Attachment 1: Description of the data processing activities

This attachment describes the general data processing activities regarding services offered by Siemens for the Product as well as the affected persons and the categories of the processed personal data.

Product	Service	Explanation
Siveillance Command	3rd level software support, also remotely via cRSP	During data transmission and with 3rd level support there are files visible in the customer`s system which may contain personal data (e. g. personal names of employees, log files of user actions).
Affected persons • Employees of customers and / or employees of third parties operating or otherwise using the Product. • Persons reporting a concern as recorded by or through the Product		
Category of data • Personal master data (name, user name, office adress, validity, user rights etc.) • Operating data within the Product • Business contacts (Mail-adress, Phone number) • Logged activities (e. g. changes at the configuration of the system) • Reported concern as recorded by or through the Product		

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

I. Introduction

This document describes the technical and organizational measures for the protection of personal data (the "Measures") which the contractor takes as a minimum in connection with the processing carried out by the contractor, taking into account the state of the art in technology, the costs for implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

If different, special measures are agreed in the underlying contract, those special measures apply instead of or in addition to the measures described in this document.

II. Basic Measures

The basic Measures assure the protection of confidentiality and the integrity of the systems with which Siemens processes personal data, especially by way of remote access. These Measures apply for all processing carried out by Siemens unless agreed otherwise in the underlying contract.

1. Internal organization of operations
The contractor has appointed a company data protection manager. All employees and service providers of the contractor having access to personal data are under obligations to process these data only upon instruction and exclusively for the performing of the contractually agreed services.

2. Protection against unauthorized access
Unauthorized persons must be prevented from entering the computer centers or business premises in which data processing takes place.

Measures:
The contractor will protect the buildings or business premises with reasonable control systems for physical access based on a security classification for the buildings or business premises and correspondingly defined entry authorization concepts. All buildings or business premises must be secured with technical entry control measures e.g. using a card reading system. Depending on the security classification, real property, buildings or individual areas must be secured with additional Measures. This can include special profiles for physical entry, biometrics, pin-pads, turnstile systems to allow only individual entry, video surveillance and security personnel.
Rights to enter for authorized persons are issued individually in accordance with established criteria. This also applies with regard to external persons.

3. Protection for computers
The computers used for the processing must be secured and protected against unauthorized use.

Measures:
Only authenticated users receive access to computers (e.g. notebooks, workstations) using, for example, the following Measures: data encryption, individualized issuance of passwords (at least 8 characters, normally with automatic expiration), employee identity cards with personal identity encryption, automatic lock-down of inactive systems. The protection of the used computers against attacks as well as accidental or intentional destruction or modification is provided, among other Measures, by intrusion detection systems, firewalls and regularly updated malware filters.

4. Protection of data upon transmission, transport and remote access
Care must be taken that personal data cannot be read, copied, changed or removed during electronic transmission or during the transport of the data or storing it on data media and that it is possible to examine and determine at which places a transmission of personal data using equipment for data transmission is provided for.

Measures:
The electronic communication channels must be secured with installation of closed networks and processes for data encryption. In the case of physical transport of data media, data will be protected by encryption. Data media must be disposed of in a manner appropriate for protection of data. Remote maintenance connections must be protected by means of encryption. The date, type and scope of the remote maintenance must be recorded in protocols.

III. Specific Measures for services in which Siemens stores customer data in IT systems

These specific Measures assure the protection of the confidentiality, integrity, availability and resilience of the IT systems in which Siemens stores customer data. These Measures apply when the storage of data represents a material aspect of the contractual services by Siemens and is not just temporary.

1. Protection against unauthorized processing
There must be assurance that the persons authorized to use an IT system exclusively can access the data subject to their access authorization and that personal data cannot be read, copied, changed or removed without authorization during the processing, use and after storage.

Measures:
Access to personal data in IT systems is granted on the basis of an authorization concept based on the function being performed ("need to know"). Furthermore, unauthorized access to personal data is prevented as needed by means of data encryption.

2. Assurance of traceability
There must be assurance that it is possible to subsequently examine and determine whether and by whom personal data have been entered, changed or removed in data processing systems.

Measures:
The contractor only permits authorized users to have access to personal data on the basis of a "need to know" authorization concept. Access to personal data is entered in log data files which record in detail in a protocol the production, modification and removal of personal data.

3. Assurance of integrity, availability and stability
There must be assurance that the systems used for the processing are secured against failure and that personal data are fully available and protected against loss at all times.

Measures:
For the situation, that the contractor stores personal data by using redundant systems, depending on the security classification. The contractor also uses interruption-free electric power (e.g. UPS, batteries, generators) to secure the supply of electric power in the contractor's computer centers. A comprehensive, written emergency plan must be prepared. Emergency procedures and systems are regularly tested.

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	
Autec GmbH	Germany	3rd level software support	☒	Not applicable, Sub-Processor located within the EEA / a Country With An Adequacy Decision
			☐	EU Model Contract
			☐	Privacy Shield
			☐	BCR-P
Siemens affiliates	(Please adjust your country)	3rd level software support	☒	Not applicable, Sub-Processor located within the EEA / a Country With An Adequacy Decision
			☐	EU Model Contract
			☐	Privacy Shield
			☐	BCR-P
Atos IT Solution & Service GmbH	Germany	**Only in case of cRSP remote support**: Service: Platform operation, maintenance.	☒	Not applicable, Sub-Processor located within the EEA / a Country With An Adequacy Decision
			☐	EU Model Contract
			☐	Privacy Shield
			☐	BCR-P
Other Siemens affiliates on a case by case basis	Germany (please adjust your country if necessary)	**Only in case of cRSP remote support**:3rd level support	☒	Not applicable, Sub-Processor located within the EEA / a Country With An Adequacy Decision
			☒	EU Model Contract
			☐	Privacy Shield
			☐	BCR-P