SIEMENS

# Data Privacy Terms

April 2021

The Data Privacy Terms ("**DPT**") are agreed between the Siemens entity ("**Siemens**") and the customer ("**Customer**") named in the Agreement.

## 1. Scope and compliance with laws

1.1. The DPT and the DPT Exhibits shall apply to Offerings provided under the Agreement that involve the Processing of Personal Data by Siemens acting as Processor for Customer. In the Agreement, Offering as defined herein may be referred to as "Service". The DPT are incorporated into the Agreement; in the event of conflicts, the DPT Exhibits prevail over the DPT which prevail over the remainder of the Agreement.

1.2. The DPT describe Customer's and Siemens' data protection related rights and obligations with regard to the Offerings captured by the DPT. All other rights and obligations shall be exclusively governed by the other parts of the Agreement.

1.3. When providing the Offerings, Siemens will comply with data protection laws and regulations directly applicable to its provision of the Offerings acting as Customer's Processor, including security breach notification law. However, Siemens shall not be responsible for compliance with any data protection laws or regulations applicable to Customer or Customer's industry that are not generally applicable to Processors. Customer shall comply with all laws and regulations applicable to Customers use of the Offerings, including Applicable Data Protection Law, and ensure that Siemens and its Subprocessor are allowed to provide the Offerings as described in the DPT.

## 2. Details of the processing

The details of the Processing operations provided by Siemens, including the subject-matter of the Processing, the nature and purpose of the Processing, the types of Personal Data Processed and the categories of affected Data Subjects, are specified in the DPT Exhibits.

## 3. Instructions

Siemens will Process Personal Data only in accordance with Customer's documented instructions. Customer agrees that the Agreement (including the DPT) are Customer's documented instructions to Siemens for the Processing of Personal Data. Any additional or alternative instructions must be agreed between the parties in writing.

## 4. Technical and organizational measures

4.1. Taking into account the state of the art, the costs of 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, Siemens shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The technical and organizational measures implemented by Siemens for this purpose are described in the DPT Exhibits. Customer understands and agrees that the technical and organizational measures are subject to technical progress and development. In that regard, Siemens shall have the right to implement appropriate alternative measures as long as the security level of the measures is maintained.

4.2. Customer is responsible for implementing and maintaining appropriate technical and organizational measures for components that Customer provides or controls, such as implementing physical and system access control measures for Customer's own premises, assets and IT-systems or configuring the Offerings to Customer's individual requirements.

## 5. Confidentiality of the processing

Siemens will ensure that personnel who are engaged in the Processing of Personal Data (i) are under an obligation to maintain the confidentiality of such data, (ii) will process such data only as described in this DPA or on Customer's documented instructions and (iii) receive adequate privacy and security trainings.

## 6. Subprocessors

6.1. Customer hereby approves the engagement of Subprocessors by Siemens. A current list of Subprocessors commissioned by Siemens is available in the applicable DPT Exhibits.

6.2. Siemens may remove or add new Subprocessors at any time. If required by Applicable Data Protection Law, Siemens will obtain Customer's approval to engage new Subprocessors in accordance with the following process: (i) Siemens shall notify Customer with at least 30 days' prior notice before authorizing any new Subprocessor to access Customer's Personal Data; (ii) if Customer raises no reasonable objections that include an explanation of the grounds for non-approval in writing within this 30 day period, then this shall be taken as an approval of the new Subprocessor; (iii) if Customer raises reasonable objections, Siemens will - before authorizing the Subprocessor to access Personal Data - use reasonable efforts to (a) recommend a change to Customer's configuration or use of the Offerings to avoid Processing of Personal Data by the objected-to new Subprocessor or (b) propose other measures that address the concerns raised in Customer's objection; (iv) if the proposed changes or measures cannot eliminate the grounds for non-approval, Customer may terminate the affected Offering without penalty with 14 days' written notice following Siemens response to Customer's objection. If Customer does not terminate the affected Offering within the 14-day period, this shall be taken as an approval of the Subprocessor by Customer.

6.3 In case of any commissioning of Subprocessors, Siemens shall enter into an agreement with such Subprocessor imposing appropriate contractual obligations on the Subprocessor that are no less protective than the obligations in this DPT. Siemens remains responsible for any acts or omissions of our Subprocessors in the same manner as for Siemens' own acts and omissions hereunder.

7. **Transfers to Non-EEA Recipients**

7.1. In case Transfers to Non-EEA Recipients relate to Personal Data originating from a Controller located within the EEA, Switzerland, or the United Kingdom, Siemens shall implement the Transfer Safeguards identified in the DPT Exhibits. Siemens shall have the right to replace the Transfer Safeguard identified in the DPT Exhibits by alternative adequate Transfer Safeguards. In this case the notification and objection mechanism in Section 6.2 shall apply mutatis mutandis.

7.2. The following shall apply if a Transfer Safeguard is based on the Standard Contractual Clauses:

(i) Siemens, if located outside the EEA or outside a Country with an Adequacy Decision, and Customer hereby enter into the Standard Contractual Clauses. Customer enters into the Standard Contractual Clauses acting in its own name and for its own account and on behalf and in the name of its Further Controllers. The "DPT Exhibits - Description of the Processing Operations" and "DPT Exhibits - Technical and organizational measures" shall form Appendix 1 and 2 of the Standard Contractual Clauses.

(ii) Siemens enters into the Standard Contractual Clauses with its Subprocessors located outside the EEA or outside a Country with an Adequacy Decision. The Standard Contractual Clauses shall cover the Processing activities provided by the respective Subprocessor. Customer and Further Controllers shall become a data exporter under the Standard Contractual Clauses as follows: (a) the Standard Contractual Clauses shall contain the right for Customer and Further Controllers to join the Standard Contractual Clauses by unilateral declaration, i.e. the Standard Contractual Clauses shall be binding upon Customer, Further Controllers and the respective Subprocessor as soon as Customer declared its accession (and regardless of the declaration being received by Siemens or the Subprocessor) ("**Accession Mechanism**"); or (b) Siemens enters into the Standard Contractual Clauses with the Subprocessor on behalf of the Customer and Further Controllers ("**Mandate Mechanism**"). The Mandate Mechanism shall apply if Siemens confirmed in the DPT Exhibits that a Subprocessor is eligible for it.

7.3. The following shall apply if a Transfer Safeguard is based on BCR-P: Siemens shall contractually bind such Subprocessor to comply with the BCR-P with regard to the Personal Data Processed under this DPT.

7.4. Siemens' additional commitment: In addition to the commitments made in the Transfer Safeguards, Siemens confirms that it has no reason to believe that the legislation applicable to it or its Subprocessors, including in any country to which Personal Data is transferred either by itself or through a Subprocessor, prevents it from fulfilling the instructions received from the Customer and its obligations under the DPT or the Transfer Safeguards and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the commitments and obligations provided by these DPT or the Transfer Safeguards, it will promptly notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of Personal Data and/or terminate the Agreement.

8. **Defending Customer Personal Data – Third party access requests**

In the event Siemens receives an order from any third party for disclosure of Personal Data, Siemens shall (i) use every reasonable effort to redirect the third party to request data directly from Customer; (ii) promptly notify Customer, unless prohibited under applicable law, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and, (iii) use all reasonable lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the EEA or applicable EEA member state law

9. **Personal Data Breach**

9.1. Siemens shall notify the Customer without undue delay after becoming aware of a Personal Data Breach. Taking into account the nature of processing and the information available to Siemens, the notification shall describe (i) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, (ii) a contact point where more information can be obtained, (iii) the likely consequences of the Personal Data Breach; and (iv) the measures taken or proposed to be taken to address the Personal Data Breach. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

9.2. Siemens shall (i) reasonably assist the Customer in ensuring compliance with its Personal Data Breach obligations pursuant to Applicable Data Protection Law, and (ii) initiate respective and reasonable remedy measures.

10. **Data subject rights, Siemens' assistance**

10.1. Siemens shall, to the extent legally permitted, notify Customer without undue delay if Siemens receives a request from a Data Subject to exercise its Data Subject's rights (such as the right to access, rectification, erasure or restriction of Processing).

10.2. Taking into account the nature of the processing and the information available to Siemens, (i) Siemens shall assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights; (ii) at its own discretion, either (a) provide Customer with the ability to rectify or erase Personal Data via the functionalities of the Offerings, or (ii) rectify or erase Personal Data as instructed by Customer; and (iii) reasonably assist Customer to comply with its further obligations under Applicable Data Protection Law. Any such further assistance under no. (iii) shall be mutually agreed between the parties.

11. **Audits**

11.1. Provided that an audit right is required by Applicable Data Protection Law, Customer shall have the right to audit, by appropriate means - in accordance with Sections 11.2 to 11.4 below - Siemens' and its Subprocessors' compliance with the data protection obligations hereunder annually, unless additional audits are necessary under Applicable Data Protection Law. Such audits shall be

limited to information and data processing systems that are relevant for the provision of the Offerings provided to Customer.

11.2. Siemens and its Subprocessors may use (internal or external) auditors to perform audits to verify compliance with the data protection obligations hereunder. Each audit will result in the generation of an audit report ("**Audit Report**"). Upon Customer´s request, Siemens shall provide such relevant Audit Reports for the Offerings concerned. Customer agrees that these Audit Reports shall first be used to address Customer's audit rights under these DPT.

11.3. If required under Applicable Data Protection Law, Siemens will allow for additional audits, including onsite audits at Siemens facilities and premises by Customer or an independent, accredited third party audit firm, during regular business hours, with reasonable advance notice to Siemens. Customer is responsible for all costs and fees related to such further audit.

11.4. The Audit Reports and any further information and documentation provided during an audit shall constitute confidential information and may only be provided to Further Controllers pursuant to confidentiality obligations substantially equivalent to the confidentiality obligations contained elsewhere in the Agreement. In case audits relate to Subprocessors, Siemens may require Customer and Further Controllers to enter into non-disclosure agreements directly with the respective Subprocessor before issuing Audit Reports and any further information or documentation to Customer or Further Controllers.

## 12. Single point of contact and liability

12.1. Customer shall serve as a single point of contact for Siemens, also with regard to Further Controllers under the DPT.

12.2. In case the DPT or any of the Transfer Safeguards in Section 7 (such as Standard Contractual Clauses) provide rights to Controllers (including Controllers other than Customer) in relation to Siemens and/or its Subprocessors, Customer shall, unless required otherwise by Appliable Data Protection Law exercise, these rights by contacting Siemens directly, in its own name and/or on behalf of the respective Controller. Siemens and its Subprocessors shall be entitled to refuse any requests, instructions or claims provided directly by a Controller other than Customer.

12.3. In case the DPT or any of the Transfer Safeguards contain notification obligations vis-a-vis Controllers, Siemens shall be discharged of its obligation to notify a Controller when Siemens has provided such notice to Customer, unless required otherwise by Appliable Data Protection Law.

12.4. Without prejudice to the statutory rights of Data Subjects, limitations of liability contained in the Agreement shall also apply to Siemens' and its Subprocessors' liability (taken together in the aggregate) vis-à-vis Customer and its Further Controllers.

12.5. Customer shall be responsible to ensure that Sections 12.1 to 12.4 above are enforceable by Siemens and its Subprocessors vis-à-vis its Further Controllers.

## 13. Notices

13.1. Siemens may provide notice to Customer under the DPT by posting a notice as described in the Agreement.

13.2. Notices concerning Subprocessors under section 6 of the DPT may be given by listing the current Subprocessors at www.siemens.com/dpt and providing Customer with a mechanism to obtain notice of any new Subprocessor. It is Customer's obligation to register a point of contact to receive Subprocessor notifications at www.siemens.com/dpt and to keep contact information for notices current.

## 14. Term and termination

The DPT shall have the same term as the Agreement. Upon termination of the DPT and unless otherwise agreed between the parties in the Agreement, Siemens shall erase all Personal Data made available to it or obtained or generated by it on behalf of Customer connection with the Offerings.

## 15. Language

If Siemens provides a translation of the English language version of the DPT or its Exhibits, the English language version of the DPT or its Exhibits will control in the event of any conflict

## 16. Country Terms

16.1. **Russian Federation.** If Siemens is Processing Personal Data within the scope of the Data Protection Act No. 152 FZ (i) Customer shall be responsible for the initial collection, recording, systematization, storing, updating, amending, transferring and extraction (collectively "**Initial Processing**") of such Personal Data; and (ii) Customer hereby represents that it will conduct the Initial Processing in compliance with the laws governing processing and protection of such information. Customer represents that it has obtained the Data Subject's consent on the transfer (including international transfer) and Processing of their Personal Data by Siemens and its Subprocessors.

16.2. **USA.** If Siemens is Processing Personal Data of US residents, Siemens makes the following additional commitments to Customer: Siemens will Process Personal Data on behalf of Customer and, not retain, use, or disclose that Personal Data for any purpose other than for the purposes set out in the DPT and as permitted under relevant US data privacy law („**US Data Privacy Law**"), including under any "sale" exemption. In no event will Customer sell (as such term are is defined under US Data Privacy Law) any such Personal Data. These additional terms do not limit or reduce any data protection commitments Siemens makes to Customer in the DPT, Agreement, or other agreement between Siemens and Customer. Siemens hereby certifies that Siemens understands the restrictions contained herein and will comply with them.

17. **Definitions**

17.1. "**Agreement**" means the commercial agreement on the provision of the Offerings between Siemens and Customer.

17.2. "**Applicable Data Protection Law**" means all applicable law pertaining to the Processing of Personal Data hereunder.

17.3. "**Binding Corporate Rules for Processors**" or "**BCR-P**" shall mean Binding Corporate Rules for Processors approved in accordance with Article 47 of the General Data Protection Regulation (EU) 2016/679.

17.4. "**Controller**" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

17.5. "**Country with an Adequacy Decision**" shall mean a country outside the EEA where the European Commission has decided that the country ensures an adequate level of protection with respect to Personal Data.

17.6. "**Data Subject**" means an identified or identifiable natural person.

17.7. "**DPT**" shall mean these Data Privacy Terms.

17.8. "**DPT Exhibits**" shall mean the documents which describe the scope, the nature and purpose of the Processing, the types of Personal Data Processed, the categories of affected Data Subjects, the Subprocessors used and technical and organizational measures and which are referenced in the Agreement and/or this DPA.

17.9. "**EEA**" shall mean the European Economic Area.

17.10. "**Further Controller**" shall mean any third party (such as an affiliated company of Customer) acting as Controller which is entitled to use or receive Offerings under the terms of the Agreement.

17.11. "**Offerings**" shall mean the Offerings under the Agreement provided by Siemens acting in its role as Processor. In the Agreement, Offering as defined herein may be referred to as "Service".

17.12. "**Personal Data**" means information that relates, directly or indirectly, to a Data Subject, including without limitation, names, email addresses, postal addresses, identification numbers, location data, online identifiers or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Personal Data, for the purposes of the DPT, includes only such Personal Data entered by Customer or any Further Controller into or derived from the use of the Offerings or that is accessed by Siemens in the context of providing the Offerings.

17.13. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed under the terms of this DPT.

17.14. "**Processor**" means a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of a Controller.

17.15. "**Process**" or **Processing**" means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, access to, transfer, and disposal.

17.16. "**Standard Contractual Clauses**" means the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries pursuant to Commission Decision 2010/87/EU of 5 February 2010 or any successor document issued by the European Commission. The Standard Contractual Clauses current as of the effective date of the Agreement are attached as Annex to the DPT.

17.17. "**Subprocessor**" shall mean any further Processor engaged by Siemens that has access to Personal Data.

17.18. "**Special Categories of Personal Data**" shall mean information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, social security measures, administrative or criminal proceedings and sanctions, or genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

17.19. "**Transfer Safeguards**" shall mean (i) an adequacy decision in the meaning of Article 45 of the General Data Protection Regulation (EU) 2016/679 or (ii) appropriate safeguards as required by Article 46 of the General Data Protection Regulation (EU) 2016/679.

17.20. **"Transfers to Non-EEA Recipients"** shall mean (i) the Processing of Personal Data outside the EEA or a Country with an Adequacy Decision or (ii) any accesses to Personal Data from outside the EEA or a Country with an Adequacy Decision by Siemens or any of its Subprocessors.

**DPT Exhibits - Description of the Processing Operations**

**This Exhibit specifies the subject-matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects. The parties may provide further details in the Agreement if required for a particular Offering.**

**Subject matter, nature and purpose of the processing**

Siemens and its Subprocessors will Process Personal Data to provide the Offerings, including:

- internet accessible or similar Offerings made available and hosted by Siemens ("**Cloud Offerings**"); or
- administration, management, installation, configuration, migration, maintenance and support Offerings or any other Offerings requiring (remote) access to Personal Data stored in the Cloud Offerings or on Customer's IT systems ("**Support and Professional Offerings**").

**Data Subjects**

The Personal Data Processed concerns the following categories of Data Subjects:

Data Subjects include:

- employees,
- contractors,
- suppliers,
- business partners; and
- other individuals whose Personal Data is stored on the Offerings and/or is Processed in the context of providing the Offerings.

**Categories of data**

The Personal Data Processed concerns the following categories of personal data:

- contact and user information, including name, phone number, email address, time zone, and address data;
- system access, usage, authorization data, operating data and any system log-files containing Personal Data or any other application-specific data which users enter into the Offerings; and
- where applicable further Personal Data as determined by Customer and its Further Controllers by uploading or connecting it to the Offerings or otherwise granting access to it via the Offerings.

**Special Categories of Personal Data (if appropriate)**

The Offerings are not intended for the processing of Special Categories of Personal Data and Customer and its Further Controllers shall not transfer, directly or indirectly, any such sensitive personal data to us.

**DPT Exhibits - List of approved Subprocessors**

A reference to the Suprocessors used by us when providing the Offering is available at www.siemens.com/DPT or contained in the respective Agreement.

**DPT Exhibits - Technical and organizational measures**

This document describes the technical and organizational measures (TOMs) implemented by Siemens and its Subprocessors. Some Offerings may be protected by different or additional TOMs, as set forth in the respective Agreement.

Scenario 1: TOMs applicable to Cloud Offerings.

Scenario 2: TOMs applicable to Support and Professional Offerings provided via remote access tools provided and controlled by Siemens.

Scenario 3: TOMs applicable to Support and Professional Offerings provided via remote access tools provided and controlled by Customer.

| # | Measures | Scenario | | |
|---|---|---|---|---|
| | | 1 | 2 | 3 |
| 1. | Physical and Environmental Security | | | |
| | Siemens implements suitable measures to prevent unauthorized persons from gaining access to the data processing equipment (namely database and application servers and related hardware). This shall be accomplished by: | | | |
| | a) establishing security areas; | X | X | - |
| | b) protecting and restricting access paths; | X | X | - |
| | c) securing the decentralized data processing equipment and personal computers; | X | X | X |
| | d) establishing access authorizations for employees and third parties, including the respective documentation; | X | X | - |
| | e) all access to the data center where Personal Data is hosted will be logged, monitored, and tracked; | X | - | - |
| | f) the data center where Personal Data is hosted is secured by restricted access controls, and other appropriate security measures; and | X | - | - |
| | g) maintenance and inspection of supporting equipment in IT areas and data centers shall only be carried out by authorized personnel | X | X | - |
| 2. | Access Control (IT-Systems and/or IT-Application) | | | |
| | 2.1 Siemens implements an authorization and authentication framework including, but not limited to, the following elements: | | | |
| | a) role-based access controls implemented; | X | X | X |
| | b) process to create, modify, and delete accounts implemented; | X | X | X |
| | c) access to IT systems and applications is protected by authentication mechanisms; | X | X | X |
| | d) appropriate authentication methods are used based on the characteristics and technical options of the IT system or application; | X | X | X |
| | e) access to IT systems and applications shall require adequate authentication; | X | X | X |
| | f) all access to data (including personal data) is logged; | X | X | - |

| # | Measures | Scenario | | |
|---|---|---|---|---|
| | | 1 | 2 | 3 |
| | g) authorization and logging measures for inbound and outbound network connections to IT systems and applications (including firewalls to allow or deny inbound network connections) implemented; | X | X | - |
| | h) privileged access rights to IT systems, applications, and network Offerings are only granted to individuals who need it to accomplish their tasks (least-privilege principle); | X | X | X |
| | i) privileged access rights to IT systems and applications are documented and kept up to date; | X | X | X |
| | j) access rights to IT systems and applications are reviewed and updated on regular basis; | X | X | X |
| | k) password policy implemented, including requirements re. password complexity, minimum length and expiry after adequate period of time, no re-use of recently used passwords; | X | X | X |
| | l) IT systems and applications technically enforce password policy; | X | X | X |
| | m) policy to lock user terminal when leaving the workplace; | X | X | X |
| | n) automatic time-out of user terminal if left idle; | X | X | X |
| | o) automatic turn-off of the user identification when several erroneous passwords are entered, along with log file of events (monitoring of break-in-attempts); | X | X | X |
| | p) access rights of employees and external personnel to IT systems and applications is removed immediately upon termination of employment or contract; and | X | X | X |
| | q) use of secure state-of-the-art authentication certificates. | X | X | - |
| | 2.2 Siemens implements a roles and responsibilities concept. | X | X | - |
| | 2.3 IT systems and applications lock down automatically or terminate the session after exceeding a reasonable defined idle time limit. | X | X | - |
| | 2.4 Siemens maintains log-on procedures on IT systems with safeguards against suspicious login activity (e.g. against brute-force and password guessing attacks). | X | X | X |
| 3. | Availability Control | | | |
| | 3.1 Siemens defines, documents and implements a backup concept for IT systems, including the following technical and organizational elements: | | | |
| | a) backups storage media is protected against unauthorized access and environmental threats (e.g., heat, humidity, fire); | X | - | - |
| | b) defined backup intervals; and | X | - | - |
| | c) the restoration of data from backups is tested regularly based on the criticality of the IT system or application. | X | - | - |
| | 3.2 Siemens stores backups in a physical location different from the location where the productive system is hosted. | X | - | - |
| | 3.3 Siemens protects systems and applications against malicious software by implementing appropriate and state-of-the-art anti-malware solutions. | X | X | X |
| | 3.4 IT systems and applications in non-production environments are logically or physically separated from IT systems and applications in production environments. | X | - | - |
| | 3.5 Data centers in which Personal Data is stored or processed are protected against natural disasters, physical attacks or accidents. | X | - | - |

| # | Measures | Scenario | | |
|---|---|---|---|---|
| | | 1 | 2 | 3 |
| | 3.6 Supporting equipment in IT areas and data centers, such as cables, electricity, telecommunication facilities, water supply, or air conditioning systems are protected from disruptions and unauthorized manipulation. | X | - | - |
| 4. | Operations Security | | | |
| | 4.1 Siemens maintains and implements a company-wide ISO 27001 Information Security Framework which is regularly reviewed and updated. | X | X | X |
| | 4.2 Siemens logs security-relevant events, such as user management activities (e.g., creation, deletion), failed logons, changes on the security configuration of the system on IT systems and applications. | X | X | X |
| | 4.3 Siemens continuously analyzes the respective IT systems and applications log data for anomalies, irregularities, indicators of compromise and other suspicious activities. | X | X | X |
| | 4.4 Siemens scans and tests IT systems and applications for security vulnerabilities on a regular basis. | X | X | X |
| | 4.5 Siemens implements and maintains a change management process for IT systems and applications. | X | X | X |
| | 4.6 Siemens maintains a process to update and implement vendor security fixes and updates on the respective IT systems and applications. | X | X | X |
| | 4.7 Siemens irretrievably erases data or physically destroys the data storage media before disposing or reusing of an IT system. | X | X | X |
| 5. | Transmission Controls | | | |
| | 5.1 Siemens continuously and systematically monitors IT systems, applications and relevant network zones to detect malicious and abnormal network activity by; | | | |
| | a) Firewalls (e.g., stateful firewalls, application firewalls); | X | X | - |
| | b) Proxy servers; | X | X | - |
| | c) Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS); | X | X | - |
| | d) URL Filtering; and | X | - | - |
| | e) Security Information and Event Management (SIEM) systems. | X | X | - |
| | 5.2 Siemens documents and updates network topologies and its security requirements on regular basis. | X | X | - |
| | 5.3 Siemens administers IT systems and applications by using state-of-the-art encrypted connections. | X | X | - |
| | 5.4 Siemens protects the integrity of content during transmission by state-of-the-art network protocols, such as TLS. | X | X | - |
| | 5.5 Siemens encrypts, or enables its customers to encrypt, customer data that is transmitted over public networks. | X | X | - |
| | 5.6 Siemens uses secure Key Management Systems (KMS) to store secret keys in the cloud. | X | - | - |
| 6. | Security Incidents | | | |
| | Siemens maintains and implements an incident handling process, including but not limited to | | | |

| # | Measures | Scenario | | |
|---|---|---|---|---|
| | | 1 | 2 | 3 |
| | a) records of security breaches; | X | X | X |
| | b) customer notification processes; and | X | X | X |
| | c) an incident response scheme to address the following at time of incident:(i) roles, responsibilities, and communication and contact strategies in the event of a compromise (ii) specific incident response procedures and (iii) coverage and responses of all critical system components. | X | X | X |
| 7. | Asset Management, System Acquisition, Development and Maintenance | | | |
| | 7.1 Siemens implements an adequate security patching process that includes: | | | |
| | a) monitoring of components for potential weaknesses (CVEs); | X | X | - |
| | b) priority rating of fix; | X | X | - |
| | c) timely implementation of the fix; and | X | X | - |
| | d) download of patches from trustworthy sources. | X | X | - |
| | 7.2 Siemens identifies and documents information security requirements prior to the development and acquisition of new IT systems and applications as well as before making improvements to existing IT systems and applications. | X | X | - |
| | 7.3 Siemens establishes a formal process to control and perform changes to developed applications. | X | X | - |
| | 7.4 Siemens plans and incorporates security tests into the System Development Life Cycle of IT systems and applications. | X | X | - |
| 8. | Human Resource Security | | | |
| | 8.1 Siemens implements the following measures in the area of human resources security: | | | |
| | a) employees with access to Personal Data are bound by confidentiality obligations; and. | X | X | X |
| | b) employees with access to Personal Data are trained regularly regarding the applicable data protection laws and regulations | X | X | X |
| | 8.2 Siemens implements an offboarding process for Siemens employees and external vendors. | X | X | X |

**DPT Exhibits – GDPR Overview**

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes.

| # | GDPR Reference | DPA Section | Title |
|---|---|---|---|
| 1. | Article 28 (1) | Section 4 and DPT Exhibits | Technical and organizational measures and DPT Exhibits |
| 2. | Article 28 (2), (3) (d) and (4) | Section 6 | Subprocessors |
| 3. | Article 28 (3) sentence 1 | Section 2 and DPT Exhibits | Details of the processing and DPT Exhibits |
| 4. | Articles 28 (3) (a) and 29 | Section 3 | Instructions |
| 5. | Article 28 (3) (b) | Section 5 | Confidentiality of the processing |
| 6. | Articles 28 (3) (c) and 32 | Section 4 and DPT Security Exhibits | Technical and organizational measures and DPT Exhibits |
| 7. | Article 28 (3) (e) | Section 9.1 | Data subject rights |
| 8. | Articles 28 (3) (f) and 32 | Sections 9.2, Section 4 and DPT Exhibits | Siemens' assistance and DPT Exhibits |
| 9. | Articles 28 (3) (f) and 33 to 34 | Section 8 | Personal Data Breach |
| 10. | Articles 28 (3) (f) and 35 to 36 | Section 9.2 | Siemens' assistance |
| 11. | Article 28 (3) (g) | Section 14 | Term and termination |
| 12. | Article 28 (3) (h ) | Section 10 | Audits |
| 13. | Article 28 (4) | Section 6 | Subprocessors |
| 14. | Article 46 (1) (b) und (c) | Section 7 and DPT Exhibits – Standard Contractual Clauses | Transfers to Non-EEA Recipients and DPT Exhibits – Standard Contractual Clauses |

## Annex – Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

### Clause 1
**Definitions**

For the purposes of the Clauses:

(a) "personal data", "special categories of data", "process/processing", "controller", "processor", "data subject" and "supervisory authority" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) "the data exporter" means the controller who transfers the personal data;

(c) "the data importer" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) "the sub-processor" means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) "the applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) "technical and organisational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

**Clause 2**
**Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

**Clause 3**
**Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

**Clause 4**
**Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing Offerings will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing Offerings which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

**Clause 5**
**Obligations of the data importer**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing Offerings by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

**Clause 6**
**Liability**

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

**Clause 7**
**Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

**Clause 8**
**Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

**Clause 9**
**Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

**Clause 10**
**Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

**Clause 11**
**Subprocessing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

**Clause 12**
**Obligation after the termination of personal data processing Offerings**

1. The parties agree that on the termination of the provision of data processing Offerings, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph