Data Processing Annex (DPA)

This Data Processing Annex ("**DPA**") is attached to, and forms part of, [insert title of agreement] ("**Agreement**"). 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.

1. Definitions

"**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 in Switzerland, the Federal Act on Data Protection (FADP), (ii) for Personal Data originating from an Authorized Entity located within the EEA, the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), and (iii) for Personal Data originating from an Authorized Entity located within the UK, the UK GDPR and the UK Data Protection Act 2018.

"**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.

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

"**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.

"**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.

"**EEA**" means the European Economic Area.

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

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

"**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.

"**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.

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

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

"**Provider**" means the provider being a party to the Agreement or related individual agreement, adoption agreement, purchase order or other contractual arrangements referencing the Agreement.

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

"**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.

"**Services**" shall mean the Services under the Agreement provided by Provider acting in its role as Processor within the meaning of this DPA. In the Agreement, Services as defined herein may be referred to as "Cloud-Services", "Online Services", "Offering", "Product" or otherwise.

"**Siemens**" means the respective Siemens group company being a party to the Agreement or related individual agreement, adoption agreement, purchase order or other contractual arrangements referencing the Agreement.

"**Standard Contractual Clauses**" means the EU Standard Contractual Clauses; and the UK Standard Contractual Clauses.

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

"**Transfer Safeguard(s)**" shall mean appropriate safeguards for Restricted Transfers as required by Applicable Data Protection Law, such as appropriate safeguards as required by Article 46 GDPR.

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

"**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].

2. 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.

3. Scope of the processing

Provider shall Process Personal Data only (i) in accordance with the terms of this DPA and the Agreement; or (ii) 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.

4. 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**.

5. 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: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) 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**.

6. 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.

7. 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.

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

[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/.

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.

b) 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.

c) Provider shall provide, at Siemens' request, a copy of such a 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.

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

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

8. International Data Processing

Provider shall ensure that Restricted Transfers are covered by adequate Transfer Safeguards as set forth in Annexes III and IV, unless the Restricted Transfer is made to a Country with an Adequacy Decision.

9. 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.

10. 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.

11. 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) The details of a contact point where 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) its

likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, 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, as it becomes available, subsequently be provided without undue delay.

c) Any notifications under this Section 11 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) 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 this Agreement shall not apply in this respect.

12. 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.

13. 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 13, 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 provide the core functionalities of the Services.

14. 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.

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

A. LIST OF PARTIES

Service recipient / Data exporter:

Name:	[Siemens Switzerland Ltd.]
Address:	[Freilagerstrasse 40, 8047 Zürich, Schweiz]
Contact name, position and contact details	Office of the Siemens Data Protection Officer Werner-von-Siemens-Straße 1, 80333 Munich, Germany E-Mail: dataprotection@siemens.com
Activities relevant to the data transferred/Processed	Siemens is a technology company focused on industry, infrastructure, transport, and healthcare.
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	[Insert]
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 (such as applicants, regular, temporary, part-time, trainees, contractors and/or 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: [insert] 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) ☐ Organizational organization (such as job position, department) ☐ Geolocation data (such as GPS) ☐ Governmental and personal identifiers (i.e., social security number, driver's license number, social insurance number)

	☐ Financial data (such as income, loan files, transactions, credit information, purchase and consumption habits, insolvency status) ☐ Employment data (such as recruiting data and qualification, compensation and payroll data, employee identification data, employee status, attendance data, work history data) ☐ User account data (such as username/ID and password) ☐ Information related to data subject's use of IT assets (such as IP address, login information) ☐ Financial account information, such as banking/ credit card data, account numbers, credit card numbers, etc. ☐ Other; please list: [insert] 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	☐ None ☐ 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 (mental or physical disabilities, family medical history, personal medical history, medical records, prescriptions, etc.) ☐ Other; please list: [insert] The restrictions or safeguards applied to such sensitive Personal Data are described in **ANNEX II**
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
Purpose/activities relevant to the data transferred/Processed; Nature of the Processing	☐ 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) services** hosted by Provider (or any of its Subprocessors). This may include collection, storage, reorganization, adaptation and making available of Personal Data. ☐ Other: [insert]

Duration	☐ The Personal Data will be retained for the period of the Agreement. Siemens has the ability to rectify, erase or restrict the Processing of Personal Data via the functionalities of the Services, or (ii) Provider rectifies, erases or restricts the Processing of Personal Data as instructed by Siemens ☐ The Personal Data will be retained for a period of: [please indicate] ☐ Other: [insert]
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**.

C. COMPETENT SUPERVISORY AUTHORITY

- Office of the Federal Data Protection and Information Commissioner FDPIC
  Feldeggweg 1
  CH - 3003 Berne

- Where Siemens is not established in an EU Member State, but falls within the 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 ORGANISTIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational security measures implemented by the Provider and its Subprocessor(s):

[Please select]

☐ The technical and organizational measures are described in the cybersecurity related clauses and/or Annexes of the Agreement, including Annex [insert reference to Cybersecurity Annex]

[*Siemens internal comment: You may use this option **only** if the unaltered "Siemens Cybersecurity Contract Clauses for indirect material" for "XaaS" or "Application Management Service and IT Outsourcing" are used and made part of the Agreement.*]

☐ Provider and its Subprocessor(s) implement the technical and organizational measures described below. The parties agree that cybersecurity related clauses and/or Annexes of the Agreement (if any) may contain further technical and organizational measures.

#	Measures
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.
2.	Access Control (IT-Systems and/or IT-Application)
	2.1 Provider implements a roles and responsibilities concept.
	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.
	2.3 IT systems and applications lock down automatically or terminate the session after exceeding a reasonable defined idle time limit.
	2.4 Provider limits privileged access to cloud assets to single or specific ranges of IP addresses.

#	Measures
	2.5 Privileged access to cloud assets is done through a bastion host.
	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).
3.	Availability Control
	3.1 Provider protects systems and applications against malicious software by implementing appropriate and state-of-the-art anti-malware solutions.
	3.2 Provider 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); b) defined backup intervals; and c) the restoration of data from backups is tested regularly based on the criticality of the IT system or application.
	3.3 Provider stores backups in a physical location different from the location where the productive system is hosted.
	3.4 IT systems and applications in non-production environments are logically or physically separated from IT systems and applications in production environments.
	3.5 Data centers in which Personal Data is stored or processed are protected against natural disasters, physical attacks or accidents.
	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.
4.	Operations Security
	4.1 Provider maintains and implements an Information Security Framework reflecting the measures described herein, which is regularly reviewed and updated.
	4.2 Provider 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.
	4.3 Provider continuously analyzes the respective IT systems and applications log data for anomalies, irregularities, indicators of compromise and other suspicious activities.
	4.4 Provider scans and tests IT systems and applications for security vulnerabilities on a regular basis.
	4.5 Provider implements and maintains a change management process for IT systems and applications.
	4.6 Provider maintains a process to update and implement vendor security fixes and updates on the respective IT systems and applications.
	4.7 Provider irretrievably erases data or physically destroys the data storage media before disposing or reusing of an IT system.
5.	Transmission Controls
	5.1 Provider documents and updates network topologies and its security requirements on regular basis.
	5.2 Provider 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); b) Proxy servers; c) Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS); d) URL filtering; and e) Security Information and Event Management (SIEM) systems.
	5.3 Provider administers IT systems and applications by using state-of-the-art encrypted connections.
	5.4 Provider protects the integrity of content during transmission by state-of-the-art network protocols, such as TLS.
	5.5 Provider encrypts or enables Siemens to encrypt, Siemens data that is transmitted over public networks.
	5.6 Provider encrypts, or enables Siemens to encrypt, Siemens data when it is stored on Provider data bases.
	5.7 Provider uses secure Key Management Systems (KMS) to store secret keys.

#	Measures
6.	Security Incidents
	Provider maintains and implements an incident handling process, including but not limited to a) records of security breaches; b) Provider notification processes; and 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.
7.	Asset Management, System Acquisition, Development and Maintenance
	7.1 Provider 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.
	7.2 Provider establishes a formal process to control and perform changes to developed applications.
	7.3 Provider plans and incorporates security tests into the System Development Life Cycle of IT systems and applications.
	7.4 Provider implements an adequate security patching process that includes: a) monitoring of components for potential weaknesses (CVEs); b) priority rating of fix; c) timely implementation of the fix; and d) download of patches from trustworthy sources.
8.	Human Resource Security
	8.1 Provider implements the following measures in the area of human resources security: a) employees with access to Personal Data are bound by confidentiality obligations; and b) employees with access to Personal Data are trained regularly regarding the applicable data protection laws and regulations.
	8.2 Provider implements an offboarding process for Provider employees and external vendors.
9.	Cryptography
	9.1 Provider uses secure state-of-the-art certificates and implements the following: a) digital certificates are only accepted and trusted if the digital certificate was issued by a trusted certification authority; b) certificates are used and allocated to dedicated IT-systems and applications; and the validity of digital certificates is verified.
	9.2 Provider implements a process for the management and implementation of cryptographic keys, including rules and requirements to generate, store, backup, distribute, and revoke cryptographic keys.

Annex III to the DPA (and, where applicable, the Standard Contractual Clauses)
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 7 shall not apply in this regard.

Entity Name, registered address and contact person (including name, position and contact details)	**Data Center Location**	**Regions served from Data Center Location**	**Transfer Safeguards in case of Restricted Transfers**
Entity name: […] Register 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: […] Register 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: […] Register 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: […] Register Address: […] Contact person: […]	[…]	[…]		☐ No Restricted Transfer ☐ Standard Contractual Clauses ☐ Processor BCR

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: […] Register 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: _____
				☐ Other: _____

Annex IV to the DPA

INTERNATIONAL DATA PROCESSING

In case of Restricted Transfers to Provider, the applicable Transfer Safeguard shall be the Standard Contractual Clauses, unless otherwise agreed in writing by Siemens. In case of Restricted Transfers to any Subprocessor, the Provider shall ensure that such Restricted Transfer is covered by the Transfer Safeguards stated in Annex III.

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

a) **EEA Providers**. If the Provider is located within the EEA, the Provider shall enter into the Standard Contractual Causes (Module 3) with its Subprocessor. Section1 paragraph g), h), i) (ii) and paragraph j) sentence 2 shall not apply if the Provider is located in the EEA.

b) **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 of this DPA.

c) **Docking clause**. The option under Clause 7 of the Standard Contractual Causes shall not apply.

d) **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.

e) **Use of Subprocessors**. Option 2 under Clause 9 shall apply. For the purposes of Clause 9 a), Provider has Siemens' general authorization to engage Subprocessors in accordance with Section 7 of this DPA.

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

g) **Governing Law**. The governing law for the purposes of Clause 17 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.

h) **Choice of forum and jurisdiction**. The courts under Clause 18 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.

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

(i) The UK Addendum shall be used, unless otherwise agreed in writing by Siemens.

(ii) Part 1 of the UK Addendum shall be applied as follows

Table 1 of the UK Addendum: The parties' details and key contact information are contained in Annex 1 to this DPA.

Table 2 of the UK Addendum: The version of the Approved EU SCCs (as defined by the UK Addendum) which the UK Addendum is appended to, are the EU Standard Contractual Clauses with the Modules and Clauses selected in section 1 of this Annex IV. No Personal Data received from the Importer is combined with Personal Data collected by the Exporter.

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

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

j) **Authorized Entities in other Countries**. [1]In case the Standard Contractual Clauses protect Restricted Transfers from Authorized Entities located outside the EEA and the United Kingdom (e.g. Switzerland), (i) 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 (ii) references to the "competent supervisory authority" shall be interpreted as references to competent data protection authority in such country. [2]The governing law, choice of forum and jurisdiction shall be governed by Sections 1 g) and h) above, 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.

2. 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.

3. 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.

4. Other. Provider agrees and understands that local Applicable Data Protection Law may contain similar or additional transfer restrictions as those contained in this Annex IV. In such case Provider agrees to use reasonable efforts and to cooperate with Siemens in good faith to address those requirements.