

# Data Protection Agreement

**Version:** Choose an item.

**Operation:**

Click or tap here to enter text.

**Partner Reference Number (optional):**

Click or tap here to enter text.

**Partnership Framework Agreement Number:**

Click or tap here to enter text.

**Cloud ERP Partner Number:**

Click or tap here to enter text.

## Parties

UNHCR	The Partner
The Office of the United Nations High Commissioner for Refugees	Click or tap here to enter text.  <b>UN Partner Portal Reference Number:</b> Click or tap here to enter text.

### Signatures

Signed by the duly authorized signatories of the parties:

**UNHCR**

**The Partner**

Name: Click or tap here to enter text.

Name: Click or tap here to enter text.

Position: Click or tap here to enter text.

Position: Click or tap here to enter text.

Email: Click or tap here to enter text.

Email: Click or tap here to enter text.

Date: Click or tap to enter a date.

Date: Click or tap to enter a date.

## Duration

**Start Date:**

Click or tap to enter a date.

**End Date:**

Click or tap to enter a date.

# Our Agreement

## 1. About This Data Protection Agreement

- 1.1. DPA. This Data Protection Agreement (**DPA**) governs the processing of Personal Data as may be required under the parties' partnership, and forms part of the Agreement (as defined in the Partnership Cover Sheet).
- 1.2. Other partner agreements. A Partnership Cover Sheet is a separate agreement that the parties will enter into, which will describe the partnership at a high level. The parties may also enter into one or more Project Workplans that describe the scope and details of a Project for which the parties agree to collaborate to deliver. A Project Workplan will set out additional data protection provisions that are required for a certain Project, and the roles of the parties when Processing Personal Data as referred to in Article 2.1 below.

## 2. Defined Terms

Defined terms in this DPA are set out below in **bold**. Any capitalized term that is not defined in this DPA is defined in the Agreement.

- 2.1. **Data Controller** means the party or parties that determine(s) the purposes and essential means of Processing Personal Data.
- 2.2. **Data Processor** means a natural or legal person that carries out Processing on behalf of the Data Controller.
- 2.3. **Data Protection Impact Assessment** means a tool and a process for assessing potential risks, harm and benefits to Data Subjects to protect their Personal Data and identify mitigating measures.
- 2.4. **Data Protection Laws** means the laws related to Data Protection applicable to the Partner in connection with its Processing of Personal Data under this DPA.
- 2.5. **Data Subject** means an individual whose Personal Data is subject to Processing.
- 2.6. **Data Subject Request** means a request from a Data Subject (or their authorized representative) relating to the Processing of Personal Data under this Agreement to assert their rights and make associated requests (including complaints or inquiries).
- 2.7. **Personal Data** means any information relating to an identified or identifiable Data Subject.
- 2.8. **Personal Data Breach** means a breach of information security leading to the accidental or illegitimate destruction, loss, alteration, disclosure, or access of Personal Data.
- 2.9. **Processing** means any operation or set of operations (whether automated or not) that are performed on Personal Data including collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure, access, transfer, dissemination, correction or destruction.
- 2.10. **Sub Processor** means any person or organization that carries out Processing on behalf of the Data Processor with the prior authorization of the Data Controller.

- 2.11. **UNHCR Data Protection Standards** means the data protection principles, namely fair and legitimate processing, purpose specification, proportionality and necessity, retention limitation, accuracy, confidentiality, security, transparency, accountability, the rights of data subjects and operational standards as set out by UNHCR's General Policy on Personal Data Protection and Privacy.

## General Obligations

### 3. Obligations

- 3.1. Roles of the parties. Depending on whether a Controller-to-Controller or a Controller-to-Processor relationship is selected under a Project Workplan, the parties agree to comply with the relevant obligations for those roles as set out in this DPA.
- 3.2. Personal Data Protection Standards. If Personal Data is Processed under the Agreement, the parties agree to respect and implement the UNHCR Personal Data Protection Standards.
- 3.3. Duration of obligations. The obligations and restrictions set out in this DPA are effective for the duration of the Agreement (including any mutually agreed extensions), unless mutually agreed otherwise in writing.
- 3.4. Survival. Any term of this DPA which is intended to survive termination or expiration of this DPA, or the Agreement will remain in full force and effect, including, but not limited to, Articles 3.5-3.15, Article 5.2, Article 7, Article 6.1, Article 11 and Article 12.
- 3.5. Security. The Partner agrees to
- implement appropriate measures to ensure an adequate level of security to protect Personal Data against accidental or unauthorized destruction, loss, access, use, alteration or dissemination, and against all other unauthorized forms of Processing,
  - at a minimum, comply with the data protection and information security measures identified through the partner DPIS capacity assessment,
  - comply with any additional information security requirements (such as certifications) set out in a Project Workplan, if any,
  - if applicable, implement the mitigating measures and risk treatments identified in its self-assessment, specified in the Risk Register as a component of the Project Workplan, and
  - periodically assess the effectiveness of the technical and organizational measures to maintain an appropriate level of security of all Personal Data.
- 3.6. Physical files. The Partner agrees to store all physical copies of Personal Data in secured filing rooms at its premises.
- 3.7. Audits. For audits conducted under the Partnership Framework Agreement by UNHCR's auditors, the relevant provision in the PFA Terms shall apply. Any sharing of Personal Data for other audits must comply with the Data Protection Principles, including necessity and proportionality principles.
- 3.8. Personal Data Breaches. The Partner agrees to notify UNHCR without undue delay, and in any event within 48 hours, of any actual or suspected Personal Data Breach. In these situations, the parties agree to consult to address and resolve the Personal Data Breach, including

communicating the Personal Data Breach to Data Subjects and implementing UNHCR's recommended mitigation measures.

- 3.9. Transferring Personal Data. Any Personal Data transfers between UNHCR and the Partner must be completed through a mutually agreed and secure Data Transfer Method, as specified in a Project Workplan.
- 3.10. Delivery of Personal Data to UNHCR. Where the Project [as set in the Project Workplan] requires the Partner to collect and/or otherwise process Personal Data which will be shared with UNHCR, the Partner shall deliver the relevant Personal Data to duly authorized representatives of UNHCR or as otherwise directed by UNHCR.
- 3.11. UNHCR Dataset Anonymization. Where the Partner provides to UNHCR, pursuant to the Project Workplan or otherwise under the Partnership Framework Agreement, surveys, assessments, censuses, administrative registers, studies or other similar reports, it is agreed that UNHCR may (i) anonymize the Personal Data contained in such reports, (ii) display the anonymized data in the form of datasets or similar information products and (iii) share such datasets and products under licensing (including open source licensing) or other arrangements.
- 3.12. Respecting UNHCR's privileges and immunities. The Partner acknowledges that Personal Data **processed** on behalf of UNHCR or shared by UNHCR with the Partner is subject to UNHCR's privileges and immunities. This Personal Data is inviolable and cannot be disclosed, provided or otherwise made available to, or searched, confiscated or otherwise be interfered with by any person, unless UNHCR expressly agrees in writing. As a result, the Partner may disclose such Personal Data if it is required by law and only to the extent required by law, however the Partner must first provide UNHCR with sufficient written notice of any request for disclosure so UNHCR can take protective measures or other appropriate actions before the Partner makes a disclosure.
- 3.13. Prohibited disclosures. Personal Data controlled by UNHCR must not be disclosed to authorities or agents of the country of origin of Data Subjects. The only exception to this is if a tripartite agreement for voluntary repatriation has been agreed with the support of UNHCR and with the consent of the Data Subjects concerned.
- 3.14. Compliance. The Partner will ensure that Partner Personnel and the personnel of third parties authorized to process personal data will comply with their respective obligations under Data Protection Laws and this DPA. UNHCR will ensure that its personnel will comply with its obligations under the UNHCR Data Protection Standards and this DPA.
- 3.15. Other restrictions. The Partner will refrain from Processing Personal Data in a manner that will adversely affect UNHCR or the United Nations.

## 4. Notices

Any formal notices which must be given under this DPA must be delivered in writing to the signatory to a Project Workplan.

## Controller to Processor (C2P) Relationship

This Part applies if a Project Workplan identifies the parties' relationship as Controller to Processor. UNHCR is the Data Controller and the Partner is the Data Processor.

## 5. Controller to Processor Obligations

5.1. The Partner's general obligations. The Partner agrees to:

- only Process Personal Data in accordance with this DPA and UNHCR's instructions, and only insofar as necessary to achieve the purposes specified under the applicable Project Work plan,
- not sell or otherwise use Personal Data for any commercial purposes,
- restrict Partner Personnel's access to Personal Data on a need-to-know basis, and ensure that such Partner Personnel are sufficiently trained in the handling and Processing of Personal Data,
- inform UNHCR without undue delay if it is unable to comply with any instructions from UNHCR, and in this case, UNHCR may suspend or terminate the relevant part of the Project impacted by the non-compliance and seek a refund of all reasonable costs,
- at UNHCR's request and without undue delay, provide UNHCR with reasonable assistance for Data Protection Impact Assessments,
- if requested, provide UNHCR with relevant information to demonstrate the Partner's compliance with Data Protection Laws and this DPA,
- allow for audits of its compliance with this DPA at UNHCR's reasonable request, provided that audits are limited to once a year and during business hours except in the event of a Personal Data Breach, and
- only Process Personal Data in a country that is a signatory to the 1946 Convention on the Privileges and Immunities of the United Nations, unless expressly authorized to do otherwise by UNHCR.

5.2. Data Subject Requests. The Partner agrees to:

- upon UNHCR's request, assist UNHCR with responding to any Data Subject Requests received by UNHCR,
- inform UNHCR without undue delay of any Data Subject Request and promptly share all relevant information with UNHCR to ensure the timely resolution of a Data Subject Request, and
- not respond to a Data Subject Request within the scope of this DPA, without UNHCR's prior instruction.

## 6. Sub Processing

6.1. Use of Sub Processors. The use of Sub Processors by the Partner is subject to UNHCR's review and approval. All permitted Sub Processors are listed in a Project Workplan.

6.2. Sub Processor obligations. The Partner agrees to:

- require its Sub Processors to comply with terms equivalent to its obligations in this DPA by means of a written agreement,
- ensure appropriate safeguards are in place before transferring Personal Data to a Sub Processor, and
- remain liable for any acts, errors or omissions of its Sub Processors as if they were a party to this DPA.

- 6.3. Approvals. The Partner may appoint new Sub Processors only if it notifies UNHCR at least 4 weeks in advance in writing. UNHCR may reasonably object to any proposed Sub Processor by notifying the Partner in writing and, if the parties are unable to agree on a solution within a reasonable time, either party may terminate this DPA by providing the other party with written notice.

## 7. Retention (C2P)

- 7.1. Return and deletion. At UNHCR's request or after the Agreement terminates or expires, the Partner agrees to delete all the Personal Data it processed or, if requested by UNHCR, return all the Personal Data processed under this Agreement (including electronic, digital, physical, online, archived or other forms) without undue delay, or in any case within 60 days, and confirm the deletion of Personal Data in writing to UNHCR.
- 7.2. Retention. If the Partner cannot delete Personal Data within the above timeframe, it must inform UNHCR immediately. The Partner can only retain Personal Data for a longer period if:
- retention is required by the Data Protection Laws, in which case the Partner must:
    - ensure the continued confidentiality of Personal Data,
    - inform UNHCR about the extended retention period in writing without undue delay,
    - minimize retained Personal Data to only what is necessary,
    - if possible and after consulting with UNHCR, irreversibly anonymize retained Personal Data, and
    - ensure security measures set out in this DPA remain in place to protect retained Personal Data.

## Controller to Controller (C2C) Relationship

This Part applies if a Project Workplan identifies the parties' relationship as Controller to Controller. UNHCR is a Data Controller, and the Partner is a Data Controller.

## 8. Obligations of the Parties

- 8.1. Mutual obligations. The parties agree to:
- collect, share or otherwise Process Personal Data in accordance with this DPA,
  - maintain appropriate technical and organizational measures following applicable standards to ensure the confidentiality of all Personal Data and the prevention of a Personal Data Breach,
  - work together as appropriate to resolve a Personal Data Breach relating to the Project if one occurs,
  - inform each other if a Data Protection Impact Assessment is required and cooperate and provide reasonable support to each other in order to complete it,
  - restrict any third party's access to Personal Data unless their access is required to perform duties for a Project. Those individuals must be committed to comply with the requirements of this DPA and the UNHCR Data Protection Standards,
  - provide Data Subjects with information and notices that comply, at a minimum, with the requirements set out in the UNHCR Data Protection Standards, and
  - where applicable, anonymize Personal Data in accordance with standards equal to or exceeding UNHCR's statistical disclosure control standards.

8.2. Partner's responsibilities. The Partner agrees to:

- comply with its obligations under the Data Protection Laws without compromising any obligations that may be more stringent under this DPA,
- not Process Personal Data in a manner that is incompatible with the purposes specified under the applicable Project Workplan or UNHCR's mandate,
- promptly inform UNHCR if it becomes impossible for the Partner to perform its obligations under this DPA, and
- if requested by UNHCR, share Personal Data as agreed by the parties, in order for UNHCR to carry out its mandate.

8.3. Requests for Additional Data. If the Partner wishes to obtain additional information or Personal Data from UNHCR, it must submit a written request which clearly explains the specific reasons why additional Personal Data should be shared with the Partner to implement the Project. UNHCR will consider the request taking into account UNHCR's mandate, rules, and its privileges and immunities. Any additional Personal Data UNHCR may share with the Partner for a Project will be in accordance with this DPA.

## 9. Onward Sharing

- 9.1. If required in the Project Workplan, the Partner is authorized to onward share with the third parties specified in the Project Workplan ("contracted third parties") the Personal Data contained in data sets shared by UNHCR. Any onward sharing is subject to compliance by the Partner with UNHCR Data Protection Standards, in particular purpose limitation, necessity and proportionality.
- 9.2. Should the above-mentioned contracted third parties be replaced in the course of the implementation of the Project or a new contracted third party be added, the Partner must inform UNHCR accordingly, including the written details of any new contracted third party.
- 9.3. The Partner shall ensure that any sharing of Personal Data with a contracted third party is subject to a contractual obligation to comply with the Partners' obligations under this DPA.

## 10. Data Processors

The Parties agree that its Data Processors, if any, will Process Personal Data only under its instructions.

## 11. Data Subject Requests

11.1. Data Subject Requests. Each party agrees to:

- respond to any Data Subject Request it receives that is connected to the Processing of Personal Data undertaken by that party and to do so in accordance with
  - the UNHCR Data Protection Standards, in the case of UNHCR,
  - Data Protection Laws, in the case of the Partner, and
  - mutually agreed arrangements, if any, for responding to Data Subject Requests,
- cooperate with each other and provide reasonable assistance to allow the other party to respond to a Data Subject Request, and
- maintain a record of Data Subject Requests it receives for accountability purposes.



11.2. Resolving Data Subject concerns. If UNHCR is notified by a Data Subject that they are dissatisfied in how their Data Subject Request was resolved by the Partner, the Partner agrees to provide UNHCR with relevant information about the resolution process.

## 12. Retention (C2C)

After the Agreement terminates or expires, the Partner shall retain Personal Data for no longer than necessary for the purposes for which it was collected or shared in connection with the Project, and for such additional periods as required for audit purposes or where otherwise required by law. The Partner shall ensure that the security measures set out in this DPA remain in place to protect retained Personal Data.

FOR INFO ONLY