ATTACHMENT 1

SCHEDULE 4 – DATA PROTECTION ADDENDUM (DPA)

1. General

All terms used but not defined in this DPA will have the same meanings provided in the Agreement. If there is any conflict between any provision in this DPA and any provision in the Agreement, this DPA shall control.

2. Definitions

(a) **"Applicable Data Protection Law"** means all applicable law pertaining to the Processing of Personal Data under the Agreement, including, but not limited to, (i) for Personal Data originating from an Authorized Entity located within the EEA, the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), and (ii) for Personal Data originating from an Authorized Entity located within the UK, the UK GDPR and the UK Data Protection Act 2018.

(b) **"Authorized Entity"** shall mean any entity (including Siemens and its group companies) acting as Controller and being entitled by the Agreement to directly or indirectly access or use Services.

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

(d) **"Country with an Adequacy Decision"** means any country for which the EU Commission has decided that such country ensures an adequate level of data protection and for personal data originating from the UK, any country for which UK adequacy regulations have been made under sections 17A or 74A of the Data Protection Act 2018.

(e) **"Data Breach"** means any breach of security (i) leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed, or (ii) would require notification of such event to any third party pursuant to applicable law.

(f) **"EEA"** means the European Economic Area.

(g) **"EU Standard Contractual Clauses"** means the Standard Contractual Clauses (EU) 2021/914.

(h) **"Origination Area"** means the EEA, the UK, Switzerland and each country with similar adequacy requirements as contained in Art. 45 et seq. GDPR.

(i) **"Personal Data"** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(j) **"Processing"** (and its other forms such as Process, Processes, Processed) means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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

(l) **"Processor Binding Corporate Rules"** means binding corporate rules for processors which are approved by the competent supervisory authority.

(m) **"Restricted Personal Data"** means any Personal Data originating from an Authorized Entity located within an Origination Area.

(n) **"Restricted Transfer(s)"** means any Processing (including transfers, international access and onward transfers) of Restricted Personal Data by Provider or any of its Subprocessors outside the relevant Origination Area.

(o) **"Services"** shall mean the Services under the Agreement provided by Provider acting in its role as Processor within the meaning of this DPA.

(p) **"Standard Contractual Clauses"** means the EU Standard Contractual Clauses and the UK Standard Contractual Clauses.

(q) **"Subprocessor(s)"** shall mean any further Processor engaged in the performance of the Services.

(r) **"Transfer Safeguard(s)"** shall mean appropriate safeguards for Restricted Transfers as required by Applicable Data Protection Law, including without limitation any appropriate safeguards required by Article 46 GDPR.

(s) **"UK GDPR"** means the GDPR as incorporated into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.

(t) **"UK Standard Contractual Clauses"** means such standard data protection clauses as are adopted from time to time by the UK Information Commissioners Office (ICO) in accordance with Article 46(2) of the UK GDPR including, but not limited to, the

international data transfer agreement (UK IDTA), and the EU Standard Contractual Clauses as amended by ICO's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("**UK Addendum**").[1]

3. Compliance with Applicable Data Protection Law

The parties shall observe Applicable Data Protection Law as they apply to them and as required herein. In providing Services, Provider shall in particular comply with the provisions of Applicable Data Protection Law regarding the Processing of Personal Data as a Processor.

4. Scope of the Processing

Provider shall Process Personal Data only (a) in accordance with the terms of this DPA and the Agreement; or (b) on other documented instructions from Siemens. Provider shall not Process Personal Data for its own purposes or transfer it to third parties, unless permitted by this DPA. Provider shall immediately inform Siemens if, in its opinion, an instruction from Siemens infringes Applicable Data Protection Law.

5. Details of the Processing Operations Provided by Provider

The details of the Processing operations provided by Provider - in particular the subject matter of the Processing, the nature and purpose of the Processing, types of Personal Data Processed and the categories of affected data subjects - are specified in **Annex I** to this DPA.

6. Technical and Organizational Measures

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, Provider shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, but not limited to, as appropriate: (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing. Without prejudice to the generality of the preceding sentence, Provider shall at all times implement at least the technical and organizational measures described in **Annex II** to this DPA.

7. Commitment to Confidentiality

Provider shall limit its personnel's access to Personal Data on a need-to-know basis. Provider shall provide detailed notice to its personnel about the applicable statutory and contractual provisions regarding data protection. Provider shall put its personnel under an obligation to comply with such provisions and, in particular, to hold Personal Data secret and not to Process Personal Data other than according to Siemens' instructions. The obligation to secrecy shall continue to apply after the expiry of this Agreement and the personnel's contractual relationship with the Provider. Provider will provide proof of such obligation upon request.

8. Subprocessors

(a) Provider has Siemens' general authorisation for the engagement of Subprocessors. A current list of Subprocessors commissioned by Provider is contained in **Annex III** to this DPA.

(b) The Provider shall specifically inform Siemens in writing of any intended changes to that list through the addition or replacement of Subprocessors at least 30 days in advance. Provider shall provide Siemens with the information necessary to enable Siemens to exercise the right to object. If Siemens raises no objections within this 30-day period, then this shall be taken as an approval of the new Subprocessor. If Siemens raises objections, Provider will - before authorizing the Subprocessor to access Personal Data - use reasonable efforts to address the concerns and reservations expressed by Siemens and (i) refrain from using the Subprocessor; or (ii) propose to Siemens a reasonable change in the Services or Siemens' configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor. If Provider is unable to eliminate the grounds for the objection by Siemens, Siemens is entitled to terminate the affected Services without any damages or penalties. In the event of termination by Siemens, Provider will refund any prepaid amounts for the applicable Service on a pro-rata basis.

(c) Where the Provider engages a Subprocessor to carry out specific processing activities (on behalf of Siemens and/or Authorized Entities), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the Provider under this DPA.

---

[1] See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

(d) Provider shall provide, at Siemens' request, a copy of such Subprocessor contract and any subsequent amendments to Siemens. To the extent necessary to protect business secrets or other confidential information, including personal data, Provider may redact the text of the contract prior to sharing a copy.

(e) Provider shall adequately and regularly audit the Subprocessor with respect to compliance with these requirements and document the results of such audits.

(f) Provider shall remain fully responsible to Siemens for the performance of the Subprocessor's obligations under its contract with Provider. Provider shall inform Siemens of any failure by the Subprocessor to fulfil its obligations under that contract.

9. International Data Processing

In case of Restricted Transfers to Provider, the Provider shall ensure that such Restricted Transfer is covered by adequate Transfer Safeguards as set forth in this **Section 9** and **Annex III** to this DPA.

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

   (i)   **EEA-Providers**. If the Provider is located within the EEA, the Provider shall enter into the Standard Contractual Clauses (Module 3) with its Subprocessor. **Sections 9(a)(vii)** ("Governing Law"), **9(a)(viii)** ("Choice of Forum and Jurisdiction"), **9(a)(ix)(b)** ("Part 1 of UK Addendum"), and the **second sentence of Section 9(a)(x)** ("Authorized Entities in Other Countries") of this DPA shall not apply if the Provider is located in the EEA.

   (ii)   **NON-EEA Providers**. If the Provider is located outside the EEA, the Restricted Transfer shall be governed by Modules 2 and 3 of the Standard Contractual Clauses. The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Annexes to the Standard Contractual Clauses are set out in **Annexes I to III** to this DPA.

   (iii) **Docking Clause**. The option under Clause 7 of the Standard Contractual Clauses shall not apply.

   (iv)   **Onward Transfers**. Any further onward transfer must comply with Clauses 8 and 9 of the applicable Module of the Standard Contractual Clauses. In case Siemens is located outside the EEA and acts itself as a data importer under Standard Contractual Clauses with Authorized Entities, the third-party beneficiary clause stipulated by Clause 9(e) of the Standard Contractual Clauses shall be in favor of such Authorized Entity.

   (v)   **Use of Subprocessors**. Option 2 under Clause 9 of the Standard Contractual Clauses shall apply. For the purposes of Clause 9(a) of the Standard Contractual Clauses, Provider has Siemens' general authorization to engage Subprocessors in accordance with **Section 8** of this DPA.

   (vi)   **Redress**. In case Provider offers data subjects the option to lodge a complaint with an independent dispute resolution body (see Option in Clause 11 of the Standard Contractual Clauses), Provider shall inform Siemens of the responsible arbitration body in writing and comply with the applicable requirements contained in Clause 11 of the Standard Contractual Clauses and the applicable arbitration rules.

   (vii) **Governing Law**. The governing law for the purposes of Clause 17 of the Standard Contractual Clauses shall be the law that is designated in the governing law section of the Agreement. If the Agreement is not governed by an EU Member State law, the EU Standard Contractual Clauses shall be governed by the laws of Germany.

   (viii) **Choice of Forum and Jurisdiction**. The courts under Clause 18 of the Standard Contractual Clauses shall be those designated in the venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with the Agreement, the parties agree that the courts of Germany, shall have exclusive jurisdiction to resolve any dispute arising from the EU Standard Contractual Clauses.

   (ix)   **Authorized Entities in the United Kingdom**. In case Restricted Transfers originate from Authorized Entities located in the United Kingdom, the following shall apply:

   a. **UK Addendum**. The UK Addendum shall be used, unless otherwise agreed in writing by Siemens.

   b. **Part 1 of UK Addendum**. Part 1 of the UK Addendum shall be applied as follows:

      1. Table 1: The parties' details and key contact information are contained in **Annex I** to this DPA.

      2. Table 2: The version of the Approved EU SCCs (as defined by the UK Addendum) to which the UK Addendum is appended to, are the EU Standard Contractual Clauses with the Modules and Clauses selected above in **Section 9(a)** of this DPA. No personal data received from the Importer is combined with personal data collected by the Exporter.

      3. Table 3: The Appendix Information as required by Table 3 of the UK Addendum are contained in **Annexes I to III** to this DPA.

      4. Table 4: Neither party may terminate the UK Addendum when the Approved Addendum (as defined in the UK Addendum) changes.

   (x)   **Authorized Entities in Other Countries**. In case the Standard Contractual Clauses protect Restricted Transfers from Authorized Entities located outside the EEA and the United Kingdom (e.g., Switzerland), (1) general and specific

references in the Standard Contractual Clauses to the GDPR or EU or Member State law shall have the same meaning as the equivalent reference in the Applicable Data Protection Laws of the country where the Authorized Entity is located, as applicable; and (2) references to the "competent supervisory authority" shall be interpreted as references to competent data protection authority in such country. The governing law, choice of forum and jurisdiction shall be governed by **Sections 9(a)(vii)** and **(viii)** of this DPA, unless required otherwise by the laws applicable to the respective Authorized Entity, in which case the Standard Contractual Clauses shall be governed by the laws of the country in which the Authorized Entity is located and any references to the competent "courts" shall be interpreted as references to competent courts in such country.

(b) **Processor Binding Corporate Rules**. The following shall apply if a Transfer Safeguard is based on Processor Binding Corporate Rules: Provider shall contractually bind such Subprocessor to comply with the Processor Binding Corporate Rules with regard to the Personal Data Processed under this DPA.

(c) **Additional Transfer Safeguards**. In case a Transfer Safeguards is not based on Standard Contractual Clauses, Clause 14 and 15 of the Standard Contractual Clauses shall apply mutatis-mutandis to Restricted Transfers under such other Transfer Safeguard, unless the respective Transfer Safeguard contains in substance, the same rights and obligations concerning (i) local laws and practices affecting compliance with the Transfer Safeguards, and (ii) obligations in case of access by public authorities as contained in Clauses 14 and 15 of the Standard Contractual Clauses.

(d) **Other**. Provider agrees and understands that local Applicable Data Protection Law, may contain similar or additional transfer restrictions as contained in this **Section 9**. In such case Provider agrees to use reasonable efforts and to cooperate with Siemens in good faith to address those requirements.

10. Provider's Assistance

Provider shall reasonably assist Siemens in ensuring compliance with Applicable Data Protection Law, in particular by assisting Siemens as follows:

(a) **Correction, Deletion or Restriction of Processing.** Provider shall either (i) provide the ability to rectify, erase or restrict the Processing of Personal Data via the functionalities of the Services, or (ii) rectify, erase or restrict the Processing of Personal Data as instructed by Siemens.

(b) **Access to Personal Data**. To the extent information relating to a data subject is not accessible through the Service, Provider will, as necessary to enable Siemens and Authorized Entities to meet its obligations under applicable Data Protection Laws, provide assistance to make such information available to Siemens and/or Authorized Entities.

(c) **Data Subject and Authority Requests**. Provider shall promptly notify Siemens concerning: (i) any request or complaints received or any notices of investigation by a law enforcement, governmental or regulatory authority or agency; and (ii) any request received directly from any data subject about their Personal Data.
   With respect to (i) and (ii) above, Provider shall not respond without instructions from Siemens. If so instructed, Provider shall reasonably support Siemens in answering such requests.

(d) **Data Portability**. Upon Siemens' request and if required under Applicable Data Protection Law, Provider will either (i) provide the ability to extract Personal Data by reference to a specific data subject in accordance with the functionalities of the Service or (ii) make the relevant set of data available to Siemens and/or the respective Authorized Entity, in each case in a structured, commonly used and machine-readable format.

(e) **Data Protection Impact Assessments.** If requested by Siemens, Provider shall provide all information and reasonable support to carry out data protection impact assessments under Applicable Data Protection Laws.

11. Termination of the Data Processing Relationship

Upon termination of the data Processing relationship, unless otherwise instructed by Siemens or set forth herein, Provider shall return to Siemens all Personal Data made available to Provider or obtained or generated by Provider in connection with the contractually agreed Services and shall irrevocably delete or destroy any remaining data. The deletion or destruction shall be confirmed by Provider in writing upon request.

12. Notification Obligations

(a) Provider shall notify Siemens immediately but in any event within 48 hours in case Provider discovers or reasonably suspects any Data Breach.

(b) In the notification to Siemens, Provider shall provide Siemens with the following information: (i) details of a contact point where (or from whom) more information can be obtained, (ii) a description of the nature of the breach (including, where possible, names, categories and approximate number of data subjects and personal data records concerned), (iii) the likely consequences and the measures taken or proposed to address the breach, including where appropriate, measures to mitigate its possible adverse effects. If and to the extent it is not possible to provide all information at the same time, the initial notification shall

contain the information then available and further information shall be, as it becomes available, subsequently provided without undue delay.

(c) Any notifications under this **Section 12** shall be made (i) to the respective point of contact identified in the Agreement and (ii) to dataprotection@siemens.com.

(d) Provider shall, at Provider's cost and expense, (i) cooperate fully with Siemens in the investigation of a Data Breach; (ii) assist and cooperate with Siemens concerning any legally-required notifications or disclosures to affected persons (by individual communication, public communication via the media or by similar measures), law enforcement, regulators and/or other third parties; and (iii) take any other action Siemens deems necessary regarding such Data Breach, and any dispute, inquiry or claim that concerns the Data Breach.

(e) Unless applicable law or an order of a competent regulator requires otherwise, Siemens shall make the ultimate determination, in its sole discretion, (i) whether a Data Breach requires notification and (ii) of the manner of the notification. In the event that the Provider provides such notifications regarding a Data Breach, any such notices must be approved, in advance, by Siemens.

(f) Provider shall at its cost take appropriate measures to address the Data Breach, including measures to mitigate its adverse effects (including steps to protect the operating environment). Provider also shall take prompt steps designed to prevent the recurrence of any Data Breach, including any action required by Applicable Data Protection Law.

(g) Provider shall reimburse to Siemens all costs and expenses incurred for such Data Breach caused by Provider, including but not limited to the costs of providing credit monitoring to the individuals whose Personal Data was affected by the Data Breach. Limitations of liability in favor of Provider under the Agreement shall not apply in this respect.

13. Documentation and Audits

(a) Provider shall (i) monitor, by appropriate means, its own compliance with its data protection obligations under this DPA and Applicable Data Protection Law; (ii) create related periodic (at least annual) and occasion-based reports (each a "**Report**"); and (iii) make the Reports available to Siemens and Authorized Entities upon request. Where a control standard and framework implemented by Provider provides for controls, such controls will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.

(b) If required to adequately address its audit rights and obligations under Applicable Data Protection Law, the applicable Transfer Safeguards or if requested by a competent data protection authority or other competent government authority or agency, Provider shall make available to Siemens and Authorized Entities - in addition to the Reports - all further information reasonably requested and allow for and contribute to audits, including inspections, conducted by Siemens or Authorized Entities or another auditor mandated by Siemens or Authorized Entities. For such purpose, Siemens, Authorized Entities or another auditor mandated by Siemens or Authorized Entities shall also have the right to carry out on-site inspections during regular business hours, without disrupting the Provider's business operations, and after a reasonable prior notice.

14. Use of Cookies

If the Service makes use of cookies or similar technologies, the following shall apply: Provider shall, unless specifically agreed otherwise by Siemens with reference to this **Section 14**, only store information (e.g., by writing a cookie), or gain access to information already stored in the terminal equipment of a user of the Service (e.g., via a cookie) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the Provider to provide the core functionalities of the Services.

15. Miscellaneous

Provider understands and agrees that the requirements in this DPA are an integral part of the Agreement and, a material breach of any of these requirements shall be considered a material breach by Provider of the Agreement, entitling Siemens to material breach related remedies contained in the Agreement.

16. Additional Requirements Concerning Data of Siemens US Companies

If and to the extent Provider accesses Personal Data received from a Siemens group company established in the United States of America ("**Siemens US Company**") or of a data subject that is the resident of the United States of America, then in addition to the above, Provider: (i) shall comply with U.S federal, state and local laws regarding Personal Data that are applicable to Provider, such Personal Data, and owners or controllers of such Personal Data; when the foregoing is applicable, the term "Applicable Data Protection Law" as used herein shall include the foregoing laws; (ii) except as specifically provided herein or the Agreement, shall not sell, share, rent, release, disclose, disseminate, or make available Personal Data to third parties; and shall not combine the Personal Data with other information; (iii) shall notify Siemens if Provider makes a determination that Provider can no longer meet its obligations hereunder; (iv) shall ensure that each person processing Personal Data is subject to a duty of confidentiality with respect to the Personal Data; (v) shall be deemed, and shall act as, a "service provider" under Applicable Data Protection Law (including the California Consumer Privacy Act, its implementing regulations, and any amendments thereto); and (vii) hereby certifies that it understands the restrictions contained herein and will comply with them.

Annex I to the DPA (and, where applicable, the Standard Contractual Clauses)

A. **LIST OF PARTIES**

Services recipient / data exporter:

Name:	Siemens Industry Software Inc. <Modify as appropriate>
Address:	5800 Granite Parkway, Suite 600, Plano, Texas 75024 <Modify as appropriate>
Contact name, position and contact details	Office of the Siemens Data Protection Officer Werner-von-Siemens-Straße 1, 80333 Munich, Germany E-Mail: datapotection@siemens.com
Activities relevant to the data transferred/Processed	Provider provides a cloud cybersecurity platform SIGRID as OEM service for Siemens, who bundled this product with Siemens Polarion. SIGRID is used to scan end customer source code and identify security vulnerabilities in the source code.
Role (Controller/Processor)	Siemens acts as Controller for the processing activities provided by Provider vis-à-vis Siemens and as Processor under the instructions of its Authorized Entities for processing activities provided by Provider vis-à-vis Authorized Entities.

Provider / data importer:

Name:	[Insert]
Address:	[Insert]
Contact name, position and contact details	[Insert]
Activities relevant to the data transferred/Processed	See above table
Role (Controller/Processor)	Provider acts as Processor Processing Personal Data on behalf of Siemens and, as the case may be, Authorized Entities.

B. DESCRIPTION OF TRANSFER / PROCESSING OPERATIONS

Categories of data subjects whose Personal Data is transferred/Processed:	☒ Employees and staff (including applicants, regular, temporary, part-time, trainees, contractors and agents) ☒ Contact persons at business partners, suppliers, vendors and other cooperation partners ☒ Customer(s) and/or their employees and staff (including applicants, regular, temporary, part-time, trainees, contractors and agents) ☒ Users of Siemens software products/services ☐ Other, please list: <mark>insert</mark> Further affected data subjects whose personal data is contained in an application or IT system which is in scope of the Services provided.
Categories of Personal Data transferred/Processed	☒ Contact information (such as name, address, phone or fax number, email address, etc.) ☒ Organizational organization (such as job position, department, etc.) ☒ Location data (such as GPS, etc.) ☐ Governmental and personal identifiers (such as social security number, driver's license number, social insurance number, etc.) ☐ Financial data (such as income, loan files, transactions, credit information, purchase and consumption habits, insolvency status, etc.) ☐ Employment data (such as recruiting data and qualification, compensation and payroll data, employee identification data, employee status, attendance data, work history data, etc.) ☒ User account data (such as username/ID and password, etc.) ☒ Information related to data subject's use of IT assets (such as IP address, login information, credentials, etc.) ☐ Financial account information (such as banking/ credit card data, account numbers, credit card numbers, etc.) ☐ Other; please list: <mark>insert</mark> Any further personal data contained in an application or IT system which is in scope of the Services provided.

Special categories of Personal Data to be accessed or Processed	☐ Information on racial or ethnic origin ☐ Information on political opinions ☐ Information on religious or philosophical beliefs ☐ Information on trade union membership ☐ Information on sex life or sexual orientation ☐ Biometric data ☐ Genetic data ☐ Health data (such as mental or physical disabilities, family medical history, personal medical history, medical records, prescriptions, etc.) ☐ Other; please list: <mark>insert</mark> The restrictions or safeguards applied to such sensitive Personal Data are described in **Annex II** to this DPA

The frequency of the transfer (accessing/Processing)	☒ Provider hosts Personal Data on behalf of Siemens and, as the case may be, Authorized Entities
	
	☒ Provider remotely accesses Personal Data when providing the services
	    ☐ on one-off basis
	    ☒ on continuous basis
	
	☐ Provider otherwise Processes Personal Data when providing the services
	    ☐ on one-off basis
	    ☐ on continuous basis

Nature of the Processing	☒ Collection ☒ Recording ☒ Organisation ☒ Structuring ☒ Storage ☒ Adaptation or alteration ☐ Retrieval ☐ Consultation ☒ Use ☐ Disclosure by transmission ☐ Dissemination ☒ Otherwise making available ☒ Alignment or combination ☒ Restriction ☒ Erasure or destruction of data ☒ Remote-access ☐ Other: <mark>insert</mark>

Purpose/activities relevant to the data transferred/Processed	☒ Provider provides **maintenance and support services** and may have access, including remote-access to Personal Data. ☒ Provider provides **professional services** by performing services in connection with an application/system or network such as: installation, configuration or data migration or other related IT services and may have access, including remote access to Personal Data. ☐ Provider provides **managed services**, including data center and infrastructure management, backup and recovery management and may have access, including remote access to Personal Data. ☐ Provider provides **XaaS (Software-, Platform-, or Infrastructure-as-a-Service)** by providing hosting, operation, management and maintenance and support services. ☐ Other: <mark>insert</mark>
Duration	☒ The Personal Data will be retained for the period of the SOW. ☒ The Personal Data will be retained for a period of: <mark>insert</mark> ☐ Other: <mark>insert</mark>
For transfers to Subprocessor(s), also specify subject matter, nature and duration of the Processing	The subject matter, nature and duration of the processing are specified per Subprocessor in **Annex III** to this DPA.

C. COMPETENT SUPERVISORY AUTHORITY

- Where Siemens is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Siemens with the GDPR as regards the data transfer shall act as competent supervisory authority. For Siemens Aktiengesellschaft, Germany, the supervisory authority is:
  > Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
  > Promenade 18
  > 91522 Ansbach
  > Germany

- Where Siemens is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2), the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) GDPR is established shall act as competent supervisory authority; namely:
  > Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
  > Promenade 18
  > 91522 Ansbach
  > Germany

Annex II to the DPA (and, where applicable, the Standard Contractual Clauses)

Technical and Organisational Measures (Including Technical and Organisational Measures to Ensure the Security of the Data)

The following measures shall only apply to the Provider, insofar as the underlying IT systems, networks and applications are the responsibility of and/or under the custody or control of the Provider. Description of the technical and organizational security measures implemented by the Provider and its Subprocessor(s):

#	Measures	SFeRA Rule ID
1.	**Physical and Environmental Security**	
	Provider 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; b) protecting and restricting access paths; c) securing the decentralized data processing equipment and personal computers; d) establishing access authorizations for employees and third parties, including the respective documentation; e) regulations on access cards; f) restrictions on access cards; g) all access to the data center where Personal Data is hosted will be logged, monitored, and tracked; h) the data center where Personal Data is hosted is secured by restricted access controls, and other appropriate security measures; and i) maintenance and inspection of supporting equipment in IT areas and data centers shall only be carried out by authorized personnel.	11.1.1-02
2.	**Access Control (IT-Systems and/or IT-Application)**	
	2.1 Provider implements a roles and responsibilities concept.	06.1.1-01
	2.2 Provider implements an authorization and authentication framework including, but not limited to, the following elements: a) role-based access controls implemented; b) process to create, modify, and delete accounts implemented; c) access to IT systems and applications is protected by authentication mechanisms; d) appropriate authentication methods are used based on the characteristics and technical options of the IT system or application; e) access to IT systems and applications shall require, at least, two-factor authentication for privileged accounts; f) all access to Personal Data is logged, monitored, and tracked; g) authorization and logging measures for inbound network connections to IT systems and applications (including firewalls to allow or deny inbound network connections) implemented; h) privileged access rights to IT systems, applications, and network services are only granted to individuals who need it to accomplish their tasks (least-privilege principle); i) privileged access rights to IT systems and applications are documented and kept up to date; j) access rights to IT systems and applications are reviewed and updated on regular basis; k) password policy implemented, including requirements regarding password complexity, minimum length and expiry after adequate period of time, no re-use of recently used passwords; l) IT systems and applications technically enforce password policy; m) access rights of employees and external personnel to IT systems and applications is removed immediately upon termination of employment or contract; and n) use of secure state-of-the-art authentication certificates ensured.	09.1.1-02 09.1.1-03 09.2.3-01 09.4.2-02
	2.3 IT systems and applications lock down automatically or terminate the session after exceeding a reasonable defined idle time limit.	11.2.9-03 11.2.9-04
	2.4 Provider limits privileged access to cloud assets to single or specific ranges of IP addresses.	ST002-0008
	2.5 Privileged access to cloud assets is done through a bastion host.	ST002-0009
	2.6 Provider maintains log-on procedures on IT systems with safeguards against suspicious login activity (e.g., against brute-force and password guessing attacks).	09.4.2-02
3.	**Availability Control**	
	3.1 Provider protects systems and applications against malicious software by implementing appropriate and state-of-the-art anti-malware solutions.	12.2.1-01
	3.2 Provider defines, documents and implements a backup concept for IT systems, including the following technical and organizational elements:	

LIST OF SUBPROCESSORS AND DATA CENTER LOCATIONS

A. **Entities (including Provider and Subprocessor(s)) engaged in the storage/hosting of content**

If and to the extent the provision of the Services consists of or includes the hosting of Personal Data, Provider shall store the Personal Data in the data center locations specified below ("**Data Center Location**"). Provider shall not transfer Personal Data from the respective Data Center Location without Siemens' consent. The notification and objection mechanism contained in **Section 8** shall not apply in this regard.

Entity Name and Registered Address	Data Center Location	Regions Served from Data Center Location	Transfer Safeguards in Case of Restricted Transfers
Entity name: [...] Registered address: [...] Contact person: [...]	[insert location of data center, e.g., European Union]	[describe whether a certain data center serves all in-scope region or whether there are dedicated data centers for certain regions]	☐ **No Restricted Transfer** ☐ **Standard Contractual Clauses** ☐ **Processor BCR** ☐ **Other: _____**
Entity name: [...] Registered address: [...] Contact person: [...]	[...]	[...]	☐ No Restricted Transfer ☒ Standard Contractual Clauses ☐ Processor BCR ☐ Other: _____

B. **Subprocessors engaged in the Processing of Personal Data for non-storage/hosting purposes**

Entity Name, Registered Address and Contact Person (including name, position and contact details)	Country/Region Where Processing is Performed	Regions Served by the Subprocessor	Description of Processing (including a clear delimitation of responsibilities in case several Subprocessors are authorized)	Transfer Safeguards in Case of Restricted Transfers
Entity name: [...] Registered address: [...] Contact person: [...]	[insert location of where the data are processed, e.g., European Union]	[describe whether the Subprocessor serves all in-scope region or whether the Subprocessor only serves certain regions]	[please describe, please also indicate where necessary the duration of the processing]	☐ **No Restricted Transfer** ☐ **Standard Contractual Clauses** ☐ **Processor BCR** ☐ **Other: _____**
Entity name: [...] Registered address: [...] Contact person: [...]	[...]	[...]		☐ No Restricted Transfer ☐ Standard Contractual Clauses ☐ Processor BCR ☐ Other: _____