This Data Processing Agreement ("**DPA**") is entered into by Alicent, Oy. ("**Alicent**") and the Alicent customer identified in the Agreement ("**Customer**") (each a "**Party**"; collectively the "**Parties**") and is incorporated by reference into the applicable subscription agreement governing Customer's use of Alicent's Platform (the "Agreement") between the Parties and takes precedence over the Agreement to the extent of any conflict. All capitalized terms used in this DPA but not defined will have the meaning set forth in the Agreement or under Data Protection Laws. Any prior data protection agreement that may already exist between the Parties is superseded and replaced by this DPA on the date this DPA has been fully executed by the Parties.

1. Definitions.

- **(a)** "**Data Protection Laws**" means all applicable laws, regulations, and other legal or regulatory requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of personal data, including without limitation, to the extent applicable, the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"); the United Kingdom Data Protection Act of 2018; the Swiss Federal Act on Data Protection ("**FADP**"); and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended and including its regulations ("**CCPA**"), and other applicable U.S. state and federal laws. For the avoidance of doubt, if Alicent's Processing activities involving Personal Data are not within the scope of a Data Protection Law, such law is not applicable for purposes of this DPA.
- **(b)** "**Data Privacy Frameworks**" means the EU-U.S Data Privacy Framework ("EU-U.S. DPF"), the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF"), and the UK Extension to the EU-U.S. DPF ("UK Extension") as administered by the U.S. Department of Commerce.
- **(c)** "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates, and is deemed to also include a "consumer" as defined under Data Protection Laws.
- **(d)** "**EU SCCs**" means the Standard Contractual Clauses issued pursuant 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, available at https://data.europa.eu/eli/dec_impl/2021/914/oj and completed as set forth herein.
- **(e)** "**Personal Data**" includes "personal data," "personal information," "personally identifiable information," and analogous terms, as defined by applicable Data Protection Laws, that Alicent Processes to provide the Platform under the Agreement.
- **(f)** "**Process,**" "**Processing**," "**Processed**," etc., mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- **(g)** "**Security Incident**" means any confirmed breach of security that results in the accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

- **(h)** "**Platform**" means Alicent's generative AI, software as a service platform provided by Alicent to Customer pursuant to the Agreement.
- **(i)** "**Subprocessor**" means any third party that Alicent engages to Process Personal Data to provide the Platform.
- **(j)** "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office, located at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf and completed as set forth herein.
- (**k**) The terms "**Business**," "**Controller**," "**Processor**," and "**Service Provider**" are defined as in Data Protection Laws. "Controller" is deemed to also refer to "Business," and "Processor" is deemed to also refer to "Service Provider."

2. Roles of the Parties; Scope and Purposes of Processing.

- **(a) Roles of the Parties**. To the extent that Customer is the Controller of Personal Data, Alicent is its Processor. To the extent that Customer is a Processor of Personal Data, Alicent is its Subprocessor.
- **(b) Scope and Purposes of Processing.** This DPA applies to all Personal Data that Alicent Processes to provide the Platform to Customer. Alicent will Process Personal Data (i) in compliance with Data Protection Laws; (ii) on Customer's behalf and in accordance with Customer's instructions as set forth in this DPA and the Agreement, and as otherwise provided by the Customer in writing; and (iii) to provide the Platform to Customer under the Agreement for the business purposes set forth in the Agreement and as set forth in this DPA, unless other Processing activities are required otherwise to comply with Data Protection Laws (in which case, Alicent shall provide prior notice to Customer of such legal requirement, unless such law prohibits this disclosure).
- **(c) Customer Rights**. Customer retains the right to take reasonable and appropriate steps to (i) ensure that Alicent Processes Personal Data in a manner consistent with Data Protection Laws, and (ii) upon notice, stop and remediate unauthorized Processing of Personal Data, including any use of Personal Data not expressly authorized in this DPA.
- **(d) Customer Obligations.** Where Customer is a Controller, Customer is responsible for providing any notices, obtaining any consents or authorizations, and otherwise satisfying its own compliance obligations with respect to the Processing of Personal Data under this DPA. Where Customer is a Processor, Customer represents to Alicent that its provision of Personal Data to Alicent is in compliance with Data Protection Laws and Customer's contractual obligations. Customer will not instruct Alicent to Process Personal Data in a violation of Data Protection Laws or any third party's legal, contractual, or other rights. Customer in its sole discretion determines the categories and types of Personal Data that it provides to Alicent through the Platform. Customer is responsible for secure and responsible use of the Platform and for determining that the Platform ensure a level of security appropriate to the risk in respect of Personal Data and agrees that the security and compliance measures set forth in the Agreement and this DPA

are deemed sufficient.

3. Personal Data Processing Requirements.

- **(a) Restrictions on Processing**. Alicent will:
  - **(i)** not retain, use, or disclose Personal Data outside of the direct business relationship between Customer and Alicent, or for any purpose (including any commercial purpose) not set forth in this DPA or the Agreement;
  - **(ii)** not "sell" or "share" any Personal Data, or use Personal Data for purposes of "targeted advertising," as such terms are defined in Data Protection Laws; and
  - **(iii)** comply with any applicable restrictions under the CCPA on combining Personal Data with personal data that Alicent receives from, or on behalf of, another person or persons, or that Alicent collects from any interaction between it and any individual.
- (b) Confidentiality. Alicent will ensure that the persons Processing the Personal Data have are bound by obligations of confidentiality no less protective than those set forth in the Agreement or are under an appropriate statutory obligation of confidentiality.
- (c) **Assistance.** Alicent will provide Customer with reasonable assistance:
  - **(i)** by implementing appropriate technical and organizational measures for the fulfilment of Customer's obligation to respond to requests for exercising Data Subjects' rights as set forth in Data Protection Laws, taking into account the nature of the Processing; and
  - **(ii)** in performing any required data protection impact assessment of Processing or proposed Processing of Personal Data, and in consulting with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including any applicable obligation upon Alicent to consult with a regulatory authority in relation to Alicent's Processing or proposed Processing of Personal Data. (d) Notice Regarding Compliance and Instructions. Alicent will promptly notify Customer if Alicent determines that it can no longer meet its obligations under Data Protection Laws or if it believes that Customer's instructions violate Data Protection Laws, and Alicent is not deemed to be in breach of this DPA if it declines to Process Personal Data in a way that Alicent reasonably and in good faith believes would cause Alicent to violate Data Protection Laws.

4. Data Security.

Alicent will use appropriate administrative, technical, physical, and organizational measures to protect Personal Data as set forth in Exhibit B. Alicent will provide the level of protection for Personal Data that is required under Data Protection Laws. Such measures will take 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, so as to ensure a level of security appropriate to the risk.

5. Security Incident.

- **(a) Notice**. Alicent will notify Customer of any Security Incident without undue delay or within the time period required under Data Protection Laws. To the extent available, this notification will include Alicent's then-current assessment of the following: (i) the nature of the Security Incident, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (ii) the likely consequences of the Security Incident; and (iii) measures taken or proposed to be taken by Alicent to address the Security Incident, including, where applicable, measures to mitigate its possible adverse effects. Alicent will provide timely and periodic updates to Customer as additional information regarding the Security Incident becomes available. Customer acknowledges that any updates may be based on incomplete information.

- **(b) Responsibilities of the Parties.** Alicent will comply with the Security Incident-related obligations applicable to it under Data Protection Laws and will assist Customer in Customer's compliance with its Security Incident-related obligations. Alicent will not assess the contents of Customer Data for the purpose of determining if such data is subject to any requirements under Data Protection Laws. Nothing in this DPA or in the EU SCCs will be construed to require Alicent to violate, or delay compliance with, any legal obligation it may have with respect to a Security Incident or other security incidents generally.

6. Subprocessors.

- **(a) Authorization to Engage Subprocessors.** Customer agrees that Alicent may engage Subprocessors to Process the Personal Data on Alicent behalf to provide the Platform. A list of Alicent's Subprocessors is available at alicent.com/legal/subprocessors/. Alicent will impose contractual obligations on any Subprocessor it appoints requiring it to protect Personal Data to standards that are no less protective than those set forth under this DPA. Alicent shall remain fully liable to Customer for the performance of the Subprocessor's data protection obligations. The subprocessor agreements to be provided under Clause 9 of the EU SCCs may have all commercial information, or provisions unrelated to the Standard Contractual Clauses, redacted prior to sharing with Customer, and Customer agrees that such copies will be provided only upon Customer's written request, no more than once annually.

- **(b) Subprocessor Notice and Objections.** If Customer subscribes to receive updates available on Alicent's Subprocessor page, Customer will be automatically notified of new Subprocessors before Alicent authorizes such Subprocessor to process Customer Personal Data (or in the case of an emergency, as soon as reasonably practicable). Customer has fourteen (14) calendar days from such notice to make an objection on reasonable grounds relating to the protection of the Personal Data by notifying Alicent.

at privacy@alicent.com. In the event Customer objects to a new Subprocessor, Alicent will use commercially reasonable efforts to make available to Customer a change in the Platform or Customer's configuration or use of the Platform to avoid processing of Customer Personal Data by the objected-to new Subprocessor. If Alicent is unable to make available such change within a reasonable period of time, which will not exceed thirty (30) days, either Party may upon written notice terminate without penalty the applicable Order Form(s) or the Agreement.

7. Data Transfers.

- **(a) Authorization to Transfer Personal Data.** Customer authorizes Alicent and its Subprocessors to make international transfers of Personal Data in accordance with this DPA and Data Protection Laws.

- **(b) Order of Precedence.** The Parties acknowledge that Data Protection Laws may require the Parties to implement certain safeguards (a "**Transfer Mechanism**") for Customer to transfer Personal Data to Alicent In the event a transfer of Personal Data is covered by more than one Transfer Mechanism, the transfer will be subject to a single Transfer Mechanism, in accordance with the following order of precedence: (i) the Data Privacy Frameworks; (ii) to the extent that the Data Privacy Frameworks do not apply to a given transfer or are invalidated, the EU SCCs and/or UK Addendum as set forth in Sections 7(d)-(f), as applicable; and (iii) if neither of the preceding is applicable, the Parties will cooperate in good faith to enter into an alternative Transfer Mechanism to the extent required by Data Protection Laws.

- **(c) Data Privacy Frameworks.** To the extent Alicent processes Personal Data originating from the EEA, United Kingdom, or Switzerland and Alicent is self-certified under the Data Privacy Frameworks, Alicent will adhere to the Data Privacy Principles with respect to Personal Data transferred to Alicent as applicable.

- **(d) EU SCCs.** To the extent legally required, by entering into this DPA, Customer and Alicent are deemed to have signed the EU SCCs, which form part of this DPA and (except as described in Sections 7(e) and (f) below) are deemed completed as follows:

  (i) Module 2 of the EU SCCs applies to transfers of Personal Data from Customer (as a Controller) to Alicent (as a Processor), and Module 3 of the EU SCCs applies to transfers of Personal Data from Customer (as a Processor) to Alicent. (as a Subprocessor);
  (ii) Clause 7 (the optional docking clause) is not included;
  (iii) Clause 9 (Use of sub-processors): Option 2 (General written authorization) will apply and the time period for prior notice of Subprocessor changes is set forth in Section 6 of this DPA.;
  (iv) Clause 11 (Redress): The optional language will not apply;
  (v) Clause 17 (Governing law): The Parties choose Option 1 (the law of an EU Member State that allows for third-Party beneficiary rights) and select the law of Ireland;
  (vi) Clause 18 (Choice of forum and jurisdiction): The Parties select the courts of Ireland;

(vii) Annexes I (List of Parties) and II (Technical and organizational measures) are completed as set forth in Exhibits A and B of this DPA, respectively; and

(viii) Annex III (List of subprocessors) is not applicable because the Parties have chosen General Authorization under Clause 9.

- **(e) UK Addendum.** To the extent legally required, by entering into this DPA, the Parties are deemed to be signing the UK Addendum, which forms part of this DPA and takes precedence over the rest of this DPA as set forth in the UK Addendum. The Tables within the UK Addendum are deemed completed as follows:

  (i) Table 1: The Parties' details shall be the Parties to the extent any of them is involved in such transfer, and the Key Contact shall be the contacts set forth in the Agreement.

  (ii) Table 2: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the Parties and completed in Section 7(d) of this DPA.

  (iii) Table 3: Annexes I and II are set forth in Exhibits A and B below, respectively. Annex III is inapplicable.

  (iv) Table 4: Either Party may end this DPA as set out in Section 19 of the UK Addendum.

- **(f) Transfers of Swiss Personal Data.** For transfers of Personal Data that are subject to the FADP, the EU SCCs form part of this DPA as set forth in Section 7(d) of this DPA, but with the following differences to the extent required by the FADP: (i) references to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR; (ii) the term "member state" in EU SCCs shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs; and (iii) the relevant supervisory authority is the Swiss Federal Data Protection and Information Commissioner (for transfers subject to the FADP and not the GDPR), or both such Commissioner and the supervisory authority identified in the EU SCCs (where the FADP and GDPR apply, respectively).

8. Audits.

- **(a) Standard Audit Process.** Alicent will make available to Customer documentation, data, certifications, reports, and records ("**Records**") relating to Alicent's Processing of Personal Data to demonstrate compliance with this DPA (an "**Audit**") provided the Agreement remains in effect and such audit is at Customer's sole expense. Customer may request an Audit upon fourteen (14) days' prior written notice to Alicent, no more than once annually, except, in the event of a Security Incident occurring on Alicent's systems, in which case Customer may request an Audit within a reasonable period of time following such Security Incident.
- **(b) Written Requests and Inspections.** If Customer has a reasonable objection that the Records provided are not sufficient to demonstrate Alicent compliance with this DPA, Customer may, as necessary: (i) request additional information from Alicent in writing, and Alicent will respond to such written requests within a reasonable period of time ("**Written Requests**"); and (ii) only where Alicent's responses to such Written Requests do not provide the

necessary level of information required by Customer, request access to Alicent's premises, systems and staff, upon twenty one (21) days prior written notice to Alicent (an "**Inspection**") subject to the parties having mutually agreed upon (a) the scope, timing, and duration of the Inspection, (b) the use of an auditor to conduct the Inspection, (c) the Inspection being carried out only during Alicent's regular business hours, with minimal disruption to Alicent's business operations, and (d) all costs associated with the Inspection being borne by Customer (including Alicent, time in connection with facilitating the Inspection, charged at Alicent then-current rates). Inspections will be permitted no more than once annually, except in the event of a Security Incident.

9. Return or Destruction of Personal Data.

Except to the extent required otherwise by Data Protection Laws, Alicent will, at the choice of Customer and upon Customer's written request return to Customer and/or securely destroy all Personal Data, unless Data Protection Laws require Alicent to retain Personal Data.

10. Survival; Amendments.

The provisions of this DPA survive the termination or expiration of the Agreement for so long as Alicent or its Subprocessors Process Personal Data. Alicent may amend this DPA in order to comply with Data Protection Laws and will notify Customer of such changes. By continuing to use the Platform after the DPA has been updated, Customer is deemed to have agreed to the updated DPA.

Exhibit A

ANNEX I TO THE EU SCCS

A. LIST OF PARTIES

Data exporter(s):

- Name: Customer, as identified in the Agreement.
- Address: As provided in the Agreement.
- Contact person's name, position, and contact details: As provided in the Agreement.
- Activities relevant to the data transferred under these Clauses: The data exporter receives access to the data importer's Platform pursuant to their underlying Agreement.
- Signature and date: The Parties agree that execution of the Agreement shall constitute execution of these EU SCCs by both parties.

- Role: Controller or Processor, as relevant.

Data importer(s):

- Name: Alicent, as identified in the Agreement.
- Address: As provided in the Agreement. Contact person's name, position, and contact details: As provided in the Agreement.
- Activities relevant to the data transferred under these Clauses: The data importer provides the Platform to the data exporter pursuant to their underlying Agreement.
- Signature and date: The Parties agree that execution of the Agreement shall constitute execution of these EU SCCs by both parties.
- Role: Processor or Subprocessor, as applicable.

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred: The categories of data subjects whose personal data is transferred are determined solely by the data exporter. In the normal course of the data importer's provision of the Platform, the categories of data subjects might include (but are not limited to): the data exporter's personnel, customers, service providers, business partners, affiliates and other end users.

Categories of personal data transferred: The categories of personal data transferred are determined solely by the data exporter. In the normal course of the data importer's provision of the Platform, the categories of personal data transferred might include (but are not limited to) any Personal Data submitted by Customer's data subjects in connection with their use of the Platform.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: At its sole discretion, the data exporter determines all categories and types of personal data it may submit and transfer to the data importer as part of its provision of the Platform. If the data exporter chooses to transmit sensitive data through the Platform or permits its end users to, the data exporter is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting the data exporter's end users to transmit or process, any sensitive data through the Platform.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous for the duration of the Agreement.

Nature of the processing: The data importer's Processing activities shall be limited to those discussed in the Agreement and the DPA.

Purpose(s) of the data transfer and further processing: The purpose of the transfer to and further Processing of Personal Data by the data importer is for the

data importer to provide the Platform to the data exporter as set forth in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Personal Data will be retained for the period of time necessary for the data importer to provide the Platform to the data exporter under the Agreement and/or in accordance with applicable legal requirements.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing: Same as above to the extent that Personal Data is provided to Subprocessors for purposes of providing the Platform.

C. COMPETENT SUPERVISORY AUTHORITY

To the extent legally permitted, the competent supervisory authority is the Irish Data Protection Commission.

Exhibit B

DATA SECURITY MEASURES

Alicent will implement and maintain the following administrative, technical, physical, and organizational security measures for the Processing of Personal Data:

1. **Information Security Policies and Standards.** Alicent will maintain written information security policies, standards and procedures addressing administrative, technical, and physical security controls and procedures. These policies, standards, and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store Personal Data.

2. **Physical Security.** Alicent will maintain commercially reasonable security systems at all Alicent sites at which an information system that uses or stores Personal Data is located ("Processing Locations") that include reasonably restricting access to such Processing Locations, and implementing measures to detect, prevent, and respond to intrusions.

3. **Organizational Security.** Alicent will maintain information security policies and procedures addressing acceptable data use standards, data classification, and incident response protocols.

4. **Network Security.** Alicent maintains commercially reasonable information security policies and procedures addressing network security.

5. **Access Control.** Access to Customer Data is restricted to authorized Alicent personnel who are required to access Customer Data to perform functions as part of the delivery of the Platform. Access is granted based on the principle of least privilege and access granted is commensurate with job function. Alicent agrees that: (a) only authorized Alicent staff can grant, modify, or revoke access to an information system that Processes Personal Data; and (b) it will implement commercially reasonable physical and technical safeguards to create and protect passwords.

6. **Virus and Malware Controls.** Alicent protects Personal Data from malicious code and will install and maintain anti-virus and malware protection software on any system that handles Personal Data.

7. **Personnel.** Alicent has implemented and maintains a security awareness program to train employees about their security obligations and requires that employees follow established security policies and procedures. Alicent also imposes contractual obligations on any Subprocessor Alicent appoints requiring it to protect Personal Data to standards which are no less protective than those set forth under this DPA.

8. **Business Continuity.** Alicent implements disaster recovery and business resumption plans that are kept up to date and revised on a regular basis. Alicent also adjusts its information security program in light of new laws and circumstances, including as Alicent business and Processing change.

alicent.com/legal/subprocessors/.

Name	Purpose	Location
Microsoft Azure	Generative AI Service Provider	EU
Salesforce Heroku	Cloud Service Provider	EU
HUBSPOT	Customer Support	EU