DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "**Addendum**") forms an integral part of and is incorporated by reference into Lokalise Master Service Agreement, Lokalise Terms of Service, Application License Agreement or other superseding written agreement by and between Customer and Lokalise Inc. (in either case referred to as the "**Agreement**") and is subject to the provisions therein, including limitations of liability. Terms defined in the Agreement shall have the same meaning when used in this Addendum, unless defined otherwise herein.

1. EXECUTION OF THE ADDENDUM

This Addendum consists of two parts: the main body of the Addendum and Appendix 1 and Appendix 2.

To complete this Addendum, Customer must:

a) Complete the information in the "Customer" signature section and sign the signature section; and

b) Submit the completed and signed Addendum via privacy@lokalise.com, indicating, if applicable, Customer Account Number (as set out on the applicable Customer order or the invoice).

This Addendum is already pre-signed by Lokalise. Upon receipt of the validly completed Addendum by Customer at the above email address, this Addendum will become legally binding. Lokalise will provide Customers with an email confirming receipt of the counter-signed Addendum. This Addendum shall become effective from the date of its countersigning by Customer, provided that it is duly delivered to the email address privacy@lokalise.com and received by Lokalise.

For the avoidance of doubt, signature on page 9 of the Addendum shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Appendices.

2. EFFECTIVENESS

A. This Addendum will be effective as of the date Lokalise receives a complete and executed Addendum from Customer in accordance with the instructions under Sections 1 and this Section 2 (the "Effective Date"). If Customer makes any deletions or other revisions to this Addendum, then this Addendum will be null and void.

B. Customer signatory represents to Lokalise that he/she has the legal authority to bind Customer and is lawfully able to enter into contracts.

C. Customer enters into the Addendum on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Affiliates.

D. This Addendum will terminate automatically upon termination of the Agreement or as earlier terminated pursuant to the terms of this Addendum.

3. DATA PROCESSING TERMS

Parties agree that the terms below shall have the following meanings:

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Controller" means the entity which determines the purposes and means of the processing of Personal Data, including as applicable any "business" as defined under the CCPA.

"Customer Data Incident" means any breach of security leading to the accidental or unlawful destruction, loss, alteration or damage, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored or otherwise Processed by Lokalise or its Sub-processors, of which Lokalise becomes aware.

“Customer Personal Data" means all the personal data processed by Lokalise as a Processor on behalf of Customer as a Controller in the course of providing Services. Customer Personal Data includes all Personal Data that Customer transfers to Lokalise in connection with its use of the Services.

“Customer” means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates). Customer shall be deemed the "Controller" for the purposes of this Addendum.

“Data Protection Law" means European Data Protection Law and U.S. Data Protection Law that are applicable to the processing of Customer Personal Data under this Addendum.

“Data Subject” means the identified or identifiable person to whom Customer Personal Data relates.

“Europe" means, for the purposes of this Addendum, the member states of the European Economic Area, Switzerland and the United Kingdom.

“European Data Protection Law" means any data protection and privacy laws of Europe applicable to Customer Personal Data in question, including where applicable (i) 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)("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) any applicable national implementations and supplementations of (i) and (ii); (iv) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance; and (v) in respect of the United Kingdom, the Data Protection Act 2018 and any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union; in each case as may be amended, superseded or replaced from time to time.

“Instruction" *and its cognates* mean the written, documented instruction issued by the Customer to Lokalise, delivered by email or courier, and directing the performance of a specific action with regard to Customer Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

“Personal Data” means information about an identified or identifiable natural person that (a) can be used to identify, contact or locate a specific individual; (b) can be combined with other information that can be used to identify, contact or locate a specific individual; or (c) is defined as "personal data" or "personal information" by applicable Data Protection Laws relating to the collection, use, storage or disclosure of information about an identifiable individual.

“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, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means the entity which processes Personal Data on behalf of the Controller, including as applicable any “service provider” as defined by the CCPA.

“Standard Contractual Clauses" or “EU-SCCs” means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), in the form set out in Appendix 2; as amended, superseded or replaced from time to time in accordance with this Addendum. When Customer is acting as a controller, the Controller-to-Processor Clauses (module 2) will apply to a Data Transfer. When Customer is acting as a processor, the Processor-to-Processor Clauses (module 3) will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that Lokalise will know the identity of Customer’s controllers because Lokalise has no direct relationship with Customer’s controllers and therefore, Customer will fulfil Lokalise’s obligations to Customer’s controllers under the Processor-to-Processor Clauses;

"Sub-Processor" means any Processor engaged by Lokalise or Lokalise Affiliates to assist in fulfilling Lokalise obligations with respect to the provision of the Services to Customer under the Agreement.

"Supervisory Authority" means an independent public authority, which is (i) established by a European Union Member State pursuant to Article 51 of the GDPR or (ii) the public authority governing data protection, which has supervisory authority and jurisdiction over Customer.

"UK Addendum" means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner's Office under S119(A) of the UK Data Protection Act 2018, as may be amended, superseded, or replaced from time to time.

"U.S. Data Protection Law" means data protection or privacy laws applicable to Customer Personal Data in force within the United States, including the California Consumer Privacy Act ("CCPA"), as may be amended from time to time, and any rules or regulations implementing the foregoing.

4. PROCESSING OF PERSONAL DATA

4.1. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Customer Personal Data pursuant to the Addendum, Customer and its Affiliates is a Controller except (a) when Customer acts as a processor of Personal Data, in which case Lokalise is a sub-processor; or (b) as stated otherwise in the Addendum, Lokalise is a Processor and that Lokalise or its Affiliates will engage Sub-processors pursuant to this Addendum. This Addendum does not apply to any content transferred through the Platform or any third-party applications or software used in connection with the Services.

4.2. Lokalise's Role as a Controller. To the extent Lokalise uses or otherwise processes Customer Personal Data for Lokalise's legitimate business operations related to the Services, Lokalise will comply with the obligations of an independent Controller under the Data Protection Laws for such use. Lokalise is accepting the added responsibilities of a Controller for processing in connection with its legitimate business operations to:

(a) facilitate contractual and pre-contractual business relationships;

(b) act consistent with regulatory and legal requirements;

(c) personalize the Platform for Customer use by understanding Customer's needs;

(d) create new features, tools and products;

(e) conduct aggregate analysis, market research and planning;

(f) protect Lokalise, Lokalise's customers and the public;

(g) provide customer support;

(h) provide Services-related communication;

(i) publish marketing and events-related communication;

(j) create interest-based advertising.

More detailed information about the categories of Personal Data, nature, and purposes of the Processing when Lokalise acts as a Controller in Lokalise Privacy Policy at https://lokalise.com/privacy-policy.

4.3. No joint controllership. The parties acknowledge and agree that each is acting independently as a Controller with respect to Personal Data, except for Customer Personal Data as defined in this Addendum, and the parties are not joint controllers. Each party will, to the extent that it, along with the other party, acts as a Controller with respect to Personal Data, reasonably cooperate with the other party to enable data protection rights to be exercised as set forth in the applicable Data Protection Laws.

4.4. Details of the Processing. The subject-matter of Processing of Customer Personal Data by Lokalise is the performance of the Services pursuant to the Agreement. The duration of the Processing, the

nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this Addendum are further specified in Appendix 1 (Details of the Processing) to this Addendum.

5. CUSTOMER'S OBLIGATIONS

5.1. Compliance with Law. Customer shall Process Personal Data in accordance with the requirements of Data Protection Laws including any applicable requirement to provide notice to Data Subjects of the use of Lokalise as a Processor and/or obtain Data Subjects consent to such Processing.

5.2. Legal Ground. Customer shall ensure that there is a legal ground and the purpose for Processing of Personal Data in accordance with the Agreement.

5.3. Instructions. Customer shall provide Lokalise with Instructions regarding Lokalise's Processing of Customer Personal Data as set out in this Addendum and in any additional documented instructions provided by Customer, if applicable. Customer shall not instruct Lokalise to Process Personal Data in violation of Data Protection Laws.

5.4. Responsibility. Customer shall undertake sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

5.5. Designation of a Contact. At Lokalise's request, Customer shall designate to Lokalise a single point of Customer's contact responsible for (i) receiving and responding to Data Subject Requests Lokalise receives from Customer Data Subjects relating to Customer Personal Data; and (ii) notifying Lokalise of Customer's intended response to Data Subject Requests processed by Lokalise on behalf of Customer and authorizing Lokalise to fulfil such responses on behalf of Customer.

6. LOKALISE'S OBLIGATIONS

6.1. Compliance with Law. Lokalise shall treat Customer Personal Data as confidential information and shall Process Personal Data in accordance with the requirements of Data Protection Laws and this Addendum.

6.2. Confidentiality. Lokalise shall ensure that any person who is authorized to Process Customer Personal Data on Lokalise's behalf, including Lokalise's Affiliates, personnel, and Sub-processors, is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

6.3. Compliance with Instructions. Lokalise shall only process Customer Personal Data in accordance with Instructions from the Customer, unless obligated to do otherwise by applicable law, in which case Lokalise shall notify the Customer of such legal requirements prior to the processing, unless the relevant law prohibits notification due to an important public interest, for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Customer's Authorized Users in their use of the Services; and (iii) Processing to comply with other documented reasonable Instructions provided by Customer (e.g., via email) where such Instructions are consistent with the terms of the Agreement. The Agreement, including this Addendum, along with Customer's configuration of any settings or options in the Service (as Customer may be able to modify from time to time), constitute Customer's complete and final Instructions to Lokalise regarding the Processing of Customer's Personal Data, including for purposes of the Standard Contractual Clauses.

6.4. Notification. Lokalise has no obligation to monitor the compliance of Customer's use of the Service with applicable law, including Data Protection Law, though Lokalise shall use commercially reasonable efforts to promptly inform Customer if an Instruction provided under this Addendum, in Lokalise's opinion, infringes applicable Data Protection Laws or is in any way misleading or unclear or if Lokalise does not have an Instruction on the Processing of Customer Personal Data in a particular situation.

6.5. Restrictions. Without limiting the foregoing: (a) Lokalise will not collect, retain, use, disclose, or otherwise Process Customer Personal Data in a manner inconsistent with Lokalise's role as Customer's Processor (regardless of whether the CCPA applies); (b) Lokalise will not "sell" the Personal Data, as such term is defined in the CCPA; and (c) Lokalise hereby certifies that it understands the restrictions and obligations set forth in this Addendum and that it will comply with them.

7. RIGHTS OF DATA SUBJECTS

7.1. Data Subject Request. Lokalise will to the extent legally permitted, promptly notify Customer if Lokalise receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated decision making, each such request being a "Data Subject Request" (including "verifiable consumer requests", as such term is defined in the CCPA). Notwithstanding the foregoing, the Customer hereby instructs Lokalise to delete user accounts upon user requests to ensure prompt deletion of data.

7.2. Assistance. Taking into account the nature of Processing, Lokalise will provide reasonable effort to assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, upon Customer's request Lokalise will provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request. Customer will be responsible for any costs arising from Lokalise's provision of such assistance.

8. LOKALISE'S PERSONNEL

8.1. Confidentiality. Lokalise shall ensure that its personnel engaged in Processing of Customer Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements or are under an appropriate statutory obligation of confidentiality regarding Customer Personal Data.

8.2. Limitation of Access. Lokalise shall ensure that access to Customer's Personal Data is limited to those personnel performing Services in accordance with the Agreement to the extent required to perform their obligations in connection with the Services.

8.3. Data Protection Officer. Lokalise has appointed a data protection officer. The appointed person may be reached by email via privacy@lokalise.com.

9. SUB-PROCESSORS

9.1. Appointment of Sub-processors. Customer acknowledges and provides general authorization that (a) Lokalise's Affiliates may be retained as Sub-processors; and (b) Lokalise and Lokalise's Affiliates may appoint third-party Sub-processors in connection with the provision of the Services. For the avoidance of doubts, the Customer generally authorizes the appointment of any third party as Sub-processors to Process Customer's Personal Data as necessary to perform the Services.

9.2. Protection. Lokalise or Lokalise's Affiliate shall use reasonable efforts to enter into an agreement in written or electronic form, including, insofar as applicable, the Standard Contractual Clauses, with each Sub-processor containing data protection obligations similar to those in this Addendum with respect to the protection of Customer Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. Such agreement shall provide, as far as possible, sufficient guarantees to implement appropriate technical and organizational measures in such a manner that Processing will meet the requirements of applicable Data Protection Laws.

9.3. List of Sub-processors. Lokalise shall make available to Customer the current list of Sub-processors for the Services. Such Sub-processor lists shall include the identities of those Sub-processors, their country of location and purposes of sub-processing of Personal Data. Customers may find a current list of Lokalise Sub-processors on Lokalise webpage accessible via https://lokalise.com/sub-processors. Lokalise will promptly update the list reflecting any addition, replacement, or other changes to Lokalise's Sub-processors. If Customer subscribes to updates using the form available on the Sub-processor list webpage mentioned above, Lokalise will email Customer notification of the updates when Lokalise posts it. Customer will be notified of the update either by checking the Lokalise webpage or by email if Customer has subscribed for the update.

9.4. Objection Right. Customers may reasonably object in writing for appointment of a new Sub-processor if the new Sub-processor is proven to represent a substantial and unreasonable risk to the protection of Customer's Personal Data, subject to the termination and liability clauses of the Agreement. An objection for a new Sub-processor shall be sent to privacy@lokalise.com within ten (10) business days after notification thereon. Customer acknowledges that appointment of Sub-processors is essential for the provision of the Services and the objection for a new Sub-processor may prevent Lokalise from offering the Services to Customers.

9.5. Limitation of access. Lokalise shall ensure that each Sub-processor only accesses and uses Customer's Personal Data to the extent required to perform the obligations subcontracted to it in connection with the Services.

9.6. Liability. Lokalise shall be liable for the acts and omissions of its Sub-processors to the same extent Lokalise would be liable if performing the services of each Sub-processor directly under the terms of this Addendum, except as otherwise set forth in the Agreement.

10. THIRD-PARTY DATA PROCESSORS

Customer acknowledges and agrees that in the provision of some Services (such as integrations and plugins accessible at: https://lokalise.com/integrations), Lokalise, pursuant to Instructions issued by Customer, may transfer Customer Personal Data to and otherwise interact with third-party data processors. Customer agrees that if and to the extent that such transfers occur, Customer is responsible for entering into separate contractual arrangements with such third-party data processors, imposing on them data protection obligations and restrictions in accordance with Data Protection Laws. For the avoidance of doubt, such third-party data processors are not considered Sub-processors within the meaning of this Addendum.

11. SECURITY AND ASSISTANCE

11.1. Protection of Customer Personal Data. Lokalise shall maintain appropriate technical and organizational measures for protection of the security, confidentiality, and integrity of Customer Personal Data, as required under the applicable Data Protection Laws. Lokalise will regularly monitor compliance with these measures. The technical and organizational measures are subject to technical progress and further development. In this respect, it is permissible for Lokalise to implement alternative adequate measures. Lokalise will not materially decrease the overall security of the Services during the term of the Agreement.

11.2. Third-Party Certifications and Audits. Lokalise will obtain the third-party certifications and audits as required under the applicable Data Protection Laws. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Lokalise will make available to Customer, who is not a competitor of Lokalise, (or Customer's independent, third-party auditor, who is not a competitor of Lokalise) a copy of Lokalise's the most recent third-party audits or certifications, as applicable (the "Report").

11.3. Data Protection Impact Assessment and Consultation. Upon Customer's request, Lokalise shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Services and to consult with Supervisory Authorities, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Lokalise. Additional support for Customer's data protection impact assessment or relations with Supervisory Authorities would require mutual agreement on fees, the scope of Lokalise's involvement, and any other terms that the parties deem appropriate.

12. CUSTOMER DATA INCIDENT MANAGEMENT

12.1. Protection. Lokalise will implement and maintain data security incident management policies and procedures, compliant with applicable Data Protection Laws, which address the management of Customer Data Incident.

12.2. Notification. Lokalise will notify Customer without any undue delay (in any event within 48 hours) after becoming aware of a Personal Data breach affecting any Customer Personal Data, and to the extent possible provide Customer with details of Customer Data Incident.

12.3. Assistance. At Customer's request, Lokalise will promptly provide Customer with all reasonable assistance necessary to enable Customer to report relevant Customer Data Incident to competent Supervisory Authorities and/or affected Data Subjects, if Customer is required to do so under the Data Protection Laws.

13. RETURN OR DELETION OF CUSTOMER PERSONAL DATA

13.1. Return and Destruction. Either upon request by Customer or when Lokalise no longer is required to Process Customer Personal Data to fulfil its obligations under the Agreement, Lokalise will (and will procure that its Affiliates and Sub-processors will) (a) cease all use of Customer Personal Data; and (b) return all Customer Personal Data and all copies thereof to Customer, or, at Company's option, delete Customer Personal Data and all copies thereof, and certify in writing that it has done so. Any additional cost arising in connection with the return or deletion of Customer Personal Data after the termination or expiration of the Agreement shall be borne by Customer.

13.2. Retention. Lokalise may retain a copy of Customer Personal Data to the extent required by applicable laws, including Data Protection Laws, for a specified period, in which case Lokalise shall ensure the confidentiality of such Customer Personal Data, shall ensure that such Customer Personal Data is Processed as necessary for the purpose(s) specified in applicable law requiring its storage and for no other purpose. After such time, Lokalise will immediately delete of all Customer Personal Data.

13.3. Exception. If Lokalise is unable to delete Customer Personal Data for technical or any other reasons, Lokalise will, to the extent possible, procure anonymization of Customer Personal Data, and apply measures to ensure that Customer Personal Data is restricted from any further Processing.

13.4. Permitted Processing. Lokalise may continue to Process any Customer Personal Data that has been anonymized, that is, aggregated in a manner that does not identify individuals or its Customers, to improve Lokalise's systems and Services or if Processing of Customer Personal Data is required to protect the legitimate interests of Lokalise and/or for any legal matters thereto. More detailed information in Lokalise Privacy Policy at https://lokalise.com/privacy-policy.

14. AUDIT RIGHTS

14.1. Audit right. Lokalise undertakes to provide the Customer, upon request, with the necessary information required to provide evidence of the implementation of the technical and organizational measures by submitting a copy of Lokalise's most recent third-party audits or certifications, as

applicable. If those documentation made available to Customer does not provide, in Customer's reasonable judgment, sufficient information to confirm Lokalise's compliance with the terms of this Addendum, the Customer or an accredited third-party auditor who is not a competitor of Lokalise, mutually agreed upon by Customer and Lokalise, has the right, after consultation with Lokalise, to audit Lokalise's compliance with the terms of this Addendum by means of random checks during the regular operating and business hours without disrupting the operational processes, with reasonable prior written notice and consent of Lokalise, provided such consent shall not be unreasonably delayed or withdrawn, and subject to reasonable confidentiality procedures, including a confidentiality agreement. Customer may not audit Lokalise more than once per calendar year, unless otherwise stipulated by a competent supervisory authority.

14.2. Audit costs. Customer shall be responsible for all costs and fees related to such audits, including all reasonable costs and fees for Lokalise's time and resources spent on any such audit in addition to the rates for Services provided by Lokalise under the Agreement. Before the commencement of any such audit, Customer and Lokalise shall mutually agree upon the scope, timing, and duration of the audit. Customer agrees that the scope of the audit shall be limited to matters specific to Customer.

14.3. Audit results. Customer will provide Lokalise with copies of any audit reports generated in connection with any audit under this Section 14, unless prohibited by applicable law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this Addendum. Customer will promptly notify Lokalise with information regarding any noncompliance discovered during the course of an audit.

15. DATA TRANSFER OUTSIDE OF EUROPE

15.1. Data Transfer. Customer consents that Lokalise may transfer Customer Personal Data outside Europe as necessary to provide the Services to a jurisdiction for which the European Commission or the UK has not issued an adequacy decision, provided Lokalise has implemented a transfer solution compliant with Data Protection Laws, which shall include:

a) Standard Contractual Clauses**.** In relation to transfers of Customer Personal Data protected by the EU GDPR Lokalise shall process Customer Personal Data in accordance with the EU-SCCs in the form set out in Appendix 2, which are incorporated into and form a part of this Addendum. The parties agree that for the purposes of the descriptions in the Standard Contractual Clauses, Lokalise is the "data importer" and Customer is the "data exporter" notwithstanding that Customer may itself be located outside Europe and/or is acting as a Processor on behalf of third-party Controllers. When Customer is acting as a controller, the Controller-to-Processor Clauses (module 2) will apply to a Data Transfer. When Customer is acting as a processor, the Processor-to-Processor Clauses (module 3) will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that Lokalise will know the identity of Customer's controllers because Lokalise has no direct relationship with Customer's controllers and therefore, Customer will fulfil Lokalise's obligations to Customer's controllers under the Processor-to-Processor Clauses;

b) UK Addendum. In relation to transfers of Customer Personal Data protected by UK data protection law, the EU-SCCs (i) apply as completed in accordance with paragraph (a) above; and (ii) are deemed amended as specified by the UK Addendum, which is deemed executed by the Parties and incorporated into and forming an integral part of this Addendum as follows:

(i) Table 1 shall be deemed completed with the information set out in Appendix 2 of this Addendum (Annex I to the EU-SCCs), as appropriate, the contents of which are hereby agreed by the Parties;

(ii) In Table 2, the Parties select the checkbox reading: "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", and the accompanying table shall be deemed to be completed according to the EU-SCCs in the form set out in Appendix 2 of this Addendum;

(iii) Table 3 shall be deemed completed with the information set out in Appendix 1 and Appendix 2 of this Addendum (Annexes I-III of the EU-SCCs), the contents of which are hereby agreed by the Parties;

(iv) Table 4 in Part 1 is deemed completed by selecting the checkbox reading: "neither party";

(v) Any conflict between the terms of the EU-SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

c) Another appropriate safeguard pursuant to Article 46 of the GDPR;

d) Derogation pursuant to Article 49 of the GDPR.

15.2. Compliance. Lokalise will promptly notify Customer if it becomes aware that it can no longer meet its obligations under this Section 15, and in such event, to work with Customer and promptly take all reasonable and appropriate steps to stop any Processing outside of Europe. Customer Personal Data that originates in Europe will then be processed and used exclusively within Europe. Lokalise will not transfer Customer Personal Data to, or process such data in, a location outside of Europe without Customer's prior written consent or until Processing meets the level of protection as is required by Section 15(1).

16. LIMITATION OF LIABILITY

Each party's and all its Affiliates' liability, taken together in the aggregate, arising out of or related to this Addendum to the other Party and/or its Affiliates, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the applicable Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all its Affiliates under the Agreement and all Addendums together. For the avoidance of doubt, Lokalise' and its Affiliates' total liability for all claims from Customer and all of its Affiliates arising out of or related to the applicable Agreement and each Addendum will apply in the aggregate for all claims under both the Agreement and all Addendums established under the Agreement, including by Customer and all Affiliates, and, in particular, will not be understood to apply individually and severally to the Customer and/or to any Affiliate that is a contractual party to any such Addendum. Neither Customer nor any of its Affiliates shall be entitled to recover more than once in respect of the same claim under this Addendum. Also, for the avoidance of doubt, each reference to the term "Addendum" herein means this Addendum including its Schedules and Appendixes.

17. GENERAL TERMS

17.1. Conflict of provisions. In the event of any conflict or inconsistency between any provisions of the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) the Standard Contractual Clauses; (b) this Addendum; (c) the effective then Customer Order to the Agreement; and (d) the Agreement.

17.2. Termination. This Addendum will have the same duration as, and will be subject to, the termination terms of the Agreement. The obligations of Lokalise to implement appropriate security measures with respect to Customer Personal Data will survive the termination of this Addendum and will apply for as long as Lokalise retains Customer Personal Data.

17.3. Governing law. This Addendum will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement unless required otherwise by Data Protection Law.

The parties' authorized signatories have duly executed this Addendum:

On behalf of …… (“Customer”, “Controller”)	On behalf of **Lokalise Inc.**: (“Processor”):
By: …….. Title: …….. Signature: …….. Date: …….. (“Effective Date”)	By: Petr Antropov Title: CRO Signature: DocuSigned by: F939FAC60AD44E3…… Date: 2/27/2023 ……

APPENDIX 1 DETAILS OF PROCESSING

Where Lokalise Acts as a Processor

Subject Matter

Lokalise will Process Customer Personal Data as necessary to provide the Services to the Customer pursuant to the Agreement.

Purpose of Processing

Processing of Customer Personal Data is necessary (i) to provide the Services to Customer, including, to facilitate payment transactions for the Services, to identify Customer's team working on the Team's Workspace at the Platform; (ii) to identify contact persons of Customer for the purposes of provision of customer and technical support to Customer; and/or (ii) disclosures required by the applicable law in accordance with the Agreement.

Duration of Processing

Lokalise will Process Customer Personal Data for the duration of the Agreement, plus the period from the expiration of the Agreement while Customer Personal Data is retained by Lokalise on behalf of Customer.

Data Subjects

Customers and their Authorized Users, including officers, employees, contractors and third parties that have, or may have, a commercial relationship with Customer (e.g., translators, editors or marketing managers).

For the avoidance of doubt, all the Personal Data is collected based on Customer's request. This means that Lokalise does not Process (collects) Customer Personal Data (bank details, credit card details) unless explicitly requested by Customer to do so.

Data Processing Activities

Personal Data transferred through the Platform will be processed in accordance with the applicable law, the Agreement, Lokalise Privacy Policy and may be subject to the following Processing operations: collecting, 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.

Categories of Personal Data

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

Users authorized by Customer to access the Platform and use the Services.

Types of Personal Data:

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include:

- Email address, full name, IP address of Authorized Users;
- Customer legal name and registered address (for legal entities);
- Position (role in the team) of Authorized Users;
- Phone number of the Customer's representatives.

If the Customer makes payments or conducts payment transactions related to the Services through a third-party website or application, Lokalise will receive Customer's transaction information in Lokalise's third-party payment processing software along with partial details of the bank account information. The information that Lokalise will be able to verify will include payment method information, such as:

- Cardholder name;
- Email address;
- Unique customer identifier;
- Order ID;
- Limited bank account details; or partial payment card details (last four numbers and card type);
- Card expiration date;
- Date/time/total amount of transaction;
- Location.

Different payment methods may require the collection of various categories of information. The payment method information that Lokalise collects will depend upon the payment method that Customer chooses to use from the available payment methods offered to Customer.

Sensitive Data

Lokalise does not knowingly process any special categories of data in the context of the processing activities described in the Addendum and the Agreement. The Agreement contains prohibition of transfer of any sensitive data through the Platform.

Location of the Processing Operations

The European Union, the United Kingdom, the United States, and other areas, if deemed necessary by Processor and Sub-processors.

APPENDIX 2

STANDARD CONTRACTUAL CLAUSES

This Appendix is attached to and forms part of the Data Processing Addendum. Unless otherwise defined in this attachment, capitalised terms used in this attachment have the meanings given to them in the Addendum.

When Customer is acting as a controller, the Controller-to-Processor Clauses (**module 2**) will apply to a Data Transfer. When Customer is acting as a processor, the Processor-to-Processor Clauses (**module 3**) will apply to a Data Transfer. Where no specific modules are mentioned, the clauses apply to all data exporters, regardless of whether the Customer is a controller or a processor.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – **Module 2** (**Controller-to-Processor Clauses)**: Clause 8.1(b), 8.9(a), (c), (d) and (e); **Module 3** (**Controller-to-Processor Clauses)**: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 – **Module 2** (**Controller-to-Processor Clauses)**: Clause 9(a), (c), (d) and (e); **Module 3** (**Controller-to-Processor Clauses)**: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE 2: Transfer controller to processor (when Customer is acting as controller)

8.1. Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout

the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6. Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE 3: Transfer processor to processor (when Customer is acting as a processor)

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue

delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE 2: Transfer controller to processor (when Customer is acting as controller)

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 20 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE 3: Transfer processor to processor (when Customer is acting as a processor)

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 20 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the subprocessor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure

that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) **MODULE 2: Transfer controller to processor (when Customer is acting as controller)**The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE 3: Transfer processor to processor (when Customer is acting as a processor)

(f) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(g) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(h) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

MODULE 2: Transfer controller to processor (when Customer is acting as controller)

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

MODULE 3: Transfer processor to processor (when Customer is acting as a processor)

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE 2: Transfer controller to processor (when Customer is acting as controller)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

MODULE 3: Transfer processor to processor (when Customer is acting as a processor)

15.1 Notification

(b) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(iii) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(iv) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

(f) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(g) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(h) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(i) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(d) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(e) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(f) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

MODULE 2: Transfer controller to processor (when Customer is acting as controller)

In these cases, it shall inform the competent supervisory authority of such noncompliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

MODULE 3: Transfer processor to processor (when Customer is acting as a processor)

In these cases, it shall inform the competent supervisory authority and the controller of such noncompliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Latvia.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Latvia.

(c) 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.

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

[Signatures on page 9 already constitute signature and acceptance of the Standard Contractual Clauses, including the following Appendices.]

ANNEX 1

A. LIST OF PARTIES

1. Data exporter(s): [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]

Name: Customer as provided in the Agreement.

Address: As provided in the Agreement.

Contact person's name, position and contact details: As provided in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Appendix 1 of the Addendum.

Signature and date: Executed on the same day as the Addendum, which shall be deemed executed the date of its countersigning by Customer, provided that it is duly delivered to the email address privacy@lokalise.com and received by Lokalise.

Role (controller/processor): Where the Customer determines the purposes and means of the Processing of Personal Data, its role is a Controller; where the Customer acts on behalf of and under the instructions of a Controller, its role is a Processor.

2. Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: Lokalise Inc.

Address: 3500 South DuPont Highway, Suite BZ-101, Dover, DE 19901, USA

Contact person's name, position and contact details: Didzis Balodis, InfoSec Officer

Activities relevant to the data transferred under these Clauses: Fulfilment of data importer's obligations with respect to the provision of the Services to data exporter under the Agreement. The activities specified in Appendix 1 of the Addendum.

Signature and date: 15/09/2021

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

1) Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include the following categories of data subjects: Customers and their Authorized Users, including officers, employees, contractors and third parties that have, or may have, a commercial relationship with Customer (e.g., translators, editors or marketing managers).

2) Categories of personal data transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, the following categories of personal data:

- Email address, full name, IP address of Authorized Users;
- Customer legal name and registered address (for legal entities);
- Position (role in the team) of Authorized Users;
- Phone number of the Customer's representatives.

If data exporter makes payments or conducts payment transactions related to the Services through a third-party website or application, data importer will receive data exporter's transaction information in data importer's third-party payment processing software along with partial details of the bank account information. The information that data importer will be able to verify will include payment method information, such as:

- Cardholder name;
- Email address;
- Unique customer identifier;
- Order ID;
- Limited bank account details; or partial payment card details (last four numbers and card type);
- Card expiration date;
- Date/time/total amount of transaction;
- Location.

Different payment methods may require the collection of various categories of information. The payment method information that data importer collects will depend upon the payment method that data exporter chooses to use from the available payment methods offered to data exporter.

3) *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.*

Data importer does not knowingly process any special categories of data in the context of the processing activities described in the Addendum and the Agreement. The Agreement contains prohibition of transfer of any sensitive data through the Platform.

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

Data exporter's personal data might be transferred on a one-off or on a continuous basis, depending on the purpose of transfer, and the data exporter's use of the Services.

5) *Nature of the processing*

The nature of the processing of data exporter's personal data may include such operations as hosting, collection, recording, organisation, structuring, storage, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, migration, erasure or destruction of data (whether or not by automated means) etc.

Personal Data transferred through the Platform will be processed in accordance with the applicable law, the Agreement, data importer's Privacy Policy and may be subject to the following processing operations: collecting, 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.

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

Processing of data exporter's personal data is necessary (i) to provide the Services to the data exporter, including, to facilitate payment transactions for the Services, to identify data exporter's team working on the Team's Workspace at the Platform; (ii) to identify contact persons of data exporter for the purposes of provision of customer and technical support to data exporter; and/or (ii) disclosures required by the applicable law in accordance with the Agreement.

7) *The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.*

Data importer will process data exporter's personal data for the duration of the Agreement, plus the period from the expiration of the Agreement while date exporter's personal data is retained by data importer on behalf of data exporter.

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

Data exporter's personal data is transferred to sub-processors to the extent needed to ensure the provision of Services under the Agreement to data exporter. The nature of processing corresponds to the nature of processing indicated under point 5. Data importer may transfer data exporter's personal data to sub-processors while the Agreement is effective provided data exporter does not object to such transfer as provided herein.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Lokalise Inc. shall maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Personal Data. Lokalise regularly monitors compliance with these safeguards. Lokalise will not materially decrease the overall security of the Service during a term of an Agreement.

Technical and Organisational measure of Lokalise include the following:

1) Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;
2) Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
3) Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing;
4) Measures for user identification and authorization;
5) Measures for the protection of data during transmission;
6) Measures for the protection of data during storage;
7) Measures for ensuring events logging and log analysis;
8) Measures for ensuring secure system configuration;
9) Measures for internal IT and IT security governance and management;
10) Measures for certification/assurance of processes and products;
11) Measures for ensuring data minimization;
12) Measures for ensuring data quality;
13) Measures for ensuring limited data retention;
14) Measures for ensuring accountability;
15) Measures for allowing data portability and ensuring erasure.

ANNEX III

LIST OF SUB-PROCESSORS

The sub-processors are specified in Section 9 of the Addendum. Customers may find a current list of Lokalise Sub-processors on Lokalise webpage accessible via https://lokalise.com/sub-processors.