KOBO TOOLBOX – DATA PROCESSING AGREEMENT

on the Processing of Personal Data by Kobo on behalf of User who is Subject to the GDPR

This Data Processing Agreement ("DPA"), as updated from time to time, is between

[Name]
[Organization]
[Title]
[Address]
[Email]

,

being the holder of the User Account [Account Name] on the [Global/Humanitarian] server or the entity or other body (e.g., employer) represented by the holder of this User Account, as applicable, in either case a Controller or Processor of User Data ("**User**"),

and

Kobo, Inc., 37 Highland Ave, Cambridge, Massachusetts 02139, U.S. ("**Kobo**"), acting as the User's Processor or sub-processor respectively for the processing of User Data.

KoboToolbox is a set of freely available open source software tools (with all code being available to the public at https://github.com/kobotoolbox) that is used predominantly by people working in the areas of humanitarian assistance, economic development, peacebuilding, and human rights.

This DPA shall apply to the extent and under the conditions that (1) the User uses the Services through their User Account, (2) so that Kobo processes Personal Data in the form of User Data on behalf of the User, and (3) the GDPR applies to this use of the Services. If the User is not the holder of the User Account but represented by the holder of the User Account, actions and conduct of the holder of the User Account within the scope of this DPA shall be deemed as actions and conduct of the User.

1. DETAILS OF THE PROCESSING OF USER DATA BY KOBO

1.1 The subject matter and purpose of the processing is the User Data which is processed by Kobo to provide the Services.
1.2 The nature of the processing is the storage, visualization, and similar processing of User Data.
1.3 The duration of the processing corresponds to the duration of the use of the Services by the User.
1.4. The type of Personal Data processed is the User Data. It may include special categories of Personal Data within the meaning of Article 9 GDPR.
1.5 The categories of Data Subjects may include, without limitation, the User's interview partners, employees, end-users, customers, sub-contractors, or customers' or subcontractors' employees.

2. DEFINITIONS

The following definitions shall apply in this DPA:
Controller: has the meaning given to it in the GDPR.
Controller-to-Processor SCCs: means the Standard Contractual Clauses – Transfer controller to processor (Module Two), as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
EEA: means the European Economic Area.
EU: means the European Union.
GDPR: means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

In Writing: includes electronic text form such as email or pdf.
KoboToolbox Server: means one or more servers maintained by Kobo for the purpose of providing the Services.
Parties: means the User and Kobo.
Personal Data: means personal data as defined in the GDPR and to the extent processed by Kobo when providing the Services.
Processor: has the meaning given to it in the GDPR.
Processor-to-Processor SCCs: means the Standard Contractual Clauses – Transfer processor to processor (Module Three), as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
Pseudonymous: refers to Personal Data that cannot be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that no such attribution takes place.
Security Breach: an event which has led or may lead to a personal data breach as defined in the GDPR, but not including unsuccessful attempts or activities that do not compromise the security of the User Data, such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other broadcast attacks on firewalls or edge servers, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.
Services: means the storage, visualization, and similar processing of data, which is induced via the KoboToolbox User Account.
Standard Contractual Clauses: means the Controller-to-Processor SCCs or Processor-to-Processor SCCs, as applicable.
Terms of Service: means the KoboToolbox terms of service, available at https://www.kobotoolbox.org/terms/.
User Account: means the KoboToolbox user account in relation to which this DPA is concluded.
User Data: means Personal Data uploaded to a KoboToolbox Server through the KoboToolbox User Account by or with the approval of the User, such as through a survey or other method of data collection, so that this Personal Data can be processed via the Services.

Any terms used in this DPA, which are defined in the GDPR and not otherwise defined in this DPA, shall have the meaning as set out in the GDPR.

3. INSTRUCTIONS OF THE USER

3.1 Kobo shall process User Data only on the User's documented instructions, that may be based on the Controllers instructions if the User acts as a Processor.
3.2 The User instructs Kobo to process User Data to provide the Services as selected by the User and to perform this DPA. The User is not entitled to issue additional instructions, unless agreed by Kobo In Writing.
3.3 Kobo shall inform the User without undue delay if it considers an instruction to violate applicable data protection law. Kobo shall be entitled to suspend the execution of such instruction until the User confirms or changes it. However, the User acknowledges and agrees that given to the nature of the Services, it is unlikely that Kobo will be able to assess whether an instruction violates applicable data protection law.

4. OBLIGATIONS OF KOBO

4.1 Kobo shall not use the User Data for any purpose other than to provide the Services and to implement the User's instructions, unless Kobo is required to do otherwise by applicable law and in compliance with the rest of this DPA, including the Standard Contractual Clauses.
4.2 *Kobo Personnel*
4.2.1 Kobo's personnel engaged in performing processing operations under this DPA are bound to confidentiality and are prohibited from accessing or otherwise processing User Data beyond what is necessary to fulfill the contractual obligations vis-à-vis the User.
4.2.2 Kobo shall familiarize all individuals having access to User Data with the data protection provisions relevant to their work.

4.3 At the User's request, Kobo shall provide, at the User's expense, reasonably assistance in fulfilling the obligations of the User or of the Controller on whose behalf the User acts, as applicable, in accordance with Articles 35 and 36 GDPR.
4.4. If Kobo becomes aware that the User Data is inaccurate, or has become outdated, Kobo shall inform the User without undue delay. However, the User acknowledges and agrees that given to the nature of the Services, it is unlikely that Kobo will become aware that the User Data is inaccurate or has become outdated.

5. OBLIGATIONS OF THE USER

5.1 The User shall ensure compliance with the statutory provisions of the applicable data protection laws, including the lawfulness of its instructions to Kobo.
5.2 The User shall inform Kobo without undue delay in case the User detects any errors or irregularities of the data processing operations which affect the compliance of the Services with the applicable data protection laws.

6. DATA SUBJECT'S RIGHTS

6.1 Kobo shall not directly respond to or meet any data subject's request pursuant to Chapter 3 of the GDPR. If the information provided by the data subject suffices for Kobo to identify the User with reasonable effort as the one the request relates to, Kobo shall refer such request to the User without undue delay. If the User acts as a Processor, it shall forward this request to the Controller on whose behalf the User acts.
6.2 Taking account of the nature of the Services and the information available to Kobo, Kobo shall reasonably assist the User or the Controller on whose behalf the User acts, as applicable, with responding to data subject requests. In any case, the User shall be Kobo's point of contact. The User is aware and acknowledges that all User Data is immediately and freely available to the holder of the User Account for viewing, downloading, editing, or permanent deletion, so Kobo's assistance will usually not be required. Kobo shall not be liable if the User or the Controller on whose behalf the User acts, as applicable, fails to correctly or timely respond to a data subject's request or to respond to a data subject's request at all.

7. TECHNICAL AND ORGANIZATIONAL MEASURES

7.1 Kobo will implement and maintain the technical and organizational measures set out in **Attachment 1** to this DPA.
7.2 The technical and organizational measures are subject to technical progress and further development and Kobo shall periodically monitor the technical and organizational measures. Kobo may amend the technical and organizational measures, provided that the new measures do not fall short of the level of security provided by the specified measures.

8. COMMUNICATION AND ASSISTANCE IN THE CASE OF SECURITY BREACHES

8.1 Kobo shall notify the User without undue delay if Kobo becomes aware of a Security Breach on its end leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to User Data. Notifications made pursuant to this section will describe, to the extent possible, details of the Security Breach, namely details of a contact point where more information can be obtained, a description of the nature of the Security 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 Security Breach, including measures to mitigate its possible adverse effects.
8.2 The User hereby instructs Kobo to take all measures Kobo deems necessary or helpful to secure the User Data and to minimize any possible adverse consequences to the data subjects.
8.3 Taking account of the nature of the Services and the information available to Kobo, Kobo shall, if required, assist the User with notifying the competent supervisory authority and the affected data subjects of the Security Breach or with providing the necessary information to the Controller on whose behalf the User acts, as applicable.

9. SUB-PROCESSING

9.1 Kobo has sub-contracted parts of the processing of User Data to the sub-processor(s) or sub-sub-processor(s) respectively (depending on whether Kobo acts as a Processor or sub-processor) listed in **Attachment 2** ("**Sub-**

Processors"). The User or the Controller on whose behalf the User acts, as applicable, grants a general authorization to Kobo to use this/these Sub-Processor(s).
9.2 Kobo shall notify the User about any intended substitution of or addition to the Sub-Processors at least one month before authorizing any new or substitute Sub-Processor to access User Data, informing the User about the exact name, location, and role of the Sub-Processor. Where the User acts as a Processor, the User is responsible for passing this information on to the Controller at the latest two weeks before the change shall take effect. If the User or the Controller on whose behalf the User acts, as applicable, does not object to the substitution or addition within one month after notification of the User, they will be deemed to have consented to the substitution or addition. If the User or the Controller does not agree to the substitution or addition, their only remedy is for the User to discontinue the use of the Services or otherwise terminate this DPA.
9.3 When engaging Sub-Processors in the processing of User Data on behalf of the User, Kobo shall ensure the fulfillment of the following conditions:
9.3.1 The sub-processing contract reflects the data protection provisions agreed between the User and Kobo in this DPA.
9.3.2 Kobo is responsible for the conduct and performance of the Sub-Processor and will be the User's point of contact regarding the processing of User Data by the Sub-Processor.
9.4 Kobo's Sub-Processors may further sub-contract any or a portion of the processing to sub-contractors ("**Sub-Sub-Processors**"), subject to Kobo's authorization. The Sub-Processor and ultimately Kobo are responsible for the conduct and performance of each Sub-Sub-Processor, and Kobo remains the User's sole point of contact regarding any portion of the Services performed by Sub-Sub-Processors.

10. AUDIT RIGHTS

10.1 The User agrees to exercise its audit right as follows:
10.1.1 At the User's request, Kobo shall provide to User documentation demonstrating Kobo's compliance with its obligations under this DPA.
10.1.2 At the User's request, Kobo shall also, at reasonable intervals or if there are indications of non-compliance, permit and reasonably contribute to audits of its processing activities conducted by the User or a third-party auditor mandated by the User. The User shall provide advance written notice of the audit of at least fifteen (15) days, unless data protection law, a competent data protection authority, or the circumstances of, in particular, a Security Breach require an earlier audit. The User shall conduct the audit during normal business hours, in an expeditious manner, in a way to not unreasonably disrupt Kobo's day-to-day business operations and respecting Kobo's legitimate confidentiality interests.

11. DATA TRANSFERS

11.1 Kobo is a non-profit organization established in the US. The User acknowledges that granting Kobo access to User Data may be a data transfer triggering the applicability of Chapter 5 of the GDPR. For this case, the Parties agree that the KoboToolbox Controller-to-Processor SCCs located at https://www.kobotoolbox.org/assets/files/dpa/Controller_to_Processor_SCC.pdf shall apply where the User acts as a Controller and the KoboToolbox Processor-to-Processor SCCs located at https://www.kobotoolbox.org/assets/files/dpa/Processor_to_Processor_SCC. pdf shall apply where the User acts as a Processor.
11.2 The User acknowledges that, in addition to entering into the Standard Contractual Clauses pursuant to Section 11.1, it may, depending on the circumstances of the case, need to take supplementary measures to ensure that the use of the Services is compliant with Chapter 5 of the GDPR. One of these measures would be to store User Data on the KoboToolbox Server only in an encrypted form. Additional information about using the option to encrypt data can be found at https://support.kobotoolbox.org/encrypting_forms.html. An alternative option may be to restrict the use of the Services to Pseudonymous User Data. Additional information on pseudonymization can be found at https://support.kobotoolbox.org/howto_edit_multiple_submissions.html.

12. DELETION OF USER DATA

When the User deletes User Data or any other data from the User Account, this data is also automatically and irretrievably deleted from the KoboToolbox Server and withdrawn from Kobo's possibility to access this data.

13. LIMITATION OF LIABILITY

Kobo shall only be liable for damages which are covered by the protective purpose of the GDPR, for example claims of data subjects. For all other damages, in particular loss of revenues and profits, frustrated investments and indirect and consequential damages, the liability limitations of the Terms of Service apply correspondingly.

14. TERM AND TERMINATION

14.1 This DPA enters into effect upon being signed and dated by the Parties. Any prior DPA signed by the Parties shall expire at the same time. It automatically terminates when the User deletes the User Account or when Kobo discontinues the provision of the Services.

15. MISCELLANEOUS

15.1 In the event of any contradictions between this DPA and Kobo's Terms of Service, the provisions of this DPA shall take precedence.
15.2 The Standard Contractual Clauses are incorporated in this DPA by reference.
15.3 Kobo may update the terms of this DPA, such as to reflect changes to applicable data protection law or if Kobo decides to modify its service. The User will be informed about the changes to this DPA at least one month in advance.
15.4 Any notices, concerns, or requests of the User regarding this DPA shall be directed to info@kobotoolbox.org.
15.5 Where this DPA provides for Kobo to inform or contact the User, this requirement is met by Kobo contacting the email address provided in the User Account.
15.6 This DPA shall be governed by German law. The exclusive place of jurisdiction shall be Frankfurt, Germany .

User	Kobo
Name:	Name:
Position:	Title:
Date:	Date:

ATTACHMENT 1

TECHNICAL AND ORGANIZATIONAL MEASURES

Kobo's administrative, physical, organizational and technical measures shall include, at a minimum, the following:

1. CONFIDENTIALITY

1.1 Physical Access Control

1.1.1 Physical access control measures, amongst others, are implemented by Kobo's Sub-Processor Amazon Web Services. For details about the Sub-Processor's technical and organizational measures see https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf and https://aws.amazon.com/compliance/data-center/controls/.

2. ELECTRONIC ACCESS CONTROL

2.1 All accounts are password-protected. Users are provided visual feedback about the complexity of their password, which encourages them to select a stronger password when applicable. Passwords are stored fully encrypted on the KoboToolbox Server, utilizing the default open-source framework provided by Django, which uses the PBKDF2 algorithm with a SHA256 hash.

2.2 All database content is encrypted at rest (database-level encryption).

2.3 Users can choose to enable encryption of their project data (data-level encryption) which renders it inaccessible at all stages of data processing and requires a private key to decrypt it locally.

2.4 Users found to abuse the use of their API keys by overburdening the KoboToolbox Server may be suspended or their account may be restricted.

3. INTERNAL ACCESS CONTROL

3.1 Only authorized system administrators can access the KoboToolbox Server. They may only do so for the express purpose of updating installed software or maintaining the server infrastructure.

3.2 System administrators require additional authentication, including SSH Public Key authentication, for accessing the KoboToolbox Server and two-factor authentication for accessing control panels provided by Sub-Processor.

3.3 Sub-Processor provides a log of actions taken in the AWS Console. For SSH connections into the individual KoboToolbox Server instances, Kobo collects " system access events" by SSH key, which can then be matched to the authorized users.

3.4 Only explicitly listed IP addresses are allowed to connect to production servers.

4. DATA PROTECTION BY DESIGN AND DEFAULT

4.1 Only limited information is required for creating a KoboToolbox user account.

4.2 Kobo staff are required to abide by the rules set out in Kobo's privacy policies.

4.3 Data processed on behalf of the user is not accessed by Kobo.

4.4 Users are provided the option of applying advanced encryption. This ensures that data is encrypted using a public key before it is submitted to a KoboToolbox Server, and that it can only be decrypted with a private key on a local computer. KoboToolbox also offers the possibility of removing information in bulk once it has been collected, facilitating the pseudonymization of Personal Data (through the removal of identifiers).

4.5 See above sub-section "Electronic Access Control" for details about visual feedback on password complexity.

5. INTEGRITY

5.1 Data Transfer Control

5.2 All data in transit is protected using SHA-256 with RSA encryption.

5.3 Data Entry Control

5.3.1 For using the Services, personal data is entered by the user. HTTP access logs include the authenticated user for most requests.

6. AVAILABILITY AND RESILIENCE

6.1 Kobo conducts daily backups of all databases to a separate, remote location. In case of a critical outage, all user data will be restored from the most recent backup as quickly as possible.

6.2

Firewalls block all external requests except for SSH connections from a small list of explicitly allowed IP addresses. Public HTTP and HTTPS traffic cannot connect directly to the KoboToolbox Server, instead it is serviced by the Sub-Processor's load balancer, which then forwards it to Kobo's front-end servers.

6.3 KoboToolbox Servers are configured to use multiple concurrently running server instances and are set to increase the number of such instances to avoid the impact of any localized failures. In case of any other failures that threaten continuous operation of critical aspects of the KoboToolbox software, system administrators stand by to intervene on short notice to restore service.

6.4 Kobo's reporting procedures include automated alerts, escalation of user-reported issues, and self-noticed problems by staff.

6.5 Contingency plans include the availability of multiple people in multiple geographic locations who can respond to emergencies and restore service.

6.6 KoboToolbox Servers have the demonstrated ability to continue operating in a degraded state, receiving submissions while simultaneously recovering lost projects/submissions via to-the-minute point-in-time recovery (PITR).

7. ASSISTANCE IN FULFILLING DATA SUBJECT'S REQUEST

7.1 All User Data is immediately and freely available to the holder of the User Account for viewing, downloading, editing, or permanent deletion.

ATTACHMENT 2
LIST OF SUB-PROCESSORS

Sub-Processor (full legal name)	**Address/country**	**Description of services provided by the Sub-Processors**
Amazon Web Services	Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 United States	Cloud services