kandji

DATA PROCESSING ADDENDUM
(Last updated March 1, 2023)

This Data Processing Addendum, including its Exhibits and Appendices ("DPA") forms part of the Master Subscription Agreement available at https://www.kandji.io/terms or, if applicable, any superseding written agreement between Kandji, Inc. ("Kandji") and You (in either case, the "Agreement").

By signing the Agreement, You (as such term is defined in the Agreement) enter into this DPA on behalf of Yourself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of Your Authorized Affiliates, if and to the extent Kandji processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purpose of this DPA only, and except where indicated otherwise, the term "You" shall include You and Authorized Affiliates. All capitalized terms not defined herein have the same meaning set forth in the Agreement.

In the course of providing the Services under the Agreement, Kandji may Process Personal Data on Your behalf and the parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

HOW TO EXECUTE THIS DPA

1. This DPA consists of two parts: (a) the main body of the DPA, and (b) Schedules 1 and 2.

2. This DPA has been pre-signed on behalf of Kandji. Schedule 1 has been pre-signed by Kandji, Inc. as the data importer.

3. To complete this DPA, You must:
   a. Complete the information in the signature box and sign on Page 12.
   b. Send the completed and signed DPA to Kandji by email to legal@kandji.io.

This DPA becomes legally binding upon receipt by Kandji of this validly executed DPA at the above email address.

For the avoidance of doubt, Your signature of the DPA on Page 12 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses including Schedules 1 and 2.

HOW THIS DPA APPLIES

If the entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case the Kandji entity that is party to the Agreement is party to this DPA.

If the entity signing this DPA has executed an Order Form with Kandji or its Affiliate pursuant to the Agreement, but is itself not a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms; and the Kandji entity that is party to such Order Form is party to this DPA.

If the entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the entity who is a party to the Agreement executes this DPA.

This DPA shall not replace any comparable or additional rights relating to Processing of Your Data contained in Your Agreement (including any existing data processing addendum to the Agreement).

Table of Contents

1. DATA PROCESSING TERMS

“**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 fifty percent (50%) of the voting interests of the subject entity.

“**Authorized Affiliate**” means any of Your Affiliate(s) which (a) is subject to Data Protection Laws and Regulations and (b) is permitted to use the Services pursuant to the Agreement between You and Kandji, but has not signed its own Order Form with Kandji and is not "You" as defined under the Agreement.

“**Controller**” means the entity which determines the means and purposes of the Processing of Personal Data.

“**Data Exporter**” means the Controller who transfers the personal data.

“**Data Importer**” means the Processor who agrees to receive from the data exporter personal data.

“**Data Protection Laws and Regulations**” means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including: 1) the California Consumer Privacy Act including as amended by the California Privacy Rights Act (together, “CCPA”), 2) the Virginia Consumer Data Protection Act, 3) and other laws and regulations of the United States and its states, 4) the General Data Protection Regulation (Regulation (EU) 2016/679) (“EU GDPR” or “GDPR”), 5) The Data Protection Act 2018 which is the UK's implementation of the General Data Protection Regulation (“UK GDPR”), 6) and other European Data Protection Laws and Regulations, each as amended from time to time.

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

“**EU Standard Contractual Clauses**” means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated June 4, 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).

“**Kandji**” means Kandji and its Affiliates engaged in the Processing of Personal Data.

“**Personal Data**” or "**Personal Information**" means any information describing or relating to (i) an identified or identifiable natural person or household and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Your Data.

“**Processing**” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“**Processor**” means the Party which Processes Personal Data on behalf of the Controller, including as applicable any "Service Provider" as that term is defined by the CCPA.

“**Security and Privacy Documentation**” means the Security and Privacy documentation applicable to the specific Services licensed by You, as updated from time to time, and available HERE.

“Standard Contractual Clauses” means the EU Standard Contractual Clauses and the UK International Data Transfer Addendum.

“**Sub-processor**” means any Processor engaged by Kandji.

“**Supervisory Authority**” means an independent public authority which is established by an EU Member State pursuant to the GDPR, or if in the UK, then the Information Commissioner’s Office (“ICO”).

“UK International Data Transfer Addendum” means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner and in force since March 21, 2022.

“**You**” means the entity that accepted the Agreement together with its Affiliates which have signed Order Forms.

“**Your Data**” has the same meaning as defined in the Agreement, provided that such data is electronic data and information submitted by or for You to the Services.

2. PROCESSING OF PERSONAL DATA

2.1. Roles of the Parties. The parties acknowledge and agree that (a) with regard to the Processing of Personal Data, You are the Controller or and Kandji is the Processor, as applicable, and (b) Kandji’s engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-Processors” below.

2.2. Duration. Kandji shall process Personal Data throughout the duration of the term of the Agreement (including any Order Form(s) thereto) or any renewal term thereof. Upon termination of the Services by either party, Kandji shall cease processing Personal Data on Your behalf upon completion of the termination provisions described herein.

2.3. Your Processing of Personal Data. You shall, in Your use of the Services, Process Personal Data in accordance with the requirements of all applicable Data Protection Laws and Regulations, including without limitation requirements to provide notice to Data Subjects of the use of Kandji as Processor. You shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which You acquired Personal Data. You represent and warrant that You have established a lawful basis to Process Personal Data, Your use of the Services will not violate the rights of any Data Subject, and You have the right to transfer, or provide access to, the Personal Data to Kandji for Processing in accordance with the terms of the Agreement (including this DPA). You shall inform Kandji without undue delay if You are not able to comply with Your obligations under this DPA or any applicable Data Protection Laws and Regulations. For the avoidance of doubt, Kandji is not responsible for compliance with any Data Protection Laws and Regulations applicable to You or Your industry that are not generally applicable to Kandji.

2.4. Kandji’s Processing of Personal Data. You appoint Kandji to process the Personal Data contained in Your Data on Your behalf as necessary for Kandji to provide the Services under the Agreement. All Personal Data Processed under the Agreement (including this DPA) will be stored, organized, and made available to You as the Controller. Kandji shall treat Personal Data as Confidential Information. If Kandji is required by applicable law to disclose Your Data for a purpose unrelated to the Agreement, Kandji will first inform You of the legal requirement and give You an opportunity to object or challenge the requirement, unless the law prohibits such notice. Notwithstanding the foregoing, Kandji shall have the right to collect and use Personal Data contained in Your Data to investigate a use of the Service that is unlawful or violates the Agreement, provide, and develop the Service, respond to legal actions, or for administrative purposes such as accounting and compliance.

2.5. Nature, Purpose, and Subject-Matter of the Processing. The nature and purpose of Kandji's Processing of Personal Data as Your Processor is described in and governed by the Agreement. The subject-matter of data Processed under this DPA is Personal Data of Your employees, contractors, representatives, and other end user Data Subjects and as otherwise described in the Agreement. Kandji shall only Process Your Data for the purpose of providing the Services to You and to comply with Your Instructions. For each Service for which Processing is involved, 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 DPA are further specified in Schedule 1 to this DPA ("Parties and Description of Transfer").

2.6. Instructions. Kandji shall Process, retain, use, store, or disclose Personal Data only according to written, documented instructions issued by You to Kandji to perform a specific or general action with regard to Personal Data for the purpose of providing the Services to You pursuant to the Agreement (Your "Instructions"). The parties agree that the Agreement (including this DPA and any Order Form(s)), together with Your use of the Services in accordance with the Agreement, constitute Your complete and final Instructions to Kandji in relation to the Processing of Your Data. You may modify, amend, add, or replace individual Instructions in writing ("Additional Instructions") to Kandji at privacy@kandji.io. Any Additional Instructions must be consistent with this DPA and the Agreement. If Kandji determines that Additional Instructions are outside the scope of the Agreement, Kandji may charge additional fees and/or require a written agreement between Kandji and You to perform such Additional Instructions. Kandji shall inform You without delay if, in Kandji's opinion, an Instruction violates applicable Data Protection Laws and Regulations or Kandji is unable to follow an Instruction and, where necessary, cease all Processing until You issue new Instructions with which Kandji is able to comply.

3. RIGHTS OF DATA SUBJECTS

Kandji shall, to the extent legally permitted, promptly notify You if Kandji receives a request from a Data Subject to exercise the Data Subject's right under applicable Data Protection Laws and Regulations relating to Your Data, each such request being a "Data Subject Request". Taking into account the nature of the Processing, if You are unable to independently address a Data Subject Request, Kandji will assist You by appropriate technical and organizational measures, insofar as this is possible and to the extent Kandji is legally permitted to do so, for the fulfilment of Your obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. You shall be legally responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data and for all costs associated with the same.

4. KANDJI PERSONNEL

4.1. Confidentiality. Kandji shall ensure that its personnel engaged in the Processing of 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. Kandji shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. Reliability. Kandji shall take commercially reasonable steps to ensure the reliability of any Kandji personnel engaged in the processing of Personal Data.

4.3. Limitation of Access. Kandji shall ensure that Kandji's access to Personal Data is limited to those personnel who are necessary to provide the Services.

4.4 Data Protection Officer. Kandji has appointed a data protection officer. The appointed person may be reached at privacy@kandji.io

5. SUB-PROCESSORS

5.1. Appointment of Sub-processors. You authorize Kandji to engage the Sub-Processors on our Sub-Processor List as of the effective date of this DPA to Process Your Data pursuant to the Agreement (including this DPA) and You acknowledge and agree that (a) Kandji's Affiliates may be retained as Sub-processors and (b) Kandji and Kandji's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Kandji or a Kandji Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Your Data to the extent applicable to the nature of the services provided by such Sub-processor.

5.2. List of Current Sub-processors and Notification of New Sub-processors. Kandji shall make available to You the current list of Sub-processors for the applicable Service(s). Such Sub-processor lists shall include the identities of those Sub-processors and their country of location. You may also find this information on Kandji's Sub-processor Page, located HERE, as well as a mechanism to subscribe to notifications of new Sub-processors, to which You shall subscribe, and if You subscribe, Kandji shall provide notification of any new Sub-processors before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

5.3. Objection Right for New Sub-processors. You may object to Kandji's use of a new Sub-processor by notifying Kandji promptly in writing within ten (10) business days after receipt of Kandji's notice in accordance with the mechanism set out in Section 5.2. In the event You object to a new Sub-processor, as permitted in the preceding sentence, Kandji will use reasonable efforts to make available to You a change in the Services or recommend a commercially reasonable change to Your configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub- processor without unreasonably burdening You. If Kandji is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, You may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Kandji without the use of the objected-to new Sub-processor by providing written notice to Kandji. Kandji will refund You any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on You.

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

6. SECURITY

6.1. Controls for the Protection of Your Data. Kandji shall maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Your Data. In doing so, Kandji shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. You are solely responsible for (a) determining whether the Services meet Your security standards and support Your obligations under Data Protection Laws and Regulations and (b) the secure use of Kandji's Services by Yourself or any individual You provide with an Authorized Device, including but not limited to securing account authentication information and ensuring no User seeks to misuse Personal Data or engages in activities likely to give rise to a Data Incident (defined below).

6.2. **Audits**. Kandji shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to You information to demonstrate compliance with the obligations set out in this DPA as set forth in this "Audits" Section.

6.2.1. **Third-Party Certifications and Audits**. Kandji has obtained the third-party certifications and audits set forth HERE. Upon Your written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Kandji shall make available to You (or Your Third-Party Auditor - as defined below in Section 6.2.4) information regarding Kandji's compliance with the obligations set forth in this DPA in the form of a copy of Kandji's then most recent third-party audits or certifications. Such third-party audits or certifications may also be shared with Your competent Supervisory Authority on its request. Upon Your reasonable request, Kandji shall provide a report and/or confirmation of Kandji's audits of third-party Sub-processors' compliance with the data protection controls set forth in this DPA and/or a report of third party auditors' audits of third party Sub-processors that have been provided by those third-party Sub-processors to Kandji, to the extent such reports or evidence may be shared with You ("Third-party Sub-processor Audit Reports"). You acknowledge that (i) Third-party Sub-processor Audit Reports shall be considered Confidential Information as well as confidential information of the third-party Sub-processor and (ii) certain third-party Sub-processors to Kandji may require You to execute a non-disclosure agreement with them in order to view a Third-party Sub-processor Audit Report.

6.2.2. **On-Site Audit**. You may contact Kandji to request an on-site audit of Kandji's Processing activities covered by this DPA ("On-Site Audit"). An On-Site Audit may be conducted by You directly or through a Third-Party Auditor (as defined below in Section 6.2.4) selected by You when: (i) the information available pursuant to Section 6.2.1 "Third-Party Certifications and Audits" is not sufficient to demonstrate compliance with the obligations set out in this DPA and its Schedules; (ii) You have received a notice from Kandji of regarding a Data Incident; or (iii) an On-Site Audit is required by Data Protection Laws and Regulations or by Your competent supervisory authority. Any On-Site Audits will occur during Kandji's normal business hours, in a manner that does not reasonably interfere with Kandji's normal business operations and will be limited to Your Data Processing and storage facilities operated by Kandji or any of Kandji's Affiliates. No On-Site Audit shall last more than two (2) consecutive business days. Your access to Kandji's proprietary and confidential information shall be limited to that which is strictly necessary to complete the On-Site Audit. You acknowledge that Kandji operates a shared cloud environment. Accordingly, Kandji shall have the right to reasonably adapt the scope of any On-Site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Kandji customers' and users' information. You shall promptly provide Kandji with the full report and complete results of any On-Site Audit.

6.2.3. **Reasonable Exercise of Rights**. An On-Site Audit shall be conducted by You or your Third-Party Auditor: (i) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Services used by You; (ii) up to one time per year with at least three weeks' advance written notice. If an emergency justifies a shorter notice period, Kandji will use good faith efforts to accommodate the On-Site Audit request; and (iii) during Kandji's normal business hours, under reasonable duration and shall not unreasonably interfere with Kandji's day-to-day operations. Before any On-Site Audit commences, You and Kandji shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which You shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of Kandji.

6.2.4. **Third-Party Auditor**. A Third Party Auditor means a third-party independent contractor that is not a competitor of Kandji. An On-Site Audit can be conducted through a Third Party Auditor if: (i) prior to the On-Site Audit, the Third Party Auditor enters into a non-disclosure agreement containing confidentiality provisions no less protective than those set forth in the Agreement to protect Kandji's proprietary information; and (ii) the costs of the Third Party Auditor are at Your expense.

7. DATA INCIDENT MANAGEMENT AND NOTIFICATION

Kandji shall notify You without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Your Data, including Personal Data, transmitted, stored or otherwise Processed by Kandji or its Sub-processors occurring on Kandji or our Sub-Processor's information system of which Kandji becomes aware (a "Data Incident"). Kandji shall make reasonable efforts to identify the cause of such Data Incident and take such steps as Kandji deems necessary and reasonable to remediate the cause of such a Data Incident to the extent the remediation is within Kandji's reasonable control. At Your reasonable request, and to the extent Kandji is required to do so under applicable Data Protection Laws and Regulations, Kandji will promptly provide You with commercially reasonable assistance as necessary to enable You to meet Your obligations under applicable Data Protection Laws and Regulations to notify authorities and/or affected Data Subjects. The obligations herein shall not apply to incidents that are caused by You or Your Users.

8. GOVERNMENT ACCESS REQUESTS

8.1 Kandji Requirements. If Kandji receives a legally binding request from a Public Authority to access Personal Data that Kandji Processes on Your behalf, Kandji shall, unless otherwise legally prohibited, promptly notify You including a summary of the nature of the request. To the extent Kandji is prohibited by law from providing such notification, Kandji shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Kandji to communicate as much information as possible, as soon as possible. Further, Kandji shall challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. Kandji shall pursue possibilities of appeal. When challenging a request, Kandji 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. Kandji agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. Kandji shall promptly notify You if Kandji becomes aware of any direct access by a Public Authority to Your Data and provide information available to Kandji in this respect, to the extent permitted by law. For the avoidance of doubt, this DPA shall not require Kandji to pursue action or inaction that could result in civil or criminal penalty for Kandji such as contempt of court.

8.2. Sub-processors requirements. Kandji shall ensure that Sub-processors involved in the Processing of Personal Data are subject to the relevant commitments regarding Government Access Requests in the EU Standard Contractual Clauses and the UK IDTA as applicable.

9. RETURN OR DELETION OF PERSONAL DATA

Upon termination or expiration of the Agreement or any renewal term thereof, Kandji will delete all Personal Data Processed under the Agreement that is in Kandji's possession. In the case of any Personal Data not so deleted, Kandji will return, destroy, or render anonymous all such Personal Data in accordance with Your reasonable written Instructions submitted to Kandji within 30 days of termination or expiration of the Agreement, subject to the limitations described in the Agreement. The requirements of this Section 9 do not apply to the extent that Kandji is required by applicable law to retain some or all of Your Data, or to Your Data that is archived on back-up systems, which data Kandji shall securely isolate and protect from any further Processing and delete in accordance with Kandji's deletion practices.

10. AUTHORIZED AFFILIATES

10.1. Contractual Relationship. The parties acknowledge and agree that, by executing the Agreement, You enter into the DPA on behalf of yourself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Kandji and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 10 and Section 11. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by You.

10.2. Communication. You as the contracting party to the Agreement shall remain responsible for coordinating all communication with Kandji under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10.3. Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Kandji, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

10.3.1. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Kandji directly by itself, the parties agree that (i) solely You as the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) You as the contracting party to the Agreement shall exercise any such rights under this DPA, not separately for each Authorized Affiliate individually, but in a combined manner for itself and all of its Authorized Affiliates together.

10.3.2. The parties agree that You as the contracting party to the Agreement shall, when carrying out an On-Site Audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Kandji and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

11. LIMITATION OF LIABILITY

Except as specifically provided in the EU Standard Contractual Clauses, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Kandji, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, Kandji's and its Affiliates' total liability for all claims from You and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by You and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to You and/or to any Authorized Affiliate that is a contractual party to any such DPA.

12. **EUROPEAN UNION SPECIFIC PROVISIONS**

The parties agree that transfers of Personal Data, which are processed in accordance with the EU GDPR, from the Data Exporter to the Data Importer outside of the European Economic Area, are made pursuant to the Module Two (Controller to Processor) EU Standard Contractual Clauses, which are deemed entered into (and incorporated into this Addendum by this reference).

For Module Two (Controller to Processor) of the EU Standard Contractual Clauses, the following applies:

1. The optional docking clause in Clause 7 does not apply.
2. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 5 of this Addendum;
3. In Clause 11, the optional language does not apply;
4. All square brackets in Clause 13 are hereby removed;
5. In Clause 17 (Option 1), the EU SCCs will be governed by Irish law;
6. In Clause 18(b), disputes will be resolved before the courts of Ireland;
7. Schedule 1 sections 1 to 10 to this Addendum contains the information required in Annex I of the EU SCCs;
8. Schedule 1 section 11 to this Addendum contains the information required in Annex II of the EU SCCs; and
9. By entering into this Addendum, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

13. **UNITED KINGDOM SPECIFIC PROVISIONS**

The parties agree that transfers of Personal Data, which are processed in accordance with the UK GDPR, from the Data Exporter to the Data Importer outside of the United Kingdom, are made pursuant to the Module Two (Controller to Processor) EU Standard Contractual Clauses and amended by the United Kingdom's International Data Transfer Addendum, which are deemed entered into (and incorporated into this Addendum by this reference).

14. **US STATE SPECIFIC PROVISIONS**

14.1 Definitions. This Section 13 shall apply only to the extent Kandji Processes Personal Data that is subject to the protection of the CCPA and other US State Privacy Laws which are materially the same as the CCPA. For the purposes of this section 13 these terms shall be defined as follows:

- "Business", "Service Provider", "Sell", and "Share" shall have the meanings given to them in the CCPA.
- "Controller" is replaced with "Business" wherever those terms appear in this DPA.
- "Processor" is replaced with "Service Provider" wherever those terms appear in this DPA.

14.2 Responsibilities. The Parties agree that Kandji will Process Personal Information contained in Your Data as Your Service Provider in accordance with the CCPA and strictly for the business purpose of performing the Service under the Agreement. Kandji shall not (i) Sell Personal Information contained in Your Data; (ii) Share Personal Information contained in Your Data with third parties for cross-contextual behavioral advertising purposes; (iii) retain, use, or disclose Personal Information contained in Your Data for a commercial purpose other than for such business purpose or as otherwise permitted by the CCPA; or (iv) retain, use, or disclose Personal Information contained in Your Data outside of the direct business relationship between You and Kandji. You agree that You are solely liable for Your compliance with the CCPA in Your use of Kandji's Service.

14.3 No CCPA Sale. The parties agree that You do not sell California Personal Information to Kandji because, as a Service Provider, Kandji may only use California Personal Information contained in Your Data for the purposes of providing the Services to You.

15. PARTIES TO THIS DPA

The section "HOW THIS DPA APPLIES" specifies which Kandji entity is party to this DPA. Where the Standard Contractual Clauses apply, Kandji, Inc. is the signatory to the Standard Contractual Clauses. Where the Kandji entity that is a party to this DPA is not Kandji, Inc., that Kandji entity is carrying out the obligations of the data importer on behalf of Kandji, Inc. Notwithstanding the signatures below of any other Kandji entity, such other Kandji entities are not a party to this DPA or the Standard Contractual Clauses.

16. LEGAL EFFECT

This DPA shall only become legally binding between You and Kandji when the requirements set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed.

List of Schedules
Schedule 1: Parties and Description of Transfers
Schedule 2: UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

[Signature Page Follows]

The parties' authorized signatories have duly executed this DPA:

Kandji, INC.	**You**
BY: DocuSigned by: Danny Zorotovich E6DA426A69734BF...	BY:
NAME (PRINTED): Danny Zorotovich	NAME (PRINTED):
TITLE: Chief Financial Officer	TITLE:
DATE: 4/24/2023	DATE:

SCHEDULE 1: PARTIES AND DESCRIPTION OF TRANSFER

1. LIST OF PARTIES

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: You and Your Authorized Affiliates

Address: __________________

Contact person's name, position, and contact details: __________________

Activities relevant to the data transferred under these clauses: Provision of the Services pursuant to the Agreement as further described in the Documentation.

Signature and date: __________________

Role: For the purposes of the EU Controller to Processor Standard Contractual Clauses You and/or Your Authorized Affiliates are a Controller.

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

Name: Kandji, Inc.

Address: 101 W. Broadway, Ste. 1440, San Diego CA 92101

Contact person's name, position, and contact details: Danny Zorotovich, CFO, legal@kandji.io

Signature and date: DocuSigned by: Danny Zorotovich F6DA426A69734BF... 4/24/2023

Role: Processor

2. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

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

- Your Users authorized by You to use the Services.

3. CATEGORIES OF PERSONAL DATA TRANSFERRED

You may submit Personal Data to the Services, the extent of which is determined and controlled by You in Your sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First Name, Last Name
- Username
- Title

- Employer
- Photographic headshots (optional)
- Unique identifier for authorized devices
- File paths, file names and associated macros, if any
- Personal Information submitted to the Services by the end users

In addition to the categories listed above, the customer, rather than Kandji , determines which additional categories of Personal Data exist and will be disclosed to and processed by the Kandji in the provisioning of the services because (i) customer's infrastructure (e.g., endpoint, virtual machine and cloud environments) is unique in configurations and naming conventions, (ii) Kandji enables the customer to configure settings in the services, and (iii) customer controls (such as via deployment, configuration, and submission) which customer content is uploaded, or is collected by, the services or products.

4. SENSITIVE DATA TRANSFERRED

The parties do not anticipate the transfer of sensitive data under the Agreement.

5. FREQUENCY OF THE TRANSFER

Data is transferred on a continuous basis depending on Your use of the Services.

6. NATURE OF THE PROCESSING

The nature of the Processing is the provision of the Services pursuant to the Agreement

7. PURPOSE OF PROCESSING, THE DATA TRANSFER AND FURTHER PROCESSING

Kandji will Process Personal Data as necessary to provide the Services pursuant to the Agreement, as further specified in the relevant Order Form and/or Documentation, and as further instructed by You in Your use of the Services.

8. DURATION OF PROCESSING

Subject to Section 2.2 of the DPA, Kandji will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

9. SUB-PROCESSOR TRANSFERS

Sub-processor(s) will Process Personal Data as necessary to provide the Services pursuant to the Agreement. Subject to section 5 of this DPA, the Sub-processor(s) will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing. Identities of the Sub-processors used for the provision of the Services and their country of location are listed on Kandji's Sub-processor Page, located at www.kandji.io/service-provider.

10. COMPETENT SUPERVISORY AUTHORITY

- 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 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 shall act as the 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: Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland shall act as the competent supervisory authority.
- Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as the competent supervisory authority.
- Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations

11. TECHNICAL AND ORGANISATIONAL MEASURES

In addition to the administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Security and Privacy documentation available HERE, Kandji also had implemented the following technical and organizational measures:

Access Control

- The Kandji platform is hosted on Amazon Web Services. Additionally, Kandji maintains contractual relationships with vendors in order to provide the Services in accordance with our Data Processing Agreement. Kandji relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

- Under AWS's shared responsibility model, the physical and environmental security controls are maintained by AWS and audited for SOC 2 Type I and ISO 27001, 27017, 17018 compliance, among other certifications by an AICPA Accredited third party public trust audit firm.

- Kandji enforces a uniform password policy for its technology infrastructure components. Customers can configure their own password requirements for Kandji platform administrative level accounts. Customers who interact with the Kandji administrative user interface must authenticate via multi-factor authentication or via their own single sign-on identity provider and associated strong identity policies. Access to systems and applications with customer data requires two-factor authentication in the form of user ID / password, and a one-time password (OTP) or certificate. Additionally access to systems that house and can expose access to personal information is restricted to those users whose job function absolutely requires access to this data, and the principle of least privilege is applied.

- Customer data is stored in multi-tenant storage systems accessible to Kandji's customers only via application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Kandji's products uses role-based access control to ensure that only appropriate individuals can access relevant resources. A systems administrator approves internal user access to the infrastructure provider for authorized personnel. Access approvals and modifications to the user access list are logged.

- Application Programming Interface ("API") access: Additional functionality may be accessed via the Kandji API. API access requires authentication via an API key. API keys can be further constrained by customers to reduce the set of capabilities that a given API key is authorized to invoke. These API invoked activities are logged within the Kandji administration web interface.

- A subset of Kandji's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. All such requests are logged. Employees are granted access by role, and reviews of high-risk privilege grants are initiated regularly. System owners conduct quarterly user access reviews of production servers, databases and applications to validate internal user access is commensurate with job responsibilities. Identified access changes are tracked to remediation.

- Background checks are performed on new hires before the new hire's start date as permitted by local laws. The Human Resources team reviews the results and takes any appropriate action deemed necessary. Kandji has an established code of conduct outlining ethical expectations, behavior standards, and ramifications of non-compliance, and requires internal personnel to acknowledge it.

Transmission Control

- In-transit: Kandji uses Transport Layer Security version 1.2 or better paired with appropriately selected cipher suites on every one of its login Interfaces and API Endpoints. Kandji's HTTPS implementation uses industry standard algorithms and certificates, specifically 256 bit AES Encryption in Galois Counter Mode, aka AES-256-GCM.

- At-rest: Kandji stores user passwords following policies that support industry standard practices for security. For example, passwords are stored as non-reversible hashes using a properly selected password-hashing function.

- All customer data is encrypted at rest using the cloud service provider's key management service and cryptographic modules.

Input Control

- Kandji implements intrusion detection and infrastructure monitoring to detect threats to the network environment. Kandji uses logging review and alerting as well as application performance monitoring software to collect data from servers and endpoints, detect potential security threats or unusual system activity, monitor system performance, and track resource utilization.

- IP Filtering (Internet protocol version 4) configurations ensure available networking ports and protocols are restricted to approved business rules. Web application firewalls ensure only appropriate messages are reviewed by our web facing API Interfaces. Distributed Denial of Service controls protect Kandji applications from network OSI layers 3,4 and 7 attacks. Kandji's DDoS provider also protects Kandji from common layer 7 attacks and removes traffic from known bad actors.

- To maintain separation of duties, one engineer plans and prepares a change request and then a second individual engineer reviews, tests, and approves configuration changes before the changes are deployed into production. Kandji has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.

- Kandji engages a qualified third party penetration testing vendor to conduct a network and application penetration test of the production environment at least annually.. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

- Kandji's infrastructure is configured to log information about system behavior, traffic, system authentication, and other application requests. System tools monitor company load balancers and notify appropriate personnel of any events or outages based on predetermined criteria. Any identified issues are tracked through resolution in accordance with the Incident Management Policy.

- Kandji maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Kandji will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

- If Kandji becomes aware of unlawful access to non-Kandji data stored within its Services, Kandji will: 1) notify the affected customers of the incident; 2) provide a description of the steps Kandji is taking to resolve the incident; and 3) provide status updates to the customer contact, as Kandji deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the customer's contacts in a form Kandji selects, which may include via email or telephone.

Availability Control

- Kandji maintains a vulnerability management program to detect and remediate system vulnerabilities. Vulnerability scans are executed monthly on production systems. Any critical or high-risk vulnerabilities are tracked through resolution.

- Infrastructure availability: Kandji's Cloud Service Provider's infrastructure services use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

- Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple datacenters.

- Online replicas and backups: Kandji databases are designed to replicate data between no less than 1 primary and 1 secondary database. Database replicas are hosted in separate availability zones. Availability zones have their own separate redundant infrastructure services. All databases are backed up and maintained using at least industry standard methods.

- Kandji's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Kandji operations in maintaining and updating the product applications and backend while limiting downtime.

SCHEDULE 2: UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	February 1, 2023	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As described in Schedule 1	As described in Schedule 1.
Key Contact	As described in Schedule 1.	As described in Schedule 1.
Signature (if required for the purposes of Section 2)	Each party's signature of Agreement shall be considered a signature to the UK Addendum.	

Table 2: Selected SCCs, Modules and Selected Clauses

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

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	No	--	--			
2	Yes	Excluded	Excluded	Refer to Section 5 of DPA	Refer to Section 5 of DPA	
3	No	--	--			
4	No	--	--			

Table 3: Appendix Information

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

Annex 1A: List of Parties: As indicated in Annex 1 of the Section 2 Model Clauses
Annex 1B: Description of Transfer: As indicated in Annex 1 of the Section 2 Model Clauses
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As indicated in Annex 2 of the Section 2 Model Clauses
Annex III: List of Sub processors (Modules 2 and 3 only): Not relevant for Module 1

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

Entering into this Addendum

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

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

Interpretation of this Addendum

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

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

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

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

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

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

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

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

Hierarchy

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

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

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

Incorporation of and changes to the EU SCCs

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

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

b. Sections 0 to 0 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

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

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 0, the provisions of Section 0 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 0 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 0) are made:

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

b. In Clause 2, delete the words:

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

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

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

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

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

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

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

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

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

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

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

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

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

m. Clause 17 is replaced with:

> “These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

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

b. reflects changes to UK Data Protection Laws;

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

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

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

b. its risk under the Addendum,

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

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

Alternative Part 2 Mandatory Clauses:

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