

Data Processing Addendum

This Data Processing Addendum (“**DPA**”) forms part of, and is subject to, the Master Services Agreement or other written agreement (the “**Agreement**”) executed between the member of the Semperis Group that is a party to such Agreement (“**Semperis**”) and the entity or person defined as ‘Customer’ thereunder, and each Customer Affiliate that is party to an Order Form pursuant to the Agreement (collectively and individually referred to herein as “**Customer**”; and together with Semperis, collectively, the “**Parties**” or individually, a “**Party**”). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. All capitalized terms not defined in this DPA or in the Agreement shall have the meaning ascribed to them in the applicable Data Protection Laws.

1. **Definitions.**

- 1.1. “**Controller**” means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.
- 1.2. “**Data Privacy Framework**” means (as applicable) the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework self-certification programs operated by the U.S. Department of Commerce, and their respective successors.
- 1.3. “**Data Privacy Framework Principles**” means the principles and supplemental principles contained in the relevant Data Privacy Framework, as may be amended, superseded, or replaced from time to time.
- 1.4. “**Data Protection Laws**” means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, as applicable: (i) California Consumer Privacy Act as amended by the California Privacy Rights Act, Cal. Civ. Code §1798.100 et seq. and the regulations at 11 C.C.R. §7000 et seq., and any binding regulations promulgated thereunder (“**CCPA**”), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) (“**EU GDPR**” or “**GDPR**”), (iii) the Swiss Federal Act on Data Protection (“**FADP**”), and (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the “**UK GDPR**”); in each case, as updated, amended, or replaced from time to time.
- 1.5. “**Data Subject**” means the identified or identifiable natural person to whom Customer Personal Data relates.
- 1.6. “**European Transfer**” means a transfer (directly from Customer to Semperis or via onward transfer by Semperis) of Customer Personal Data that is subject to GDPR, UK GDPR or FADP to a country outside the European Economic Area, the United Kingdom, and Switzerland.
- 1.7. “**Personal Data**” means information about an identified or identifiable natural person, or that otherwise constitutes “personal data”, “personal information”, “personally identifiable information” or similar terms as defined in Data Protection Laws.
- 1.8. “**Processing**” refers to any operation that is performed on 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.
- 1.9. “**Processor**” means a natural or legal person, public authority, agency, or other body that Processes Personal Data on behalf of the Controller.
- 1.10. “**Standard Contractual Clauses**” means the standard contractual clauses approved pursuant to Commission Decision (EU) 2021/91 of 4 June 2021.
- 1.11. “**Sub-processor**” means Semperis’ affiliates and third parties engaged by Semperis (or by Semperis’ affiliates) for the provision of any or all of the services provided by Semperis, who process Customer Personal Data in accordance with this DPA.
- 1.12. “**UK Addendum**” means the International Data Transfer Addendum issued by the Information Commissioner’s Office under s.119(A) of the UK Data Protection Act 2018.

2. Scope and Applicability. This DPA applies only where and to the extent that Semperis is Processing Personal Data as a Processor on behalf of the Customer in the course of providing Semperis products or services. It does not apply to Semperis' Processing Personal Data of Customer's representatives to market or promote its products, to administer the business or contractual relationship between Semperis and the Customer or in other instances where Semperis operates as the Controller.

3. Roles and Scope of Processing.

3.1. Semperis shall Process Customer Personal Data only as a Processor (or sub-processor) acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined therein, in each case regardless of whether Customer acts as a Controller or as a Processor on behalf of a third-party Controller (such third-party, the "**Third-Party Controller**") with respect to Customer Personal Data. To the extent any usage or performance data is considered Personal Data under applicable Data Protection Laws, Semperis is the Controller of such data and shall Process such data in accordance with the Agreement and applicable Data Protection Laws.

3.2. Semperis will Process Customer Personal Data only for the purposes set forth in the Agreement. Customer shall ensure its Processing instructions are lawful and that the Processing of Customer Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. The Parties agree that the Agreement (including this DPA) sets out the exclusive instructions to Semperis for all Processing of Customer Personal Data, and (if applicable) include and are consistent with all instructions from Third-Party Controllers. Any additional requested instructions require the prior written agreement of Semperis. Semperis shall promptly notify Customer if, in Semperis' opinion, such instruction violates Data Protection Laws. Where applicable, Customer shall be responsible for any communications, notifications, assistance and/or authorizations that may be required in connection with a Third-Party Controller.

3.3. Each Party will comply with its respective obligations under Data Protection Laws.

4. Data Transfers

4.1. European Data Transfers

4.1.1 If the Data Privacy Framework applies to the European Transfer, Semperis shall ensure that it provides at least the same level of protection to such Customer Personal Data as is required by the Data Privacy Framework Principles.

4.1.2 If Data Protection Laws applicable to the European Transfer require the European Transfer to be subject to appropriate safeguards, the Standard Contractual Clauses will apply to such European Transfer, and Semperis and Customer shall enter the Standard Contractual Clauses (with respect to Customer's transfer of Customer Personal Data from the European Economic Area or Switzerland) and/or the UK Addendum (with respect to Customer's transfer of Customer Personal Data from the United Kingdom), and the respective European Transfer shall be governed by such terms. The Standard Contractual Clauses and UK Addendum (as applicable) shall be incorporated into the Agreement and deemed signed by the Parties. For transfers from Switzerland, references in the Standard Contractual Clauses shall be interpreted to include applicable terminology for Switzerland (e.g.: "Member State" shall be interpreted to mean "Switzerland").

4.1.3 With respect to the Standard Contractual Clauses, Semperis and the Customer hereby assent to the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, under its MODULE TWO, as follows:

1. In Section II (Obligations of the Parties), Clause 9(a) for MODULE TWO: Transfer Controller to Processor: Option 2 applies. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right

to object

2. In Section II (Obligations of the Parties), Clause 11(a) for MODULE TWO: Transfer Controller to Processor: the optional language shall not apply.
3. In Section II (Obligations of the Parties), Clause 13(a) for MODULE TWO: Transfer Controller to Processor: the following option will apply: The supervisory authority of one of the Member States in which the Data Subjects whose Personal Data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
4. In Section IV (Final Provisions), Clause 17 for MODULE TWO: Transfer Controller to Processor: The Parties agree that this shall be the law of Ireland.
5. In Section IV (Final Provisions), Clause 18(b) for MODULE TWO: Transfer Controller to Processor: The Parties agree that those shall be the courts of Ireland.
6. In Annex I, for MODULE TWO: Transfer Controller to Processor:
 - a. Data Exporter: The Customer.

Activities relevant to the data transferred under these Clauses in one or more of these scenarios, which involve the provision of Personal Data to the data importer, including transfers outside of the European Economic Area: (A) using the Product in a software-as-a-service deployment model ("SaaS Services") and which involve processing Personal Data in the course of data hosting; (B) seeking of technical support for the Product; (C) seeking professional services which involve processing Personal Data in the course of performing the services.

Role: Controller

- b. Data Importer: Semperis.

Activities relevant to the data transferred under these Clauses in one or more of these scenarios, which involve the receipt of Personal Data from the data exporter, including through transfers to the data importer outside of the European Economic Area: (A) operating the Product in the software-as-a-service deployment model and which involves processing Personal Data in the course of data hosting; (B) providing technical support for the Product; (C) providing professional services which involve processing Personal Data in the course of performing the services.

Role: Processor.

4.2 U.S. State-Specific Contract Clauses Prescribed by Data Protection Laws

California: If Semperis Processes Customer Personal Data, which includes Personal Data governed by the CCPA, then the clauses in **Annex A** shall additionally apply in relation to Semperis' role as a 'Service Provider' for such Customer Personal Data.

4.3 Other Data Transfers

If the data transfer mechanisms detailed in Sections 4.1 and 4.2 are not applicable to specific Data Protection Laws, and said Data Protection Laws have prescribed specific mechanisms for the transfer of Customer Personal Data to Semperis and/or contract clauses for Processing of Customer Personal Data by Semperis, Semperis and the Customer shall cooperate to shall make such specific transfer mechanism available. Such transfer mechanisms shall not apply and shall not be incorporated into this DPA if they are not applicable to (i) transfers from Customer to Semperis (including where no such transfer occurs), or (ii) Processing by Semperis of Customer Personal Data.

5. Details of Data Processing

- 5.1 Categories of Data Subjects whose Personal Data is transferred: As determined and transferred by Customer. Usually includes employees and contractors of the Customer. In **Ready1** and **Migrator** may also include former employees and vendors and external third-party contacts.
- 5.2 Categories of Personal Data transferred: As determined and transferred by Customer. Usually includes usernames, email addresses, IP addresses, directory service user identifiers (e.g., identifiers from identity and access management systems such as Microsoft Entra ID/Azure AD, Okta, or similar providers, as applicable) and other information contained in log files and meta-data of the Customer's technology systems. In **Ready1** may also include: first and last names, phone numbers (including mobile phone numbers), business addresses, browser identification data, and user generated content (including disaster recovery plans and incident response details). In **Semperis Recovery** may also include first and last names, phone numbers and customer IdP/tenant configuration and identity object data (such as users, groups, applications/service principals, policies, roles, associations/relationships, backup snapshots, restore/sync payloads, and related customer-generated audit/change history where applicable). In **Migrator**, may also include former employees. In **Migrator** may also include: user and account identifiers, email profile data, device and network identifiers (including MAC addresses), and user activity telemetry data.
- 5.3 Sensitive data transferred: None (with respect to GDPR).
In **Ready1**, CCPA sensitive information, in the form of geolocation data from an end user's browser, may be transferred. In **Migrator**, CCPA sensitive information, in the form of domain passwords, may be transferred.
- 5.4 The frequency of the transfer: (A) As determined by Customer and up to a daily basis (per Customer's preferences) in case of Product deployment in a software-as-a-service model (other than Lightning, Ready1 and Semperis Recovery); (B) At discrete eventualities of technical support requests and professional service assignments; (C) **Lightning**: continuous, at least once per hour; (D) **Ready1**: Logging into sessions is performed at user's discretion. During sessions, browser data is transferred continuously. User generated content is uploaded at user's discretion, as frequently as several times per day; (E) **Semperis Recovery**: as determined by Customer, as often as constantly; and (F) **Migrator**: as determined by Customer.
- 5.5 Nature of the Processing: Recording, storage, consultation, use, disclosure by transmission and erasure, as necessary to store the Personal Data, provide technical support for the Product, and provide professional services.
- 5.6 Purpose(s) of the data transfer and further Processing: (A) Data hosting, in case of deployment in a software-as-a-service model; (B) provision of technical support for the Product or SaaS Services; (C) provision of professional services.
- 5.7 The period for which the Personal Data will be retained: (A) For the duration of the Agreement and for ninety (90) days after the termination or expiration of the Agreement, in case of Product deployment in a software-as-a-service model or professional services; (B) For the duration of technical support requests and for twenty-one (21) days after the completion of such requests;

6. Transfers to Sub-processors

- 6.1 Customer provides Semperis with a general authorization to engage Sub-processors (subject to Section 6.3), as well as Semperis' current Sub-processors listed below and members of the Semperis Group.
- 6.2 Semperis shall: (i) enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Customer Personal Data as Semperis' obligations under this DPA to the extent applicable to the services provided by the Sub-processor; and (ii) remain liable for each Sub-processor's compliance with the obligations under this DPA.
- 6.3 Semperis shall inform Customer of any appointment of new Sub-processors at least ten (10) days in advance of allowing the new Sub-processor to Process Customer Personal Data (the "**Objection Period**"). During the

Objection Period, objections (if any) to Semperis' appointment of a new Sub-processor must be provided to Semperis in writing and based on reasonable grounds. In such event, the Parties will discuss those objections in good faith with a view of achieving resolution. If it can be reasonably demonstrated that the new Sub-processor is unable to Process Customer Personal Data in compliance with the terms of this DPA and Semperis cannot provide an alternative Sub-processor, or the Parties are not otherwise able to achieve resolution as provided in the preceding sentence, Customer, as its sole and exclusive remedy, may terminate the Order Form(s) with respect to only those aspects which cannot be provided by Semperis without the use of the new Sub-processor by providing advance written notice to Semperis of such termination. If Customer provides no objections to Semperis within the Objection Period, the new Sub-processor shall be deemed accepted by Customer.

6.4 Semperis will maintain a list of its third-party sub-processors at www.semperis.com/subprocessors, which may be updated in accordance with Section 6.3.

7. Security. Semperis shall implement the technical and organizational security measures specified at www.semperis.com/technical-organizational-measures as a minimum security standard. Customer acknowledges and agrees that the nature of Semperis' products mean that the technical and organizational measures may be updated from time to time by Semperis, but such updates shall not result in a lesser standard of security than that in place upon execution of this DPA.

8. Customer's Audit Rights.

8.1. Upon written request and at no additional cost to Customer, Semperis shall provide Customer, and/or its appropriately qualified third-party representative (collectively, the "Auditor"), access to reasonably requested documentation evidencing Semperis' compliance with its obligations under this DPA in the form of the relevant audits or certifications, such as (i) Semperis' ISO 27001 or (ii) Semperis' SOC 2 Type II audit reports (collectively, "Reports").

8.2. If additional audit activities are legally required, the Customer may request inspections conducted by the Customer or an Auditor mandated by the Customer ("On-Site Audit"). Such On-Site Audit is subject to the following conditions: (i) On-Site Audits are limited to Semperis Processing facilities and to personnel involved in the Processing activities covered by this DPA; (ii) On-Site Audits shall occur no more than once annually or as required by applicable data protection law or by a competent supervisory authority or immediately subsequent to a material Personal Data breach that affected the Personal Data processed by Semperis under this DPA; (iii) On-Site Audits may be performed during regular business hours, solely insubstantially disrupting Semperis' business operations and in accordance with Semperis' security policies, and after a reasonable prior notice; and (iv) Customer shall bear any costs arising out of or in connection with the On-Site Audit. Customer shall be obliged to create an audit report summarizing the findings and observations of the On-Site Audit ("On-Site Audit Report"). On-Site Audit Reports as well as Audit-Reports are confidential information of Semperis and shall not be disclosed to third parties unless required by applicable data protection law or subject to Semperis' consent. On-Site Audit Reports as well as Audit-Reports shall be provided to Semperis without undue delay.

8.3. Prior to any review of Reports or performance of On-Site Audits, the Customer and/or the Auditor may be required to execute a separate confidentiality agreement with Semperis, and Semperis may object in writing to such Auditor, if in Semperis' reasonable opinion, the Auditor is not suitably qualified, is a competitor of Semperis or is in a conflict of interests with Semperis. Any such objection by Semperis will require Customer to either appoint another Auditor or conduct the On-Site Audit itself.

9. Security Incident Response.

9.1. If Semperis becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer's Personal Data ("Security Incident"), Semperis shall notify Customer without undue delay, and in any case, where feasible, notify Customer within seventy-two (72) hours after becoming aware. Semperis shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

9.2. Unless legally prohibited to do so, Semperis shall provide Customer timely information about the Security Incident, including, but not limited to, the nature and consequences of the Security Incident, the measures

taken and/or proposed by Semperis to mitigate or contain the Security Incident, the status of Semperis' investigation, and a contact point from which additional information may be obtained. Notwithstanding the foregoing, Customer acknowledges that because Semperis personnel may not have visibility to the content of Customer's Personal Data, it is unlikely Semperis can provide information as to the particular nature of the Customer's Personal Data. Communications by or on behalf of Semperis with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Semperis of any fault or liability with respect to the Security Incident.

- 9.3. Customer will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Security Incident which directly or indirectly identifies Semperis (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Semperis' prior written approval, unless, and solely to the extent that, Customer is compelled to do so pursuant to applicable Data Protection Laws. In the latter case, unless prohibited by law, Customer shall provide Semperis with reasonable prior written notice, to provide Semperis with the opportunity to object to such disclosure and in any case, Customer will limit the disclosure to the minimum scope required.

10. Cooperation.

- 10.1. Semperis shall, to the extent legally permitted, promptly notify Customer or refer Data Subject to Customer, if Semperis receives a request from a Data Subject to exercise their rights (to the extent available to them under applicable law) of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, its right not to be subject to an automated individual decision making, or to opt-out of the sale of Personal Data ("Data Subject Request"). Taking into account the nature of the Processing, Semperis shall assist Customer by appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfilment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Laws. Semperis may refer Data Subject Requests received, and the Data Subjects making them, directly to the Customer for its treatment of such requests.
- 10.2. If Semperis receives a demand to retain, disclose, or otherwise Process Customer's Personal Data from law enforcement or any other government and/or public authority ("Third-Party Demand"), then Semperis shall attempt to redirect the Third-Party Demand to Customer. Customer agrees that Semperis can provide information to such third-party to the extent reasonably necessary to redirect the Third-Party Demand to Customer. If Semperis cannot redirect the Third-Party Demand to Customer, then Semperis shall, to the extent legally permitted to do so, provide Customer reasonable notice of the Third-Party Demand as promptly as feasible under the circumstances to allow Customer to seek a protective order or other appropriate remedy.

Annex A

1. The following capitalized terms used in this Annex A but not defined in the DPA or in the Agreement have the meaning ascribed to them in the CCPA: "Business", "Consumer", "Collect", "Personal Information", "Sell", "Share", "Business Purpose", and "Service Provider".
2. The Customer is disclosing the Personal Information to Semperis only for one or more of the following limited and specified Business Purpose: (A) operating the Product in the software-as-a- service deployment model and which involves Processing Personal Data in the course of data hosting; (B) providing technical support for the Product; (C) providing professional services which involves Processing Personal Data in the course of performing the services.
3. Semperis commits to refrain from Selling or Sharing any Personal Information. Semperis is prohibited from retaining, using, or disclosing the Personal Information that it Collects pursuant to the Agreement for any commercial purpose other than the foregoing Business Purposes, unless expressly permitted by the CCPA. Additionally, Semperis is prohibited from retaining, using, or disclosing the Personal Information that it Collects pursuant to the Agreement outside the direct business relationship between Customer and Semperis, unless expressly permitted by the CCPA.
4. Semperis shall comply with all applicable sections of the CCPA and shall provide, with respect to Personal Information it Collects pursuant to the Agreement, the same level of privacy protection as required of Businesses by the CCPA as specified in Sections 6 and 7 below.

- 5.** Semperis grants Customer the right to take reasonable and appropriate steps to ensure that Semperis uses the Personal Information it Collects pursuant to this Agreement in a manner consistent with Semperis' obligations under the CCPA. If required by Semperis' obligations under the CCRA, Semperis shall grant Customer the right, upon notice, to take reasonable and appropriate steps to stop and remediate Semperis' unauthorized use of Personal Information.
- 6.** Semperis must promptly notify Customer once it makes a determination that it can no longer meet its obligations under the CCPA.
- 7.** Semperis shall cooperate with the Customer in responding to and complying with Consumers' requests made pursuant to the CCPA.
- 8.** Semperis shall implement reasonable security procedures and practices appropriate to the nature of the Personal Information to protect it from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Cal. Civ. Code §1798.81.5. Semperis shall perform regular internal or third-party assessments, audits, or other technical and operational testing of its security procedures and practices at least once every 12 months.
- 9.** Semperis shall take all steps reasonably necessary to ensure that the individuals who may have access to Personal Information (i) are informed of the confidential nature of Personal Information; and (ii) are subject to confidentiality undertakings or appropriate statutory obligations of confidentiality.