Intapp Data Processing Addendum

This Data Processing Addendum ("Addendum") forms part of the Master Subscription and Services Agreement (the "Agreement") between: (i) Integration Appliance, Inc. and its Affiliates (collectively, "Intapp") and (ii) Customer and its Affiliates (collectively, "Customer"). Intapp's Affiliates may also enter into OSAs and SOWs with Customer, which OSAs and SOWs will be governed by the Agreement and in which event references in this Addendum to "Intapp" or "Integration Appliance, Inc." shall be deemed to be the Intapp Affiliate entering such OSA or SOW, including, where such Intapp Affiliate is a data importer, to its then current applicable address and other contact information.

The terms used in this Addendum shall have the meanings set forth in the Agreement unless otherwise provided. Except as modified below, the terms of the Agreement remain in effect.

In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement and apply to the processing of Customer Personal Data (as defined below) by Intapp. This Addendum shall not apply where and to the extent Intapp processes Personal Data (as defined below) as a Controller (as defined below). Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below:

1.1.1 **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with a party, or that is a successor (whether by change of name, dissolution, merger, consolidation, reorganization, sale or other disposition) to any such business entity or its business and assets.

1.1.2 **"Applicable Laws"** means, with respect to any Customer Personal Data, European Union or Member State laws and the laws applicable in the United Kingdom, United States, Switzerland, or Singapore (each as applicable).

1.1.3 "**Customer Personal Data"** or **"Customer Personal Information**" means any Personal Data Processed by Intapp on behalf of the Customer as a Processor pursuant to or in connection with the Agreement in respect of which the Customer is subject to applicable Data Protection Law; Customer Personal Data excludes Intapp CRM Data.

1.1.4 "**Data Protection Law**" means the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), the UK Data Protection Law, the Swiss Data Protection Law, the GDPR and laws implementing or supplementing the GDPR, the Singaporean Data Protection Law (each as applicable), as amended, replaced or superseded from time to time.

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

1.1.6 "**EEA Standard Contractual Clauses**" means the EEA Controller to Processor SCCs, the EEA Processor to Controller SCCs, and the EEA Processor to Processor SCCs.

1.1.7 "**EEA Controller to Processor SCCs**" means the Controller to Processor module (Module 2) of the standard contractual clauses, for the transfer of personal data from a data exporter acting as a controller to a data importer acting as a processor, which is approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021. A copy of the EEA Controller to Processor Clauses is set out as Appendix 2 at https://www.intapp.com/dpa/scc-2021-c2p/ .

1.1.8 "**EEA Processor to Controller SCCs**" means the Processor to Controller module (Module 4) of the standard contractual clauses, for the transfer of personal data from a data exporter acting as a processor to a data importer acting as a controller, which is approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021. If, applicable A copy of the EEA Processor to Controller Clauses is set out as Appendix 3 at https://www.intapp.com/dpa/scc-2021-p2c/ .

1.1.9 "**EEA Processor to Processor SCCs**" means the Processor to Processor module (Module 3) of the standard contractual clauses, for the transfer of personal data from a data exporter acting as a processor to a data importer acting as a processor, which is approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021. A copy of the EEA Processor to Processor Clauses is set out at https://www.intapp.com/vendor-dpa/v2022-03/scc-p2p/ .

1.1.10 "**GDPR**" means the EU General Data Protection Regulation 2016/679.

1.1.11 "**Intapp CRM Data**" means any data and information (including any personally identifiable information) provided or made available by Customer (including its employees, contractors agents and representatives) to Intapp which is required for Intapp's management of its relationship with Customer (including business contact information such as names, email addresses and telephone numbers).

1.1.12 **"Restricted Transfer**" means a transfer of Customer Personal Data:

(a) from a data exporter subject to the GDPR which is only permitted in accordance with the GDPR if a Transfer Mechanism is applicable to that transfer, ("**EEA Restricted Transfer**");

(b) from a data exporter subject to the UK GDPR which is only permitted in accordance with UK Data Protection Law if a Transfer Mechanism is applicable to that transfer ("**UK Restricted Transfer**"),

(c) from a data exporter subject to Swiss Data Protection Law which is only permitted in accordance with the Swiss Data Protection Law if a Transfer Mechanism is applicable to that transfer ("**Swiss Restricted Transfer**"),

(d) From a data exporter subject to Singapore Data Protection Law which is only permitted in accordance with the Singapore Data Protection Law if a Transfer Mechanism is applicable to that transfer ("**Singapore Restricted Transfer**").

For the avoidance of doubt, if the data exporter exports personal data from the EEA, the United Kingdom, or Switzerland, there will not be a Restricted Transfer where:

(a) the jurisdiction to which the personal data is transferred has been approved by the European Commission pursuant to Article 25(6) of the EC Directive 95/46 or Article 45 of the GDPR or, as applicable, an equivalent provision under UK Data Protection Law or Swiss Data Protection Law, as ensuring an adequate level of protection for the processing of personal data (an "**Adequate Country**"); or

(b) the transfer falls within the terms of a derogation as set out in Article 49 of the GDPR, the UK GDPR or similar provision under Swiss Data Protection Law (as applicable);

(c) insofar as and to the extent that the GDPR applies to a particular transfer, the data importer falls within the territorial scope of application of the GDPR in accordance with Article 3 of the GDPR.

1.1.13 "**Services**" means, for the purposes of this Addendum, Services (as defined in the Agreement) as well as Support and Cloud Services (as applicable).

1.1.14 "**Singapore Data Protection Law**" means the Personal Data Protection Act of 2012 ("**PDPA**") as amended, replaced, or superseded from time to time.

1.1.15 "**Standard Contractual Clauses**" means the EEA Standard Contractual Clauses, the Swiss Standard Contractual Clauses, and the UK Standard Contractual Clauses (each as applicable).

1.1.16 "**Subprocessor**" means any third party (including an Intapp Affiliate) appointed by or on behalf of Intapp to Process Customer Personal Data.

1.1.17 **"Swiss Data Protection Law"** means the Swiss Federal Act on Data Protection and its ordinances in the form applicable from time to time.

1.1.18 "**Transfer Mechanism**" means the Standard Contractual Clauses and/or any other means of effecting a Restricted Transfer which is permitted under the Data Protection Law that applies to the data exporter.

1.1.19 "**UK Data Protection Law**" means all laws relating to data protection, the processing of personal data, privacy, and/or electronic communications in force from time to time in the United Kingdom, including the UK GDPR, the UK Data Protection Act 2018 and the UK Privacy and Electronic Communications Regulations 2003.

1.1.20 **"UK GDPR"** has the meaning defined in the UK Data Protection Act 2018.

1.1.21 "**UK Standard Contractual Clauses**" means the applicable EEA Standard Contractual Clauses for the transfer of Personal Data, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 and which is amended and incorporated into this Addendum by Appendix 5.

2. GDPR Terms

2.1 The Parties hereby agree that the terms and conditions set forth in Sections 2 through 11 and Section 13 only apply where the UK Data Protection Law and/or the GDPR govern the Processing of Personal Data (each as defined below) processed hereunder, and that for purposes of such Sections, the UK Data Protection Law and/or the GDPR (and laws implementing or supplementing the GDPR) shall be the applicable Data Protection Law.

2.2 The terms "**Commission"**, "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**" and "**Supervisory Authority**"have the same meaning as in in the GDPR. The terms **"data exporter"** and **"data importer"** have the meanings set out in the applicable Standard Contractual Clauses.

3. Processing of Customer Personal Data

3.1 This Addendum applies to Intapp's Processing of Customer Personal Data in the course of Intapp providing Services to the Customer as a Processor. As such, for the purposes of the GDPR and UK GDPR, Intapp is the Processor and the Customer is the Controller.

3.2 Intapp will only Process Customer Personal Data in accordance with the Customer's documented instructions unless Processing is required by Applicable Laws to which Intapp is subject, in

which case Intapp will, to the extent permitted by Applicable Laws, inform the Customer of that legal requirement before Processing the Personal Data.

3.3 The Customer (i) instructs Intapp and (and authorises Intapp to instruct each Subprocessor) to Process Customer Personal Data, and in particular, transfer Customer Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Agreement; and (ii) represents and warrants that (a) it is and will at all relevant times remain authorised to give such instructions, and (b) all such instructions comply with Applicable Laws. In the event Customer instructs Intapp to Process Customer Personal Data in a manner that Intapp believes violates Applicable Law, Intapp will not Process the Customer Personal Data in that manner and will inform the Customer that Intapp believes such instruction violates Applicable Law.

3.4 Intapp will promptly notify the Customer if, in Intapp's reasonable opinion, any instructions violate Applicable Laws.

3.5 Appendix 1 to this Addendum sets out certain information regarding Intapp's Processing of the Customer Personal Data as required by Article 28(3) of the GDPR or equivalent provisions of any other applicable Data Protection Law (including the UK GDPR). Subject to the terms of, and the scope of the Services agreed by the Parties in the Agreement, Customer may make reasonable amendments to Appendix 1 by written notice to Intapp from time to time as Customer reasonably considers necessary to meet those requirements.

3.6 Nothing in the Addendum shall prevent Intapp from processing Intapp CRM Data for its own purposes in its capacity as a Controller (subject to Intapp's compliance with Data Protection Law).

4. Intapp Personnel

Intapp will ensure that any Intapp employee, agent or contractor who may have access to the Customer Personal Data is subject to confidentiality undertakings in respect of the Customer Personal Data.

5. Security

5.1 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, Intapp will implement appropriate technical and organisational measures in respect of Customer Personal Data to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR or equivalent provisions of any other applicable Data Protection Law.

5.2 In assessing the appropriate level of security, Intapp will take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. Subprocessing

6.1 Customer authorises Intapp to appoint (and permit each Subprocessor appointed in accordance with this Clause 6 to appoint) Subprocessors in accordance with this Clause 6 and any restrictions in the Agreement.

6.2 Intapp may continue to use those Subprocessors it has engaged as at the date of this Addendum.

6.3 Intapp will post a notice of the appointment of any new Subprocessor, including details of the Processing to be undertaken by the Subprocessor, on its website. Provided that Customer subscribes to notifications from Intapp by emailing dpa@intapp.com, Customer will receive notice of such

posting. If, within 10 business days of receiving the notice, Customer notifies Intapp in writing of any reasonable objections to the proposed appointment, Intapp will not appoint (or disclose any Customer Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by Customer and Customer has been provided with a reasonable written explanation of the steps taken.

6.4 With respect to each Subprocessor, Intapp will ensure that the arrangement between Intapp and the Subprocessor is governed by a written contract including terms offering at least the same level of protection for Customer Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR or equivalent provisions of any other applicable Data Protection Law.

6.5 Intapp will remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of any Subprocessor that cause Intapp to breach any of its obligations under this Addendum.

7. Data Subject Rights

7.1 The Services provide the Customer with a number of means by which the Customer may retrieve, correct, delete or restrict Customer Personal Data. Customer may use these means as technical and organizational measures to assist it in connection with its obligations under the applicable Data Protection Law, including its obligations relating to responding to requests from Data Subjects.

7.2 Intapp will (i) promptly notify Customer if it receives a request from a Data Subject under any applicable Data Protection Law in respect of Customer Personal Data; and (ii) not respond to that request except as required by Applicable Laws to which Intapp is subject, in which case Intapp will, to the extent permitted by Applicable Laws, inform Customer of that legal requirement before Intapp responds to the request.

8. Personal Data Breach

8.1 Intapp will notify Customer without undue delay, and in any event within 72 hours, upon becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under applicable Data Protection Law.

8.2 Intapp will cooperate with Customer and take such reasonable commercial steps as are appropriate in the circumstances to investigate, mitigate, and remediate each such Personal Data Breach.

9. Deletion or Return of Customer Personal Data

9.1 Subject to Clause 9.2, within 180 days of the expiration or termination of the Agreement (the "Termination Date"), Intapp will delete permanently the Customer Personal Data unless the Customer has previously deleted all such Customer Personal Data before the Termination Date.

9.2 Notwithstanding the foregoing, Intapp may retain Customer Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws (and Intapp may retain business contact information for Customer's staff); provided, however, that Intapp will ensure the confidentiality of all such Customer Personal Data and will ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its retention, and for no other purpose.

10. Data Protection Impact Assessments and Audit Rights

10.1 Intapp will provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of it by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, Intapp. The information made available in Clauses 10.2 through 10.4 is provided to assist the Customer in its compliance with those obligations.

10.2 Intapp is certified under ISO 27001 and agrees to maintain an information security program for the Services that complies with the ISO 27001 standards or such other alternative standards as are substantially equivalent to ISO 27001.

10.3 Intapp uses external auditors to verify the adequacy of its security measures. This audit (i) will be performed at least annually; (ii) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; and (iii) will be performed by independent third-party security auditors. At the conclusion of the audit the auditor will prepare an audit report ("Report"). Upon the Customer's request, Intapp will provide Customer with the Report so that Customer can reasonably verify Intapp's compliance with its obligations under this Addendum. The Report will be deemed Intapp Confidential Information.

10.4 Customer agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing Intapp to carry out the audit described in Clause 10.3. If the Standard Contractual Clauses apply, nothing in this Clause 10 varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses.

11. Restricted Transfers

11.1 The Parties will have in effect a Transfer Mechanism in respect of any Restricted Transfer.

11.2 Without prejudice to Clause 11.1, in the event of an EEA Restricted Transfer or a Swiss Restricted Transfer whereby Customer Personal Data is transferred from a data exporter acting as a controller to a data importer acting as a processor, the Parties shall comply with the EEA Controller to Processor SCCs provided that, for any Swiss Restricted Transfer, the EEA Controller to Processor SCCs shall apply as amended by Appendix 4.

11.3 Without prejudice to Clause 11.1, in the event of an EEA Restricted Transfer or Swiss Restricted Transfer whereby Customer Personal Data is transferred from a data exporter acting as a processor to a data importer acting as a controller, the Parties shall comply with the EEA Processor to Controller SCCs provided that, for any Swiss Restricted Transfer, the EEA Processor to Controller SCCs shall apply as amended by Appendix 4.

11.4 Without prejudice to Clause 11.1, in the event of a UK Restricted Transfer, whereby Customer Personal Data is transferred from a data exporter acting as a controller to a data importer acting as a processor, the Parties shall comply with the applicable UK Standard Contractual Clauses, which are hereby incorporated into this Addendum by virtue of Appendix 5.

11.5 Without prejudice to Clause 11.1, in the event of a UK Restricted Transfer, whereby Customer Personal Data is transferred from a data exporter acting as a processor to a data importer acting as a controller, the Parties shall comply with the applicable UK Standard Contractual Clauses, which are hereby incorporated into this Addendum by virtue of Appendix 5.

11.6 The Customer agrees that where Intapp engages a Subprocessor in accordance with Clause 6 for carrying out specific processing activities (on behalf of the Customer) and those processing activities involve a transfer of Customer Personal Data within the meaning of Chapter V of the GDPR or the UK GDPR, Intapp and Subprocessor can ensure compliance with Chapter V of the GDPR by using EEA Processor to Processor SCCs and ii) Chapter V of the UK GDPR by using the applicable UK Standard Contractual Clauses, provided the conditions for the use of those Standard Contractual Clauses are met. Where any updates or amendments to, or replacement of, a Transfer Mechanism is approved by the competent authority/ies (including, where applicable, the European Commission, a UK Government Department or a competent regulatory authority) during the Term ("New Transfer Mechanism"), the New Transfer Mechanism will be deemed to replace the applicable Transfer Mechanism under this Addendum from the date on which Intapp issues notice to Customer and shall be deemed to take effect and be binding on the parties from the date stipulated in such notice.

12. CCPA Terms

12.1 The Parties hereby agree that the terms and conditions set forth in Sections 4, 5, 7, 8 , 9, 12, and 14 apply only where the California Consumer Privacy Act, California Civil Code Sections 1798.100-1798.199 (as may be amended from time to time, the "**CCPA**") governs the processing of Personal Information (as defined below) processed hereunder, and that for purposes of such Sections, the CCPA shall be the applicable Data Protection Law.

12.2 The terms, "**Business**", "**Business Purpose**", "**Commercial Purpose**", "**Consumer**", "**Personal Information**", "**Sale**", "**Sell**", "**Selling**", and "**Service Provider**" have the same meaning as in the CCPA.

12.3 For the purposes of the CCPA, Customer is the Business and Intapp is the Service Provider.

12.4 For Customer Personal Information subject to the CCPA, Intapp acknowledges that it is prohibited from: (i) selling such Customer Personal Information; (ii) retaining, using, or disclosing such Customer Personal Information for a commercial purpose other than providing the Services or as otherwise permitted by the CCPA; and (iii) retaining, using, or disclosing such Customer Personal Information outside of the Agreement or other direct business relationship between Intapp and Customer; provided that (A) the foregoing shall not restrict Intapp's use of subcontractors or subprocessors in accordance with the Agreement and (B) nothing herein shall prevent Intapp from processing Intapp CRM Data for its own purposes in its capacity as a Business (subject to Intapp's compliance with Data Protection Law).

13. PDPA Terms

13.1 The Parties hereby agree that the terms and conditions set forth in Sections 3 to 10, 11.1, 13, and 14 apply only where Singapore Data Protection Law governs the processing of Customer Personal Data processed hereunder, and that for purposes of such Sections, Singapore Data Protection Law shall be the applicable Data Protection Law, save that the following shall apply:

13.1.1 the terms, "**Commission**", "**Data Breach**", "**Data Intermediary**", "**Individual**", "**Organisation**", and "**Process**" and have the same meaning as in Singapore Data Protection Law;

13.1.2 with respect to Clause 3.1, for the purposes of Singapore Data Protection Law, Customer is the Organisation and Intapp is the Data Intermediary;

13.1.3 with respect to Clause 3.6, nothing in the Addendum shall prevent Intapp from processing Intapp CRM Data for its own purposes in its capacity as an Organisation;

13.1.4 any reference to Personal Data Breach in the aforementioned sections shall be deemed to refer to Data Breach (as defined in Singapore Data Protection Law); and

13.1.5 any reference to Data Subject in the aforementioned sections shall be deemed to refer to Individuals (as defined in Singapore Data Protection Law.

13.2 Without prejudice to Clause 11.1, in the event of a Singapore Restricted Transfer where Customer Personal Data is transferred or Processed by Intapp in territories outside of Singapore, Intapp shall (a) make available information to the Customer on the specific countries and territories to which the Customer Personal Data may be transferred to, by keeping its Subprocessor page up-to-date, as outlined in Clause 6 herein; and (b) ensure that the recipient of such Customer Personal Data is bound by legally enforceable obligations to provide the transferred Customer Personal Data a standard of protection at least as comparable to that under Singapore Data Protection Law.

14. General Terms

14.1 Without prejudice to clauses 17 (Governing Law) and 18 (Choice of forum and jurisdiction) of the Standard Contractual Clauses:

14.1.1 the Parties agree to submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

14.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

14.2 In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses prevail. In the event of inconsistencies between this Addendum and any other agreements between the Parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum prevail.

14.3 This Addendum remains in effect until termination or expiration of the Agreement.

14.4 The limitations of liability set out in the Agreement shall also apply to this Addendum such that the total, aggregate liability of Intapp under or in connection with this Addendum (including the Standard Contractual Clauses), together with all liability of Intapp under or in connection with the Agreement, shall be subject to the financial limitations and restrictions of liability set out in the Agreement.

14.5 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum will remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties" intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

APPENDIX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Appendix 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR or equivalent provisions of any other European Data Protection Law (including the GDPR).

Subject matter and duration of the Processing of Customer Personal Data

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement and this Addendum.

The nature and purpose of the Processing of Customer Personal Data

Intapp provides software and/or services designed to support Customer's management and execution of its internal business operations

The types of Customer Personal Data to be Processed

The Personal Data to be Processed by Intapp on behalf of Customer may include, but is not limited to the following categories of Personal Data:

- Names, contact details and other identification information
- Personal information
- Biographical and occupational information
- Employment and HR information

The categories of Data Subjects to whom the Customer Personal Data relates

The Personal Data to be Processed by Intapp on behalf of Customer may relate to, but is not limited to, the following categories of Data Subjects:

- Employees, workers, contractors, agents and volunteers
- Clients, customers and (where applicable) their personnel

The obligations and rights of Customer

The obligations and rights of the Customer are set out in the Agreement and this Addendum.

ANNEX I TO APPENDIX 2 AND APPENDIX 3

A. LIST OF PARTIES

Data exporter(s):

1. Name: See Order and Sale Agreement

   Address: See Order and Sale Agreement

   Contact person's name, position and contact details:

   Activities relevant to the data transferred under these Clauses: Procurement of cloud services, support and related professional services from the Data Importer

   Signature and date: See Order and Sale Agreement

   Role: Controller

Data importer(s):

1. Name: Integration Appliance, Inc.

   Address: 3101 Park Blvd, Palo Alto, CA 94306

   Contact person's name, position and contact details: Robert Barrett, Senior Counsel Privacy, legal@intapp.com

   Activities relevant to the data transferred under these Clauses: Provision of cloud services, support and related professional services to the Data Exporter

   Signature and date: See Order and Sale Agreement

   Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Employees, contractors, and agents of the
- Clients, customers and (where applicable) their personnel

Categories of personal data transferred

- Names, contact details and other identification information
- Personal Information
- Biographical and occupational information
- Employment and HR information

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.

- N/A_____

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

- Frequently, if using a portion of the applicable Intapp Product that is provided by a sub-processor outside of the EEA, as detailed at www.intapp.com/sub-processors/
- Occasionally, depending on the amount of Support requests from the Data Exporter.
- Rarely, as necessary for the Data Importer to fulfill its security and availability commitments

Nature of the processing

- Depends on the processing taking place, for transfers necessitated by use of Products provided by Subprocessors the nature of the processing could include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.

Purpose(s) of the data transfer and further processing

- Provision of the Cloud Service, as outlined in the Agreement and applicable OSA and SOW (as these terms are defined 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

- Until the termination or expiration of the applicable OSA plus 180 days.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

- Same as above

C. COMPETENT SUPERVISORY AUTHORITY

The competent Supervisory Authority that has supervision over the relevant data exporter.

ANNEX II TO APPENDIX 2 AND APPENDIX 3

See www.intapp.com/dpa/scc-annex/

ANNEX III TO APPENDIX 2 AND APPENDIX 3

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

- See www.intapp.com/sub-processors

APPENDIX 4

Modification of the EEA Standard Contractual Clauses for the application of Swiss Data Protection Law

The Parties agree that the term Member State also applies to Switzerland. In particular, this shall ensure that data subjects are not excluded from the possibility to sue for their rights in their place of habitual residence.

The Parties agree that the references to provisions of the GDPR are to be understood as references to the corresponding provisions of the Swiss Federal Data Protection Act in the version applicable at the moment of initiation of any dispute.

The Parties agree that the term personal data also protects the data of legal persons until the entry into force of the revised Swiss Federal Data Protection Act.

The Parties agree that where Swiss Data Protection Law applies then clauses 17 and 18 of the EEA Standard Contractual Clauses shall be amended as follows:

Clause 17

Governing law

These Clauses shall be governed by the substantive laws of Switzerland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of Geneva, Switzerland.

(b) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(c) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX 5
UK International Data Transfer Addendum to the EEA Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start date	Effective Date of the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See Annex I to Appendix 2 and Appendix 3	See Annex I to Appendix 2 and Appendix 3
Key Contact	See Annex I to Appendix 2 and Appendix 3	See Annex I to Appendix 2 and Appendix 3
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: N/A Reference (if any): N/A Other identifier (if any): N/A Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	×	×	×			
2	✓	✓	×	General	14 days	
3	×	×	×	General	14 days	
4	✓	✓	×	N/A	N/A	N/A

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: **Data exporters**: Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union / United Kingdom are set out in Annex I to Appendix 2 and Appendix 3. **Data importers**: Identity and contact details of the data importer(s), including any contact person with responsibility for data protection are set out in Annex I to Appendix 2 and Appendix 3.
Annex 1B: Description of Transfer: See Annex I to Appendix 2 and Appendix 3
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II to Appendix 2 and Appendix 3
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex III to Appendix 2 and Appendix 3

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.