
c) Firewall policies: described above
d) Implement an incident response plan: described above.
e) Storage Device Decommissioning: When a storage device has reached the end of its useful life, procedures implemented include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices and applicable data protection law.
f) Secure Access Points: there are only a limited number of secure access points to the cloud), which allow you to establish a secure communication session with your storage or compute instances within the Services.
g) Connections to the network by personnel: personnel connect to the network using secure authentication that restricts access to network devices and other cloud components.

5. Data Input Control

The following measures are implemented to retrospectively examine and establish whether and by whom **Personal Data** have been entered, modified or removed from data processing systems used to provide the digital services:

Logging User Activity: developers and administrators who need to access to our systems in order to maintain them must explicitly request access. Approved personnel connect to the network using secure authentication that restricts access to network devices and other cloud components, logging all relevant activity for security review.

6. Order Control

The following measures are implemented in order to ensure that Personal Data which are processed on your behalf can only be processed in compliance with your instructions:

a) Internal communication: various methods of internal communication are implemented at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employees and regular management meetings for updates on business performance and other matters.
b) Corporate Segregation: Logically, the production network is segregated from the corporate network by means of a complex set of network security / segregation devices. Developers and administrators on the corporate network who need to access in order to maintain them must explicitly request access. Approved personnel then connect to the network through secure means.
c) Robust Compliance Program: The IT infrastructure is designed and managed in alignment with security best practices and certain IT security standards.
d) Policies and Security Awareness Training: We and our Subprocessors maintain and provide periodic security awareness training to all information system users. Policies and procedures have been established based upon data security and data protection requirements.

7. Availability Control

The following measures are implemented to protect Personal Data against accidental or unauthorized destruction or loss.

a) Fire Detection and Suppression: Automatic fire detection and suppression equipment has been installed with our data centers. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms.
b) Redundant Power Systems: The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.
c) Climate and Temperature Control: Personnel and systems monitor and control temperature and humidity at appropriate levels at data centers.
d) Preventative maintenance: Preventative maintenance is performed to maintain the continued operability of the data center equipment.

8. Data Separation Control

The following measures are implemented to control that Personal Data collected for different purposes can be processed separately:

a) Multi-tenant environment: The Platform is a virtualized, multi-tenant environment. Security management processes and security controls designed to isolate each customer from other customers are implemented. Systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.
b) Corporate Segregation: described above.

Attachment 3: List of approved Sub-Processors

This attachment lists the Sub-Processors engaged by Siemens when providing Services to the customer

Sub-Processor name	Sub-Processor Country	Service provided by Sub-Processor	Transfer Safeguards implemented by Sub-Processor	
Amazon Web Services Inc. (incl. other entities see: https://aws.amazon.com/de/compliance/sub-processors)	USA **Remark:** The data are processed exclusively within the EEA (currently Ireland/Dublin).	Hosting of data	☒ ☐ ☐	Not applicable, processing takes place within the EEA / a country with an adequacy decision EU Model Contract BCR-P
Siemens Affiliated Companies on a case by case basis	Switzerland Bulgaria (Please adjust your country if needed)	2nd level cloud infrastructure 3rd level application support	☒ ☐ ☐	Not applicable, processing takes place within the EEA / a country with an adequacy decision EU Model Contract BCR-P