Alicent Data Processing Agreement (DPA)

This Data Processing Agreement ("DPA") is entered into by and between **Alicent Oy** (Business ID 3421735-5), P.O. Box 1002, 00101 Helsinki, Finland ("Alicent") and the **customer identified in the Agreement** ("Customer") (each a "Party" and together the "Parties").

This DPA 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. Any prior data protection agreement between the Parties is superseded and replaced by this DPA as of the effective date of the Agreement (or, if executed later, the effective date of this DPA).

Data protection contact: privacy@alicent.com.

1. Definitions

- **"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, to the extent applicable, the General Data Protection Regulation, Regulation (EU) 2016/679 ("GDPR"); the United Kingdom Data Protection Act 2018 and UK GDPR; the Swiss Federal Act on Data Protection ("FADP"); 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.
- **"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"), each as administered by the U.S. Department of Commerce.
- **"Data Subject" means** an identified or identifiable natural person to whom Personal Data relates, and, where applicable under Data Protection Laws, includes a "consumer."
- **"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 GDPR, available at https://data.europa.eu/eli/dec_impl/2021/914/oj, as completed in Section 7(d) and the Exhibits.
- **"Personal Data" means** "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.
- **"Process / Processing" means** 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, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- **"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.
- **"Platform" means** Alicent's generative AI, software-as-a-service platform provided to Customer pursuant to the Agreement.
- **"Subprocessor" means** any third party that Alicent engages to Process Personal Data in order to provide the Platform.
- **"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, as completed in Section 7(e).
- **"Business / Controller / Processor / Service Provider" means** have the meanings set forth in the applicable Data Protection Laws. "Controller" is deemed to also refer to "Business," and "Processor" is deemed to also refer to "Service Provider," as applicable.

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

2.1 Roles of the Parties.

To the extent that Customer is a Controller of Personal Data, Alicent acts as Customer's Processor. To the extent that Customer is a Processor of Personal Data, Alicent acts as Customer's Subprocessor.

2.2 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 documented instructions as set forth in this DPA and the Agreement, and as otherwise provided by Customer in writing; and (iii) to provide, maintain, and secure the Platform and related support and professional services under the Agreement for the business purposes described therein. If Processing is required by applicable law, Alicent will (unless legally prohibited) inform Customer of that legal requirement in advance.

2.3 Customer Rights.

Customer may 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.

2.4 Customer Obligations.

Where Customer is a Controller, Customer is responsible for providing required notices, obtaining consents or other lawful bases, and otherwise complying with its obligations under Data Protection Laws for the Personal Data it provides to Alicent. Where Customer is a Processor, Customer represents that its provision of Personal Data to Alicent is authorized and complies with Data Protection Laws and its agreements with the relevant Controller. Customer will not instruct Alicent to Process Personal Data in violation of Data Protection Laws or any third party rights.

3. Personal Data Processing Requirements

3.1 Restrictions on Processing.

1. Alicent will 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.
2. Alicent will not "sell" or "share" any Personal Data, and will not use Personal Data for "targeted advertising," as such terms are defined in Data Protection Laws.
3. Alicent will comply with applicable restrictions under the CCPA on combining Personal Data with personal data Alicent receives from, or on behalf of, another person or persons, or that Alicent collects from any interaction between it and any individual.

3.2 Confidentiality.

Alicent will ensure that persons authorized to Process Personal Data 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.

3.3 Assistance.

- **Data Subject requests.** Taking into account the nature of the Processing, Alicent will implement appropriate technical and organizational measures and provide reasonable assistance to enable Customer to respond to requests for exercising Data Subjects' rights under Data Protection Laws.
- **DPIAs and consultations.** Alicent will provide reasonable assistance to Customer in connection with data protection impact assessments and prior consultations with supervisory authorities, to the extent required under Data Protection Laws and to the extent the relevant information is available to Alicent.

3.4 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 Alicent reasonably believes that Customer's instructions violate Data Protection Laws. Alicent is not in breach of this DPA if it declines to Process Personal Data in a manner that Alicent reasonably and in good faith believes would cause Alicent to violate Data Protection Laws.

3.5 Use of Customer Data; No Cross-Customer Training.

Unless expressly agreed otherwise in the Agreement, Alicent will not use Customer Personal Data to train foundation models or to develop or improve Alicent's general-purpose models for use outside of Customer's environment. Customer inputs, conversations, configurations, and usage data may be used to provide, maintain, and improve the Platform for Customer within Customer's own environment (for example, to enhance accuracy, personalization, or memory functions in Customer's workspace), and for security, abuse prevention, and service reliability.

4. Data Security

Alicent will implement and maintain appropriate administrative, technical, physical, and organizational measures to protect Personal Data as set forth in Exhibit B. 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, to ensure a level of security appropriate to the risk.

5. Security Incident

5.1 Notice.

Alicent will notify Customer of any Security Incident without undue delay and, where feasible, within seventy-two (72) hours after becoming aware of the Security Incident, unless a shorter period is required by applicable Data Protection Laws. To the extent available, such notice will include Alicent's then-current assessment of: (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; and (iii) measures taken or proposed to address the Security Incident, including, where applicable, measures to mitigate possible adverse effects. Alicent will provide timely updates as additional information becomes available.

5.2 Responsibilities of the Parties.

Alicent will comply with Security Incident obligations applicable to it under Data Protection Laws and will assist Customer in Customer's compliance with Security Incident-related obligations. Alicent is not required to assess the contents of Customer Data to determine whether Customer Data is subject to any requirements under Data Protection Laws. Nothing in this DPA or the EU SCCs requires 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

6.1 Authorization to Engage Subprocessors.

Customer authorizes Alicent to engage Subprocessors to Process Personal Data on Alicent's behalf to provide the Platform. A current list of Alicent's Subprocessors is available at alicent.com/legal/subprocessors/ (or successor URL). Alicent will impose contractual obligations on any Subprocessor it appoints requiring it to protect Personal Data to standards no less protective than those set forth in this DPA. Alicent remains fully liable to Customer for the performance of its Subprocessors' data protection obligations.

6.2 Subprocessor Notice and Objections.

If Customer subscribes to receive updates on Alicent's Subprocessor page, Customer will be 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 object on reasonable grounds relating to the protection of Personal Data by notifying Alicent at privacy@alicent.com. If Customer objects, Alicent will use commercially reasonable efforts to make available a change in the Platform, configuration, or Customer's use of the Platform to avoid Processing by the objected-to Subprocessor. If Alicent cannot provide such change within thirty (30) days, either Party may terminate the affected Order Form(s) without penalty upon written notice.

7. Data Transfers

7.1 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.

7.2 Order of Precedence.

If Data Protection Laws require the Parties to implement a transfer safeguard or mechanism ("Transfer Mechanism") for transfers of Personal Data to Alicent, and a transfer is covered by more than one Transfer Mechanism, the transfer will be subject to a single Transfer Mechanism in the following order of precedence: (i) the Data Privacy Frameworks (if applicable); (ii) the EU SCCs and/or the UK Addendum as set forth below; and (iii) if neither of the foregoing applies, the Parties will cooperate in good faith to implement an alternative Transfer Mechanism to the extent required by Data Protection Laws.

7.3 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 applicable Data Privacy Principles with respect to such Personal Data.

7.4 EU SCCs.

To the extent legally required, by entering into this DPA the Parties are deemed to have executed the EU SCCs, which form part of this DPA and are deemed completed as follows:

- **Modules:** Module 2 applies to transfers from Customer (Controller) to Alicent (Processor); Module 3 applies to transfers from Customer (Processor) to Alicent (Subprocessor).
- **Docking clause:** Clause 7 (optional docking clause) is not included.
- **Subprocessors:** Clause 9: Option 2 (general written authorization) applies; prior notice period is set forth in Section 6.2.
- **Redress:** Clause 11 (optional language) does not apply.
- **Governing law:** Clause 17: Option 1 applies and the Parties select the law of Ireland.
- **Forum:** Clause 18: the courts of Ireland.
- **Annexes:** Annexes I and II are completed as set forth in Exhibits A and B of this DPA; Annex III is not applicable because general authorization is used under Clause 9.

7.5 UK Addendum.

To the extent legally required, by entering into this DPA the Parties are deemed to execute the UK Addendum, which forms part of this DPA and takes precedence as set out in the UK Addendum. The Tables are completed as follows:

- **Table 1:** Parties' details are the Parties to the Agreement, and the Key Contact is as set forth in the Agreement.
- **Table 2:** The Approved EU SCCs are the EU SCCs as completed in Section 7.4.
- **Table 3:** Annexes I and II are set forth in Exhibits A and B; Annex III is inapplicable.
- **Table 4:** Either Party may end this DPA as set out in Section 19 of the UK Addendum.

7.6 Transfers of Swiss Personal Data.

For transfers of Personal Data subject to the FADP, the EU SCCs apply as set forth in Section 7.4, with the following modifications to the extent required: (i) references to the GDPR are understood as references to the FADP where transfers are subject exclusively to the FADP; (ii) "Member State" is not interpreted to exclude Swiss Data Subjects from suing in Switzerland as permitted under Clause 18(c); and (iii) the competent 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 both apply.

8. Audits

8.1 Standard Audit Process.

Alicent will make available to Customer, upon request, documentation, certifications, reports, and records reasonably necessary to demonstrate compliance with this DPA ("Records"), provided the Agreement remains in effect. Customer may request an audit of such Records no more than once per calendar year upon fourteen (14) days' prior written notice, except that Customer may request an additional audit following a Security Incident on Alicent's systems within a reasonable time after such Security Incident. Any audit is at Customer's expense.

8.2 Written Requests and Inspections.

If Customer has reasonable grounds to believe the Records are insufficient to demonstrate compliance, Customer may submit written requests for additional information, and Alicent will respond within a reasonable time. Only if the written responses remain insufficient, Customer may request an on-site inspection upon twenty-one (21) days' prior written notice, subject to the Parties agreeing in advance on scope, timing, duration, and an independent auditor; inspection during Alicent's business hours with minimal disruption; and Customer bearing all costs (including Alicent's reasonable time at Alicent's then-current rates). On-site inspections will occur no more than once per calendar year, except following a Security Incident.

9. Return or Destruction of Personal Data

Except as required otherwise by Data Protection Laws, Alicent will, at Customer's choice and upon Customer's written request, return to Customer and/or securely delete or destroy Personal Data, within a reasonable time (and, where feasible, within thirty (30) days), unless applicable law requires retention.

10. Survival; Amendments

This DPA survives termination or expiration of the Agreement for as long as Alicent or its Subprocessors Process Personal Data. Alicent may update this DPA to comply with changes in Data Protection Laws and will provide notice of material changes. Continued use of the Platform after an updated DPA becomes effective constitutes Customer's acceptance of 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:** As provided in the Agreement.
- **Activities relevant to the transfer:** Customer receives access to the Platform pursuant to the Agreement.
- **Signature and date:** Execution of the Agreement constitutes execution of the EU SCCs by Customer.
- **Role:** Controller or Processor, as applicable.

Data importer(s):

- **Name:** Alicent Oy.
- **Address:** P.O. Box 1002, 00101 Helsinki, Finland.
- **Contact person:** As provided in the Agreement (privacy matters: privacy@alicent.com).
- **Activities relevant to the transfer:** Alicent provides the Platform to Customer pursuant to the Agreement.
- **Signature and date:** Execution of the Agreement constitutes execution of the EU SCCs by Alicent.
- **Role:** Processor or Subprocessor, as applicable.

B. DESCRIPTION OF TRANSFER

- **Categories of Data Subjects:** Determined by Customer. In the ordinary course of providing the Platform, this may include Customer personnel, customers, service providers, business partners, affiliates, and other end users.
- **Categories of Personal Data:** Determined by Customer. In the ordinary course of providing the Platform, this may include Personal Data submitted by or on behalf of Customer in connection with use of the Platform.
- **Sensitive data:** Customer determines whether to submit sensitive data. If Customer submits or permits submission of sensitive data, Customer is responsible for ensuring appropriate safeguards before submission. Alicent does not require the submission of special categories of data to provide the Platform.
- **Frequency:** Continuous for the duration of the Agreement.
- **Nature of Processing:** Processing activities are limited to those necessary to provide, maintain, secure, and support the Platform as described in the Agreement and this DPA.
- **Purpose(s):** To provide the Platform and related services to Customer under the Agreement.
- **Retention:** For the period necessary to provide the Platform under the Agreement and/or as required by applicable law.
- **For transfers to (sub-)processors:** Same as above, to the extent Personal Data is provided to Subprocessors to deliver 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:

4. **Information Security Policies and Standards.** Maintain written information security policies, standards, and procedures addressing administrative, technical, and physical controls. Keep them up to date and revise when relevant system changes occur.
5. **Physical Security.** Maintain commercially reasonable security systems at Processing Locations, including access controls and measures to detect, prevent, and respond to intrusions.
6. **Organizational Security.** Maintain policies and procedures addressing acceptable use standards, data classification, and incident response.
7. **Network Security.** Maintain commercially reasonable policies and procedures addressing network security.
8. **Access Control.** Restrict access to Customer Data to authorized personnel with a need to know, based on least privilege. Only authorized staff may grant, modify, or revoke access. Implement safeguards to create and protect credentials.
9. **Virus and Malware Controls.** Protect Personal Data from malicious code and maintain appropriate anti-malware controls on systems that handle Personal Data.
10. **Personnel.** Maintain a security awareness program and require employees to follow established security policies. Impose comparable obligations on Subprocessors.
11. **Business Continuity.** Maintain disaster recovery and business resumption plans and review them regularly; adjust the security program in light of new laws and changes in Processing.

Appendix 1 – Subprocessors (as of the Effective Date)

This list is provided for convenience. The authoritative and up-to-date list is available at alicent.com/legal/subprocessors/.

Name	Purpose	Location
Microsoft Azure	Cloud hosting and managed services / AI infrastructure	EU/EEA (as configured)
Salesforce Heroku	Application hosting / platform services	EU/EEA (as configured)
Pipedrive	Customer relationship management	EU/EEA (as configured)
Amazon Web Services (AWS)	Cloud infrastructure (compute, storage, CDN, logging, backups)	EU/EEA (as configured)
Mailgun / Sinch Email	Transactional email delivery	EU (as configured)

HubSpot	Customer support / CRM (as applicable)	EU/EEA (as configured)