Alauda Data Processing Addendum

Effective Date: November 2026 **Version:** 1.3

This Data Processing Addendum ("Addendum") is by and between Customer (defined below) and Alauda Singapore Pte. Ltd. (UEN 202524557C) ("Alauda") and shall apply when Alauda is Processing Personal Data provided by Customer, or collected, generated, or otherwise Processed by Alauda on behalf of Customer, in connection with Client Information or the relevant products or services under the Alauda Enterprise Agreement (available at https://www.alauda.io/legal/enterprise-agreement) (the "Agreement"). This Addendum is incorporated into the Agreement. This Addendum applies where and only to the extent that Alauda is acting as a Processor or Subprocessor of Personal Data on behalf of Customer (who is acting as a Controller, or as a Processor on behalf of other Controllers) in the course of providing Alauda Products or Services under the Agreement, including Online Services, Subscription Services (such as the handling of support cases and related diagnostic materials), and Professional Services (such Personal Data, "Customer Personal Data"). As used in this Addendum, "Personal Data" refers to Customer Personal Data unless the context requires otherwise. For clarity, Personal Data that Alauda Processes as an independent Controller — including business-contact, account, billing, and relationship-management data — is governed by the Alauda Privacy Policy and not this Addendum. This Addendum is intended to demonstrate the parties' compliance with EU Data Protection Law, the UK GDPR and the UK Data Protection Act 2018, the Singapore Personal Data Protection Act 2012 ("PDPA"), and all other laws and regulations relating to privacy, data protection, or the Processing of Personal Data that apply to the relevant Processing under the Agreement (together "Data Protection Laws").

---

1. Definitions

Any capitalized terms not defined herein shall have the meanings given in the Agreement. For purposes of this Addendum, words and phrases in this Addendum shall, to the greatest extent possible, have the meanings given to them in the applicable Data Protection Laws. In particular:

(a) "**Customer**" means the customer entity that has executed the Agreement or "You" as such term is defined in the Agreement.

(b) "**Controller**" has the meaning given to it in the applicable Data Protection Laws, and includes a "data controller" under the GDPR and an "organisation" determining the purposes and means of processing under the PDPA.

(c) "**Data Subject**" has the meaning given to it in the applicable Data Protection Laws, and includes an "individual" under the PDPA.

(d) "**EU Data Protection Law**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation" or "GDPR"), and laws implemented by EEA member states, which contain derogations from, or exemptions or authorizations for the purposes of, the GDPR, or which are otherwise intended to supplement the GDPR or convert the GDPR into domestic law.

(e) "**EU Standard Contractual Clauses**" or "**Clauses**" means the standard contractual clauses, including Annexes I, II, and III, for the transfer of personal data to third countries pursuant to the GDPR, with optional clauses applied (except for option 1 of Clause 9(a), the optional language in Clause 11(a), and option 2 of Clause 17), as officially published by the European Commission Implementing Decision 2021/914, dated 4 June 2021, and as updated or replaced by the European Commission from time to time.

(f) "**PDPA**" means the Personal Data Protection Act 2012 (No. 26 of 2012) of Singapore, as amended from time to time, and any subsidiary legislation and regulations made thereunder.

(g) "**Personal Data**" has the meaning given to it in the applicable Data Protection Laws.

(h) "**Process**" or "**Processing**" has the meaning given to it in the applicable Data Protection Laws.

(i) "**Processor**" has the meaning given to it in the applicable Data Protection Laws, and includes a "data intermediary" under the PDPA.

(j) "**Subprocessor**" means any natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of a Processor (including any affiliate of the Processor).

(k) "**UK GDPR**" means the GDPR as incorporated into the laws of England and Wales, Scotland, and Northern Ireland by the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (as amended).

(l) "**UK International Data Transfer Addendum**" or "**UK IDTA**" means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner's Office under Section 119A of the UK Data Protection Act 2018, as updated or replaced from time to time.

---

2. Scope and Roles

2.1 This Addendum applies to Alauda's Processing of Personal Data on behalf of Customer in the course of providing products or services under the Agreement.

2.2 As between the parties: (a) Customer is the Controller (or Processor acting on behalf of other Controllers) with respect to the Personal Data; and (b) Alauda is the Processor (or Subprocessor, as applicable) with respect to the Personal Data.

2.3 Customer is responsible for the lawfulness of the Processing of the Personal Data and for taking appropriate steps within Customer's control to maintain appropriate security, protection, and deletion of Personal Data. If Customer is acting as a Processor on behalf of another Controller, Customer represents and warrants that it has obtained all necessary authorizations from the relevant Controller(s) and that Customer shall serve as the single point of contact for Alauda.

2.4 Alauda will comply with all Data Protection Laws applicable to Alauda in its capacity as Processor in respect of the products and services under the Agreement. Alauda is not responsible for determining the requirements of laws or regulations applicable to Customer's business, or for determining that Alauda's products or services meet the requirements of any such laws. Customer will not use the products and services in a manner that would violate applicable Data Protection Laws.

---

3. Processing Instructions

3.1 Alauda shall only Process the Personal Data: (a) as needed to provide the products or services to Customer in accordance with the Agreement; (b) in accordance with the specific instructions that it has received from Customer, including with regard to any transfers; and (c) as needed to comply with applicable laws, in which case Alauda will inform Customer of that legal requirement before Processing unless the law prohibits such information on important grounds of public interest.

3.2 Alauda shall immediately inform Customer if, in Alauda's opinion, an instruction by Customer infringes Data Protection Laws. The Agreement, this Addendum, and Customer's use and configuration of the applicable products and services constitute Customer's complete documented instructions; additional or alternate instructions require the parties' prior written agreement, including as to any fees payable.

3.3 The types of Personal Data, the categories of Data Subjects, and other details of the Processing activities are described in Annex 1 of this Addendum.

3.4 Alauda shall undertake to implement appropriate technical and organizational measures in such a manner that its Processing of Personal Data will meet the requirements of the applicable Data Protection Laws and ensure the protection of the rights and freedoms of the Data Subjects. Alauda will Process Customer Personal Data only for the duration of the relevant products or services involving such Processing, unless otherwise instructed in writing by Customer.

---

4. Confidentiality

4.1 Alauda shall ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.2 Alauda shall ensure that access to Personal Data is limited to those personnel who need access to the Personal Data to perform Alauda's obligations under the Agreement, and that all such personnel are subject to confidentiality obligations that are no less protective than the confidentiality terms set forth in the Agreement.

---

5. Security

5.1 Alauda shall implement the technical and organizational measures set forth in Annex 2 and as set forth in the Agreement to ensure a level of security appropriate to the risks that are presented by Alauda's Processing of Personal Data, 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.

5.2 Alauda shall regularly test, assess, and evaluate the effectiveness of the technical and organizational measures for ensuring the security of the Processing.

5.3 In assessing the appropriate level of security, Alauda shall take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed.

---

6. Sub-processing

6.1 General Authorization. Customer provides general authorization to Alauda to engage and use Subprocessors to fulfil its contractual obligations to Customer under the Agreement or to provide certain services on behalf of Alauda, such as providing hosting and infrastructure services.

6.2 Subprocessor List. A list of the current applicable Subprocessors is published at https://www.alauda.io/legal/subprocessors (the "**Subprocessor List**") or is available on written request from Customer. The Subprocessor List forms Annex 3 to this Addendum.

6.3 Notification of Changes. Alauda will provide advance notice to Customer of any addition or replacement of Subprocessors by updating the Subprocessor List published at https://www.alauda.io/legal/subprocessors at least thirty (30) days before the new Subprocessor begins Processing Personal Data, or as otherwise agreed upon by the parties in writing.

6.4 Right to Object. Within thirty (30) days after Alauda's notification of the intended change, Customer may object to any new Subprocessor on the basis that such addition would cause Customer to violate applicable legal requirements. If Customer objects to Alauda's use of any new Subprocessor by giving written notice to Alauda within thirty (30) days of being informed by Alauda of the appointment of such new Subprocessor, and Alauda fails to provide a commercially reasonable alternative to avoid the Processing of Personal Data by such Subprocessor within thirty (30) days of Alauda's receipt of Customer's objection, Customer may, as its sole and exclusive remedy, terminate the services that cannot be provided by Alauda without the use of the objected-to new Subprocessor. If Customer does not object within such period, the respective Subprocessor may be commissioned to Process Personal Data.

6.5 Subprocessor Obligations. Subprocessors are required to abide by the same level of data protection and security as Alauda under this Addendum as applicable to their Processing of Personal Data. Alauda shall enter into a written agreement with each Subprocessor that imposes data protection obligations no less protective than those set out in this Addendum. Alauda will remain responsible to Customer for any acts or omissions of any Subprocessor that cause Alauda to breach any of Alauda's obligations under this Addendum.

6.6 Access Restrictions. Alauda will restrict Subprocessors' access to, and Processing of, Personal Data only to what is necessary to provide products or services to Customer in accordance with the Agreement.

6.7 Confidentiality. The identity, location, and stated processing function of each Subprocessor on the published list are not Confidential Information; any non-public security or diligence materials that Alauda provides concerning a Subprocessor are Alauda's Confidential Information under the terms of the Agreement.

---

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Alauda shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising Data Subjects' rights under applicable Data Protection Laws, including requests for access, rectification, erasure, restriction, portability, and objection.

7.2 Alauda shall promptly notify Customer if Alauda receives a request from a Data Subject in respect of Personal Data. Alauda shall not respond to such request itself unless authorized to do so by Customer or

required by applicable law, in which case Alauda shall, to the extent permitted by applicable law, inform Customer of such legal requirement before responding to the request.

---

8. Breach Notification

8.1 Alauda will promptly investigate all allegations of unauthorized access to, or use or disclosure of, Personal Data. If Alauda becomes aware of a Personal Data breach, or otherwise has reason to believe that a Personal Data breach has occurred, Alauda will notify Customer without undue delay and in any event within seventy-two (72) hours of becoming aware of the breach.

8.2 Such notification shall include, to the extent reasonably available:

(a) a description of the nature of the Personal Data breach, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the name and contact details of Alauda's contact point from whom more information can be obtained;

(c) a description of the likely consequences of the Personal Data breach; and

(d) a description of the measures taken or proposed to be taken by Alauda to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.3 Where it is not possible to provide all information at the same time, the information may be provided in phases without undue further delay.

8.4 Taking into account the nature of Processing and the information available to Alauda, Alauda shall assist Customer with Customer's compliance with its obligations regarding personal data breaches, data protection impact assessments, security of processing, and prior consultation, each as and to the extent required by applicable Data Protection Laws.

---

9. Data Transfer Mechanisms

9.1 General. Customer agrees and will ensure that it is entitled to transfer Personal Data to Alauda so that Alauda may lawfully Process the Personal Data in accordance with the Agreement and this Addendum. Alauda agrees that it will comply with applicable Data Protection Laws regarding transfers of Personal Data from Customer to Alauda.

9.2 EU/EEA Transfers. In the case of a transfer of Personal Data to a country not providing an adequate level of protection pursuant to the applicable EU Data Protection Law ("Non-Adequate Country"), the parties shall comply with the provisions set out below.

(a) By entering into this Addendum, Customer and Alauda are entering into the EU Standard Contractual Clauses, including Annexes I, II, and III, if Customer, Alauda, or both are located in a Non-Adequate Country. If the EU Standard Contractual Clauses are not required because both parties are located in a country considered adequate by the applicable Data Protection Laws, but during the Agreement the country where Customer or Alauda is located becomes a Non-Adequate Country, then the EU Standard Contractual Clauses will apply to Personal Data that is transferred to such Non-Adequate Country.

(b) The parties acknowledge that the applicable module of the EU Standard Contractual Clauses will be determined by their role as Controller and/or Processor under the circumstances of each case and are

responsible for determining the correct role undertaken in order to fulfil the appropriate obligations under the applicable module. When Customer is acting as a Controller, Module 2 (Controller-to-Processor) of the EU Standard Contractual Clauses will apply to the Personal Data transferred to any Non-Adequate Country. When Customer is acting as a Processor, Module 3 (Processor-to-Processor) of the EU Standard Contractual Clauses will apply to the Personal Data transferred to any Non-Adequate Country.

(c) With regards to Clause 13 of the EU Standard Contractual Clauses and as set forth in Annex 1, Section C below, the competent supervisory authority shall be determined in accordance with Clause 13(a), including, where the data exporter is subject to the GDPR under Article 3(2) without being established in an EU Member State, by reference to the member state in which its representative under Article 27 GDPR is established or, where no representative is required, a member state in which the Data Subjects whose Personal Data is transferred are located. With regards to Clause 17 of the EU Standard Contractual Clauses, the parties agree that the EU Standard Contractual Clauses shall be governed by the laws of the EU Member State in which the data exporter is established or, where the data exporter is not established in an EU Member State, the laws of Ireland. With regards to Clause 18(b) of the EU Standard Contractual Clauses, the parties agree that disputes shall be resolved before the courts of that same member state (or, as applicable, the courts of Ireland).

(d) With regards to the use of Subprocessors, Clause 9(a), option 2 of the EU Standard Contractual Clauses shall apply, and Alauda has Customer's general authorization for the engagement of Subprocessors as described in more detail in Section 6 of this Addendum. Alauda will enter into the EU Standard Contractual Clauses with each Subprocessor located in a Non-Adequate Country.

(e) Annex I, Annex II, and Annex III of the EU Standard Contractual Clauses shall be completed with the information set out in Annex 1, Annex 2, and Annex 3 to this Addendum (Annex III being furnished as the Subprocessor List maintained under the general written authorization in Clause 9(a), Option 2).

9.3 UK Transfers. For transfers of Personal Data that are subject to the UK GDPR:

(a) The UK International Data Transfer Addendum (UK IDTA) is hereby incorporated by reference into this Addendum. The UK IDTA shall apply to the transfer of Personal Data from the United Kingdom to any country that is not recognized as providing an adequate level of data protection under UK data protection law.

(b) For the purposes of the UK IDTA: (i) the applicable EU Standard Contractual Clauses shall be those referenced in Section 9.2 above; (ii) Table 1 of the UK IDTA shall be completed with the information set out in Annex 1 to this Addendum; (iii) Table 2 of the UK IDTA shall reference the EU Standard Contractual Clauses as set out in Section 9.2; (iv) Table 3 of the UK IDTA shall be completed with the information set out in Annex 1, Annex 2, and Annex 3 to this Addendum; and (v) Table 4 of the UK IDTA shall select "Importer" as the party that may end the UK IDTA.

(c) The competent supervisory authority for UK transfers is the UK Information Commissioner's Office (ICO).

9.4 Singapore Transfers. For transfers of Personal Data that are subject to the PDPA:

(a) Alauda shall comply with its obligations under the PDPA with respect to all Personal Data transferred by Customer to Alauda, including section 26 of the PDPA regarding the transfer of personal data outside Singapore; Alauda's obligations concerning notifiable data breaches under Part 6A of the PDPA are addressed in Section 8.

(b) Where Personal Data is transferred outside Singapore, Alauda shall ensure that the recipient of such Personal Data is bound by legally enforceable obligations to provide a standard of protection to the Personal Data that is comparable to the protection under the PDPA.

9.5 Swiss Transfers. For transfers of Personal Data subject to the Swiss Federal Act on Data Protection to a country not recognized as providing adequate protection, the EU Standard Contractual Clauses as implemented under Section 9.2 apply with the adaptations required under Swiss law: references to the GDPR include the Swiss Federal Act on Data Protection; the competent authority is the Swiss Federal Data Protection and Information Commissioner (FDPIC); references to EEA member states are read to include Switzerland; and Data Subjects in Switzerland may enforce their rights in Switzerland.

9.6 If Customer believes the measures set out in this Section 9 are not sufficient to satisfy the applicable Data Protection Laws with respect to such transfer of Personal Data, Customer shall notify Alauda and the parties shall work together to find an alternative.

---

10. Audit Rights

10.1 Upon Customer's written request, Alauda shall provide Customer with a confidential summary report of any relevant third-party audit certifications or reports (such as SOC 2 Type II or ISO 27001 reports, if and when available) to verify the adequacy of its security measures and other information necessary to demonstrate Alauda's compliance with this Addendum.

10.2 Only to the extent required by Data Protection Laws (and no more than once per year unless otherwise required by Data Protection Laws), Customer may request, and Alauda shall allow for and contribute to, audits, including inspections of Alauda facilities Processing Customer Personal Data, with reasonable advance written notice from Customer (not less than thirty (30) days) and at a time mutually agreed upon by the parties.

10.3 Such audits or inspections shall: (a) occur during normal business hours; (b) be conducted in a manner that causes minimal disruption to Alauda's business; (c) be conducted by Customer or another auditor mandated by Customer and approved by Alauda (such approval not to be unreasonably withheld); and (d) be at Customer's sole expense.

10.4 Customer agrees to treat the audit report, summary report, and other information described in this Section 10 as Alauda's Confidential Information under the terms of the Agreement.

10.5 Alauda shall maintain all records required by applicable Data Protection Laws, and (to the extent they are applicable to Alauda's activities for Customer) shall make them available to Customer upon its written request.

---

11. Return and Deletion of Personal Data

11.1 Upon Customer's written request, or after the end of the provision of the products or services relating to the Processing (and in any event upon the expiration or termination of the Agreement), Alauda shall, at Customer's election, either delete or return to Customer all of the Personal Data in Alauda's possession, unless retention is required by applicable laws. In such cases, Alauda will ensure that Personal Data is only Processed as necessary to comply with applicable laws. If Customer does not make an election within

thirty (30) days after the end of the relevant products or services, Alauda will delete the Personal Data, subject to the legal retention exceptions in this Section 11.1 and Section 11.3.

11.2 Alauda shall provide written confirmation of the deletion of Personal Data upon Customer's written request.

11.3 The obligation to delete or return Personal Data shall also apply to copies of Personal Data, except to the extent that applicable law requires continued storage of such Personal Data.

---

12. Term and Termination

12.1 This Addendum shall take effect upon the effective date of the Agreement (or, if later, the date on which Alauda first begins Processing Personal Data on behalf of Customer) and shall remain in effect for the duration of the Agreement.

12.2 Any provision of this Addendum that expressly or by implication should come into force or continue in force on or after the termination or expiration of the Agreement (including Sections 3, 4, 5, 6, 7, 8, 9, 10, 11, and 13) shall remain in full force and effect. This Addendum, including its Annexes, remains in effect for as long as Alauda or any Subprocessor Processes or retains Customer Personal Data.

12.3 Except as amended by this Addendum, the Agreement will remain in full force and effect. Customer agrees that this Addendum, including any claims arising from it, is subject to the terms set forth in the Agreement, including the limitations of liability.

12.4 If there is any conflict or inconsistency between the EU Standard Contractual Clauses, the UK IDTA, this Addendum, and/or the remainder of the Agreement, then the following order of precedence will apply: (a) the EU Standard Contractual Clauses or the UK IDTA (as applicable); (b) the remainder of this Addendum; and (c) the remainder of the Agreement. Nothing in this Addendum is intended to modify or contradict the applicable terms in the Data Protection Laws, the EU Standard Contractual Clauses, or the UK IDTA, or prejudice the fundamental rights or freedoms of Data Subjects under Data Protection Laws.

---

13. Third Party Requests

13.1 If any government or regulatory authority requests access to Personal Data, unless prohibited by law, Alauda will notify Customer of such request to enable Customer to take necessary actions to communicate directly with the relevant authority and respond to such request.

13.2 If Alauda is prohibited by law from notifying Customer of such request, Alauda will use reasonable efforts to challenge the prohibition on notification and will provide the minimum amount of information permissible when responding, based on a reasonable interpretation of the request.

---

14. Governing Law

14.1 This Addendum and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the laws of the Republic of Singapore, except where Section 14.2 applies.

14.2 Where Customer is established in the European Economic Area or the United Kingdom, and the Personal Data being Processed is subject to the GDPR or the UK GDPR, this Addendum shall be governed by and construed in accordance with the laws of England and Wales.

14.3 The provisions of Section 14.1 and 14.2 are without prejudice to the governing law applicable to the EU Standard Contractual Clauses or the UK IDTA as set forth in Section 9.

---

15. Contact

For privacy-related inquiries or requests related to this Addendum, Customer may contact Alauda at:

Alauda Singapore Pte. Ltd. 6 Raffles Quay, #14-02 Singapore 048580 Email: privacy@alauda.io

---

ANNEX 1: Description of Processing

A. List of Parties

1. Data Exporter(s)

Name: The data exporter is Customer.

Address: As set out in the Agreement.

Contact person's name, position, and contact details: As set out in the Agreement or as otherwise notified in writing to Alauda by Customer.

Activities relevant to the data transferred under these Clauses: As set out in the Agreement.

Signature and date: By entering into the Agreement, Customer is entering into these Clauses and deemed to have signed this Annex 1 as of the effective date of the Agreement.

Role (controller/processor): Customer is Controller or Processor or both. The role of Customer as Controller, Processor, or both is determined by the circumstances of each case and Customer is responsible for determining the correct role undertaken in order to fulfil the appropriate obligations under the applicable module.

2. Data Importer(s)

Name: The data importer is Alauda Singapore Pte. Ltd. acting as a Processor or Subprocessor, as applicable, if located in a Non-Adequate Country.

Address: 6 Raffles Quay, #14-02, Singapore 048580.

Contact person's name, position, and contact details: As set out in the Agreement, or privacy@alauda.io.

Activities relevant to the data transferred under these Clauses: As set out in the Agreement.

Signature and date: By entering into the Agreement, Alauda is entering into these Clauses in such cases where Alauda is located in a Non-Adequate Country and deemed to have signed this Annex 1 as of the effective date of the Agreement.

Role (controller/processor): Alauda as Processor (or Subprocessor, as applicable).

Note: Where a transfer is Processor-to-Controller (Module 4), the data exporter is Alauda as Processor and the data importer is Customer as Controller.

B. Description of Transfer

1. Categories of Data Subjects whose Personal Data is transferred

Data exporter may submit Personal Data to data importer, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

- Employees or contractors of data exporter
- Data exporter's users authorized by data exporter to use the services
- Employees or contact persons of data exporter's customers, business partners, and vendors

2. Categories of Personal Data transferred

Data exporter may submit Personal Data to Processor, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

- First and last name
- Employment information (such as title, position, employer)
- Contact information (such as email, phone, physical address)
- IP address, online identifier, or other identification data
- Platform usage and access log data (such as login timestamps, feature usage, cluster identifiers)
- Personal Data incidentally contained in support case content and diagnostic materials submitted by Customer (such as logs, diagnostic bundles, screenshots, or configuration excerpts, which may contain usernames, identifiers, or IP addresses)
- Personal Data incidentally contained in materials provided by Customer in connection with Professional Services engagements

3. Special or sensitive categories of Personal Data transferred

None. Customer shall not submit special categories of Personal Data (as defined in Article 9 of the GDPR) or equivalent sensitive personal data under other Data Protection Laws to Alauda unless otherwise explicitly agreed in writing. Any such written agreement must amend this Section B.3 to identify the special categories of data concerned, the purposes, and the applied restrictions and safeguards before any such Processing begins.

4. Frequency of the transfer

Personal Data is transferred in accordance with Customer's instructions and at Customer's determination, but it is generally on a continuous basis during the term of the relevant products or services involving the transfer.

5. Nature of the Processing

The Personal Data transferred may be subject to the following Processing activities: collecting, monitoring, supporting, operating, storing, hosting, backup, development, and the other services as set forth in the Agreement.

6. Purpose(s) of the data transfer and further processing

The transfer and Processing of Personal Data is made for the following purposes: to provide the products, services, and support as set forth in the Agreement.

7. Duration of Processing

The Processing of Personal Data will occur only for the duration of the relevant products or services involving such Processing, subject to the return and deletion obligations in Section 11 of the Addendum, unless otherwise instructed in writing by Customer.

8. Transfers to Subprocessors

The subject matter, nature, and duration of Processing by Subprocessors are as set forth in the above sections and as described in Annex 3.

C. Competent Supervisory Authority

The competent supervisory authority shall be determined in accordance with the applicable Data Protection Laws:

- For transfers subject to the GDPR: determined in accordance with Clause 13(a) of the EU Standard Contractual Clauses — where the data exporter is established in an EU Member State, the supervisory authority of that Member State; where the data exporter is not established in an EU Member State but is subject to the GDPR under Article 3(2) and has appointed a representative under Article 27 GDPR, the supervisory authority of the member state in which the representative is established; where no representative is required, the supervisory authority of a member state in which the Data Subjects whose Personal Data is transferred are located.
- For transfers subject to the UK GDPR: the UK Information Commissioner's Office (ICO).
- For transfers subject to the PDPA: the Personal Data Protection Commission of Singapore (PDPC).
- For transfers subject to the Swiss Federal Act on Data Protection: the Swiss Federal Data Protection and Information Commissioner (FDPIC).

D. Alauda Privacy Contact

The Alauda privacy contact can be reached at privacy@alauda.io.

ANNEX 2: Technical and Organizational Security Measures

In connection with its provision of products and services under the Agreement, Alauda agrees that it shall take all reasonably necessary steps and security precautions in accordance with commercially reasonable industry standards to minimize the risk of unauthorized access to, or compromise of, Personal Data.

Alauda will maintain and keep updated administrative, physical, and technical safeguards and procedures designed to protect the security, confidentiality, and integrity of Personal Data while under Alauda's possession, custody, or control that cover the areas below.

---

1. Encryption

- All Personal Data transmitted over public networks is encrypted using Transport Layer Security (TLS) version 1.2 or higher.
- Personal Data at rest is encrypted using AES-256 encryption or equivalent cryptographic standards.
- Encryption keys are managed in accordance with industry best practices, including regular rotation and secure storage in dedicated key management systems.

2. Access Controls

- Access to Personal Data is restricted on a need-to-know basis using Role-Based Access Control (RBAC).
- Multi-Factor Authentication (MFA) is required for all personnel accessing systems that Process Personal Data.
- Alauda maintains a password policy that establishes standards for creating and protecting strong passwords, including minimum length, complexity, and rotation requirements.
- Unique user identification and access credentials are assigned to all authorized personnel. Shared accounts are prohibited for systems that Process Personal Data.
- Access rights are reviewed at least quarterly, and promptly revoked upon personnel role change or termination.

3. Network Security

- Alauda maintains appropriate antivirus and malware protection for Alauda's network and systems.
- Network segmentation is implemented to isolate systems Processing Personal Data from other networks.
- Firewall and intrusion detection/prevention systems are deployed and monitored to protect against unauthorized network access.
- Periodic vulnerability assessments and penetration testing of Alauda's network are conducted at least annually.

4. Information Security Procedures

- Alauda maintains, updates, and monitors procedures designed to protect Alauda's information systems from loss, damage, unauthorized disclosure, or disruption of business, which includes the physical and logical protection of information systems including Personal Data that is Processed or transmitted.

5. Organization of Information Security

- Alauda maintains an information security organization to coordinate the implementation of security measures and policies. A designated information security officer or equivalent role oversees the program.

6. Asset Management

- Alauda maintains procedures to identify, control, and maintain the security of Alauda assets and Personal Data, including asset inventories, classification, and secure disposal.

7. Human Resources Security

- Alauda maintains procedures to determine whether personnel are suitable for their roles, including background checks where permitted by applicable law.
- All personnel with access to Personal Data receive appropriate security and data protection training upon onboarding and at least annually thereafter.
- Alauda personnel with access to Personal Data are subject to Alauda's ethical business conduct, confidentiality, security, and privacy policies as a condition of their engagement.

8. Physical and Environmental Security

- Alauda provides measures that protect information systems that Process Personal Data with an appropriate level of physical security and suitable environmental controls for information and information systems, as well as the supporting infrastructure.
- Controls at the entrance of facilities managed by Alauda (such as validation by human personnel or electronic access controls) limit physical access to Alauda facilities to authorized persons.
- Emergency response procedures are in place at Alauda facilities in the event of a fire, flood, or similar event.

9. Incident Response

- Alauda maintains an incident response plan and program designed to allow for investigation, response, and corrective actions for any security incident.
- The incident response plan includes procedures for notification of the data exporter in accordance with Section 8 of this Addendum.
- Post-incident reviews are conducted to identify root causes and implement preventive measures.

10. Vendor Management

- Alauda evaluates the security posture of Subprocessors and third-party service providers prior to engagement and on an ongoing basis.
- Subprocessors are contractually required to implement security measures that are no less protective than those described in this Annex 2.
- Alauda maintains a register of Subprocessors and conducts periodic reviews of Subprocessor compliance.

11. Business Continuity and IT Disaster Recovery

- Alauda maintains a business continuity and IT disaster recovery program to oversee and implement policies and procedures designed to sustain Alauda's critical business operations in the event of major operational disruptions or natural disasters.
- Backup and recovery procedures are tested at least annually.

12. Product Security

- Alauda maintains a product security program responsible for monitoring and assessing vulnerabilities and threats that may impact Alauda services.
- Security patches and updates are applied in accordance with a documented patch management policy.
- Secure development lifecycle practices, including security review and code analysis, are integrated into Alauda's software development process.

13. Continued Review

- Alauda will continue to review its information security safeguards and controls and implement additional or different measures when deemed appropriate.
- Alauda reserves the right in its sole discretion to modify and update its IT and security controls so long as such modification or update does not materially reduce the level of security afforded to the Personal Data.

ANNEX 3: List of Subprocessors

Annex 3 is the Subprocessor List published at https://www.alauda.io/legal/subprocessors, as updated from time to time in accordance with Section 6.3, and is incorporated into this Addendum by reference. A copy is available on written request from Customer. For each Subprocessor authorized by Customer under Section 6 of this Addendum, the Subprocessor List identifies its name, its location, the purpose of its Processing, and the categories of Personal Data it Processes.

ANNEX 4: Standard Contractual Clauses Reference

A. EU Standard Contractual Clauses

4.1 The EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914 of 4 June 2021) are incorporated by reference into this Addendum and apply to transfers of Personal Data as described in Sections 9.2 and 9.5 of this Addendum.

4.2 The applicable module(s) of the EU Standard Contractual Clauses are determined as follows:

- **Module 2 (Controller to Processor):** Applies where Customer is acting as a Controller and Alauda is acting as a Processor with respect to the Personal Data transferred.

- **Module 3 (Processor to Processor):** Applies where Customer is acting as a Processor on behalf of another Controller and Alauda is acting as a Subprocessor with respect to the Personal Data transferred.

4.3 The following optional clauses and selections apply to the EU Standard Contractual Clauses:

Clause	Selection
Clause 7 (Docking clause)	Included
Clause 9(a) (Use of sub-processors)	Option 2: General written authorization (with 30-day prior notice per Section 6.3)
Clause 11(a) (Redress)	Optional language not included
Clause 13 (Supervision)	Competent supervisory authority determined per Annex 1, Section C
Clause 17 (Governing law)	Option 1: Law of the EU Member State in which the data exporter is established or, where the data exporter is not established in an EU Member State, the laws of Ireland (per Section 9.2(c))
Clause 18(b) (Choice of forum and jurisdiction)	Courts of the EU Member State in which the data exporter is established or, where the data exporter is not established in an EU Member State, the courts of Ireland (per Section 9.2(c))

4.4 The Annexes to the EU Standard Contractual Clauses are completed as follows:

- **Annex I (Details of parties, description of transfer, competent supervisory authority):** As set out in Annex 1 to this Addendum.
- **Annex II (Technical and organizational measures):** As set out in Annex 2 to this Addendum.
- **Annex III (List of sub-processors):** As set out in Annex 3 to this Addendum (Annex III being furnished as the Subprocessor List maintained under the general written authorization in Clause 9(a), Option 2).

B. UK International Data Transfer Addendum

4.5 The UK International Data Transfer Addendum to the EU Standard Contractual Clauses (version B1.0, in force 21 March 2022, as updated from time to time by the UK Information Commissioner's Office under Section 119A of the UK Data Protection Act 2018) is incorporated by reference into this Addendum and applies to transfers of Personal Data as described in Section 9.3 of this Addendum.

4.6 The tables in the UK IDTA are completed as follows:

UK IDTA Table	Completion
Table 1 (Parties)	As set out in Annex 1, Section A to this Addendum
Table 2 (Selected SCCs, Modules, and Selected Clauses)	The EU Standard Contractual Clauses as referenced in Section A above, with the Module and clause selections as set out in paragraphs 4.2 and 4.3 of this Annex 4
Table 3 (Appendix Information)	Annex 1A (List of Parties): As set out in Annex 1, Section A; Annex 1B (Description of Transfer): As set out in Annex 1, Section B; Annex II (Technical and Organizational Measures): As set out in Annex 2; Annex III (List of Sub-processors): As set out in Annex 3

UK IDTA Table	Completion
Table 4 (Ending the UK IDTA)	The Importer may end the UK IDTA as set out in Section 19 of the UK IDTA

4.7 The competent supervisory authority for the purposes of the UK IDTA is the UK Information Commissioner's Office (ICO).

C. Supplementary Measures

4.8 In addition to the EU Standard Contractual Clauses and the UK IDTA, Alauda implements the following supplementary measures to ensure the effectiveness of the transfer mechanisms:

(a) **Technical measures:** Encryption of Personal Data in transit (TLS 1.2+) and at rest (AES-256), as further described in Annex 2.

(b) **Organizational measures:** Strict access controls, personnel training, and confidentiality obligations, as further described in Annex 2.

(c) **Contractual measures:** Binding data protection obligations on all Subprocessors, as described in Section 6.5 of this Addendum.

(d) **Transparency:** Alauda will promptly inform Customer if Alauda becomes aware of any changes in the laws of a country to which Personal Data is transferred that are likely to have a substantial adverse effect on the guarantees and obligations provided by the EU Standard Contractual Clauses, the UK IDTA, or the Swiss adaptation under Section 9.5 (including FDPIC-relevant changes).

End of Alauda Data Processing Addendum