

[UNICEF HEADQUARTERS / COUNTRY OFFICE LETTERHEAD]

[Date]

[IMPLEMENTING PARTNER FULL LEGAL NAME]

[IMPLEMENTING PARTNER ADDRESS]

PCA: [____]; no [____]

Programme Document Title: [____]; eTools Reference no. [____]

Collection of, Access to and Processing of Personal Data - Confidentiality Obligations

Dear [_____]

We refer to the Programme Cooperation Agreement (“PCA”) and Programme Document (“PD”) identified in the Annex to this Agreement between the United Nations Children’s Fund (“UNICEF”) and your organization, [IMPLEMENTING PARTNER FULL LEGAL NAME] (the “Implementing Partner”, “Partner” or “you”). To facilitate the fulfillment of your responsibilities under the PCA and the implementation of the parts of the Programme assigned to you under the PD, UNICEF instructs you to collect, access, use and/or otherwise process (collectively, “processing”) certain personal data specified in the Annex to this Agreement (collectively, the “Data Sets”).

This letter (together with the Annex attached to this letter, this “Agreement”) is to confirm that UNICEF instructs you to process the Data Sets on the conditions set out below in this Agreement and in line with any additional documented instructions by UNICEF. All capitalized terms used but not defined in this Agreement have the meaning assigned to them in the Annex to this Agreement or in the PCA. The terms contained in this Agreement are in addition to, and not in replacement of, the terms of the PCA and PD. This Agreement, the PCA and PD will be construed and interpreted as complementary of one another.

1. Data Rights. You accept and acknowledge that the Data Sets are proprietary to UNICEF or the relevant third parties identified in the Annex to this Agreement (collectively, the “Third Parties”) as identified in the Annex and that you will not claim any ownership or any other rights in the Data Sets.
2. Confidential Information. For the purposes of Section 8.1 of the General Terms and Conditions of the PCA, the Data Sets are deemed to be UNICEF’s confidential information and all of the obligations in respect of such confidential information set out in Section 8 of the General Terms and Conditions of the PCA apply to your processing of the Data Sets. You will take the Additional Security Measures described in the Annex to this Agreement.
3. Filing System and Access. Your processing of the Data Sets is limited to the Data Sets. For Data Sets that you will be collecting, you will collect, store and otherwise process the Data Sets through the Filing System described in the Annex to this Agreement. For Data Sets that you will be provided access to, UNICEF will make the Data Sets available to you through the Access Modality described in the Annex to this Agreement. To the extent that such access is provided through access credentials (such as password protected means), you agree to treat all such access credentials as Confidential Information and to take all reasonable precautions to

FINAL DRAFT 2023.1.25 (updated and adjusted to the new PCA template issued in Jan 2023)
For Information Only (DPA is filled by UNICEF and Share with Partner to complete)

prevent unauthorized or accidental disclosure of such access credentials. You will not share such access credentials with any person except your Authorized Data Processor Personnel.

4. Permitted Purpose Only. You will only use the Data Sets for the Permitted Purpose specified in the Annex to this Agreement and no other purpose. You will not use the Data Sets, and you will ensure that your Authorized Data Processor Personnel and Authorized Data Sub-processors (if any) do not use the Data Sets, for any other purposes, including (but not limited to) developing analyses, publications, product or service offerings to customers or other third parties, without the express prior written consent of UNICEF and, if relevant, the Third Party holder of the Data Sets.
5. Authorized Data Processor Personnel. Access to the Data Sets under this Agreement is limited exclusively to your Personnel that need to be involved for purposes of performing obligations under this Agreement ("Authorized Data Processor Personnel"). You will keep a list of your Authorized Data Processor Personnel that has access to the Data Sets and you will share that list upon request with UNICEF. You will be responsible for the compliance by your Authorized Data Processor Personnel with the conditions on access set out in this Agreement.
6. Authorized Data Sub-processor. Only those of your sub-contractors or affiliates that are approved by UNICEF and that sign a separate agreement with you substantially consistent with the terms of this Agreement can receive access to the Data Sets ("Authorized Data Sub-processor"). You will impose the same requirements relating to data protection and non-disclosure as are imposed upon you under this Agreement to the Authorized Data Sub-processors and you will remain responsible for compliance with such requirements by such Authorized Data Sub-processors.
7. Compelled Disclosure. If you or any of your Authorized Data Sub-processors receive a request for disclosure of any of the Data Sets under any judicial or law enforcement process, before you make the requested disclosure, you will give UNICEF (to the UNICEF Data Manager identified in the Annex) sufficient notice of the request prior to any disclosure being made in order to allow UNICEF to have a reasonable opportunity to take protective measures or take such other action as may be appropriate and will notify the relevant authority of this.
8. Data Protection Standards. You confirm that you have a data protection policy in place that is consistent with UNICEF's Policy for Personal Data Protection and meets all applicable data protection standards and legal requirements and that you have uploaded it on your UN Partner Portal profile. You will apply such policy in the storage, processing, retention and destruction of the Data Sets. If you do not have your own data protection policy in place or if your policy does not meet at least the protection standards of UNICEF's Policy for Personal Data Protection, you will comply with and apply UNICEF's Policy for Personal Data Protection in the performance of your obligations under this Agreement.
9. Safeguards and Control of Data. You will implement appropriate organizational, administrative, physical and technical safeguards and procedures to protect the security of the Data Sets, including against or from accidental or unauthorized destruction, loss, alteration, disclosure, access, or unplanned loss of availability in line with Annex 3.
10. Security Incident. You will immediately notify UNICEF (to the UNICEF Data Manager identified in the Annex) if there is any actual, suspected or threatened unauthorized or accidental disclosure of the Data Sets or other Security Incident affecting the Data Sets and you will implement all necessary damage mitigation and remedial actions as per your security incident

FINAL DRAFT 2023.1.25 (updated and adjusted to the new PCA template issued in Jan 2023)
For Information Only (DPA is filled by UNICEF and Share with Partner to complete)

management procedure and UNICEF's instructions. UNICEF will report the incident through the required channels in accordance with the UNICEF Procedure for Personal Data Breach. For these purposes, "Security Incident" means a breach of security leading to the accidental, or unauthorized destruction, loss, alteration, disclosure, access, or unplanned loss of availability of personal data processed or stored by the Partner.

11. Access Period; Termination. The access and permission given to you under this Agreement is limited to the Access Period. Unless otherwise expressly stated in the Annex, the Access Period is defined as the duration of the relevant Programme Document. UNICEF may, but is not obliged to, agree to extend the Access Period upon your request. If you or any of your Authorized Data Processor Personnel or Authorized Data Sub-processors breach any of the conditions set out in this Agreement, UNICEF may terminate your access to the Data Sets and withdraw its permission for you to continue to process the Data Sets with immediate effect. UNICEF may also terminate the PCA in accordance with Section 13.1 of the General Terms and Conditions of the PCA.
12. Data Subject's Right to Information and Access Requests. If you or any of your Authorized Data Sub-processors receive a request from a data subject to access, rectify or delete its personal data or obtain information about the data processing, you will immediately notify UNICEF (to the UNICEF Data Manager identified in the Annex) of such request. You will provide your reasonable cooperation to UNICEF to address such requests in accordance with the mechanisms set out in Annex 2 of the UNICEF Policy on Personal Data Protection.
13. Return / Destruction of Data. Unless otherwise expressly indicated in the Annex to this Agreement, when the Access Period ends, you will transfer and return to UNICEF all the Data Sets, or, at UNICEF's option, irrevocably destroy by applying industry standards all copies of the Data Sets held by you and your Authorized Data Processor Personnel or Authorized Data Sub-processors and confirm such destruction to UNICEF in writing. For the avoidance of doubt, the requirement to destroy the Data Sets does not apply to Data Sets held within a UNICEF Filing System.
14. Survival of Obligations. Your obligations under this Agreement will survive the expiry of the Access Period or the earlier termination of this Agreement or the expiry or earlier termination of the PCA.
15. Disagreements. Any disagreements or conflicts relating to this Agreement or the Data Sets will be addressed in accordance with Article 12 of the PCA.

Nothing in or related to this Agreement will be treated as a waiver of the privileges and immunities of the United Nations and its subsidiary organs, including UNICEF.

Please confirm your agreement with the conditions set out in this Agreement, on behalf of your organization, by signing, dating, and returning to us the enclosed copy of this Agreement. As soon as we receive the copy of this Agreement countersigned by you, this Agreement will come into effect.

We look forward to working with you for the implementation of the Programme.

Yours sincerely,

FINAL DRAFT 2023.1.25 (updated and adjusted to the new PCA template issued in Jan 2023)
For Information Only (DPA is filled by UNICEF and Share with Partner to complete)

[_____]
[Name]
[Title]

CONFIRMED AND AGREED ON BEHALF OF [FULL LEGAL NAME OF IMPLEMENTING PARTNER]:

_____ Date: _____

Name:
Title:

ANNEX 1
Personal Data Processing Details

[Instruction: Before entering into this Data Processing Agreement, you need to ensure that the personal data processing of the Implementing Partner for the purposes of the project complies with the UNICEF Policy for Personal Data Protection. If UNICEF acts as controller and the processing is likely to involve high risks to the rights and freedoms of the data subjects, in particular when new technologies are involved, a Data Protection Impact Assessment (DPIA) must be conducted prior to the processing. Even if you are not obliged under the Policy to conduct a DPIA, you may conduct such assessment. Risk assessment findings provide valuable information regarding appropriate project mitigations and safeguards to be implemented to ensure compliance with UNICEF’s Policy on Personal Data Protection. You will find guidance on the DPIA on the data protection website of Data for Children or you can request support through the [Evidence Helpdesk](#)]

This Annex applies to, and forms an integral part of, the Data Processing Agreement between UNICEF and the Partner named below under the Programme Cooperation Agreement (PCA) referenced below.	
1. OVERVIEW	
Partner	[FULL LEGAL NAME] [ADDRESS]
PCA	PCA between UNICEF and the Implementing Partner dated [___] with PCA no [_____]
Programme	[Instructions: Include the title and brief description of the Programme that is being supported through this data processing as well as Programme Document reference number.]
Partner Data Protection Policy	[Instructions: Include the title of the Partner’s data protection policy. Also make sure that the Partner uploads its policy to the organization’s UN Partner Portal profile as per Section 8 above. If the Partner does not have a data protection policy, or its data protection policy does not meet at least the standards of UNICEF Policy on Personal Data Protection, the Implementing Partner will have to follow UNICEF’s Policy on Personal Data Protection as per Section 8 above.] [TITLE OF POLICY]; a copy of which [can be found at [<i>include WEB LINK</i>]; and has been uploaded to the UN Partner Portal].
UNICEF Data Manager	[include name and contact details]
Partner Data Manager	[include name and contact details]
Access Period	[Instructions: Specify the duration of the collection, access, use and processing of the data. This is typically the entire duration of the relevant Programme Document. The Access Period may differ depending on the Data Set. Adapt as appropriate.] [The term of the relevant Programme Document.] OR [From [dd/mm/yr] to [dd/mm/yr]]

FINAL DRAFT 2023.1.25 (updated and adjusted to the new PCA template issued in Jan 2023)
For Information Only (DPA is filled by UNICEF and Share with Partner to complete)

UNICEF Ethical Review Committee/Board	[Instructions: If your project requires ethical review (i.e., meets the criteria noted in Instruction 3 of the UNICEF Procedure for Ethical Standards and is not a part of routine data collection for programme implementation) include the name of the ethical review board, committee or panel that reviewed the evidence programme and the date of sign off and authorisation to proceed. If this is not applicable for your project, simply add “Not applicable” in this column.]
2. DATA SETS	
[Instructions: For each data set, fill out the required information below. Add more lines below depending on how many data sets are involved. The processing of personal data must be relevant, limited and adequate to what is necessary in relation to the purpose(s) specified for processing. So, it is important to only share the data that the Partner actually needs to do its work under the Programme. In some cases, this may only be a subset of an original data set. If UNICEF is sharing data that we received from a third party (e.g. the government, private sector partner or another implementing partner), then make sure you have the required permission to share that data and that any conditions/restrictions on sharing are appropriately reflected in this Annex. Include a detailed description of each data set or components of data sets]	
DATA SET #1	
Data Set Originator	[Instructions: describe where the data comes from (e.g., collected by UNICEF or Partner OR received from [Third Party name])]
Description of Data Set	[overall description]; [specific data points to be shared/collected];[type of data subjects, i.e. children, etc];[format of data content (e.g., paper, digital)]; [time period of data set/date of data collection]; [geographic range]; [other relevant features of data set]
Permitted Purpose for Data Processing	[Instructions: Describe the purpose(s) for which Personal Data may be processed in order for the Partner to fulfill its responsibilities in the manner specified in the Programme Document. Be as specific as possible. For example: For a cash assistance intervention: “For the purposes of registering the individual as a beneficiary of the cash assistance programme and providing further follow-up and support as part of grievances management and monitoring as described in the Programme Document attached to the PCA.]
Conditions/Restrictions on Data Processing	[Instructions: Please include here any restrictions/conditions that carry forward from any agreement we have with a third-party from which we received the data.]
Access Modality	[Instructions: Describe here how the Partner will receive access to the data. For example: the data will be sent to the Partner’s Data Manager through a password protected link/site. The password will be sent separately via email to the Partner’s Data Manager.]
Filing System	[Instructions: Specify whether the system for storing the data will be a UNICEF Filing System (see Policy) or an Implementing Partner or other system. Be as specific as possible. For example: For a cash assistance programme: “UNICEF’s Humanitarian cash Operations and Programme Ecosystem (HOPE) in [COUNTRY]”.]
DATA SET # 2	

FINAL DRAFT 2023.1.25 (updated and adjusted to the new PCA template issued in Jan 2023)
For Information Only (DPA is filled by UNICEF and Share with Partner to complete)

Data Set Originator	[Instructions: describe where the data comes from (e.g., collected by UNICEF or Partner OR received from [Third Party name])]
Description of Data Set	[overall description]; [specific data points to be shared/collected];[type of data subjects, I.e. children, etc];[format of data content (e.g., paper, digital)]; [time period of data set/date of data collection]; [geographic range]; [other relevant features of data set]
Permitted Purpose for Data Processing	[Instructions: Describe the purpose(s) for which Personal Data may be processed in order for the Partner to fulfill its responsibilities in the manner specified in the Programme Document. Be as specific as possible. For example: For a cash assistance intervention: “For the purposes of registering the individual as a beneficiary of the cash assistance programme and providing further follow-up and support as part of grievances management and monitoring as described in the Programme Document attached to the PCA.]
Conditions Restrictions on Data Processing	[Instructions: Please include here any restrictions/conditions that carry forward from any agreement we have with a third-party from which we received the data.]
Access Modality	[Instructions: Describe here how the Partner will receive access to the data. For example: the data will be sent to the Partner’s Data Manager through a password protected link/site. The password will be sent separately via email to the Partner’s Data Manager.]
Filing System	[Instructions: Specify whether the system for storing the data will be a UNICEF Filing System (see Policy) or an Implementing Partner or other system. Be as specific as possible. For example: For a cash assistance programme: “UNICEF’s Humanitarian cash Operations and Programme Ecosystem (HOPE) in [COUNTRY]”.]
3. DATA COLLECTION	
[Instructions: if the Partner will not collect new Personal Data as part of the work under the Programme, please delete this section]	
[Instruction: If CONSENT is not the legitimate basis for data collection and processing, please contact the Evidence Helpdesk]	
Consent Form	<p>The legal basis for collecting new Personal Data will be: CONSENT.</p> <p>After having provided the required information to the data subjects in line with the next section, the Partner will ensure that appropriate consent forms are obtained by it for each data subject for which the Partner will collect data.</p> <p>The consent form to be used for the processing of data under the programme [has been approved by UNICEF and the Partner and is attached as Annex 2] OR [is subject to UNICEF’s approval before use].</p> <p>The consent form will clearly indicate that the Partner is collecting the data on behalf of UNICEF and that the data will be shared by the Partner with UNICEF [and the Government] only for the Permitted Purpose.</p> <p>The consent form will be collected and stored as follows: <i>[specify whether it is paper form, mobile/tablet/other device, etc.]</i></p> <p>[Consent will be recorded in a secure Filing System.]</p> <p>If a data subject raises concerns of providing his/her data and consent, the Partner will not try to convince the individual to provide the consent, but instead inform</p>

FINAL DRAFT 2023.1.25 (updated and adjusted to the new PCA template issued in Jan 2023)
 For Information Only (DPA is filled by UNICEF and Share with Partner to complete)

	that UNICEF takes any concerns seriously and will provide professional support and immediately notify UNICEF.
Information about the Processing of Personal Data (Privacy Notice)	<p>When collecting Personal Data, the Partner will inform the individuals (data subjects) about the personal data processing, in line with Annex 2, including</p> <ul style="list-style-type: none"> - the legal basis for processing their data (CONSENT) - The alternatives, if a beneficiary does not want to provide his/her consent - the specified purpose for which the data will be used - who will obtain access to the data - what measures are taken to keep the data secure - when the data will be deleted and - what rights the individual has on the data, namely right to access, rectify and delete the data and where to request these rights.
4. SECURITY MEASURES	
Additional Security Measures	<p>[Instructions: Include here any specific precautions you would like the Partner to take in the relevant context which go beyond the IT security annex for each Data Sets.]</p> <p>Remember some data is particularly sensitive as further defined in the UNICEF Data Protection Policy. Particular attention should be given to data access and security measures when dealing with particularly sensitive personal data. We strongly encourage you to reach out early to discuss your plans with the Evidence Helpdesk, to address the necessary data security measures required by your office.]</p>
4. DATA TRANSFER, RETENTION, AND DESTRUCTION	
Transfer of Data Sets	[Instructions: If the data is being collected in a non-UNICEF Filing system and/or delivery of cleaned up data sets to UNICEF is part of the deliverables as set out in the Programme Document, then specify that here providing details of what the data set should cover and what format the data set should be provided in, and specify the mode for transfer of those data sets to UNICEF and any other relevant requirements.]
Retention / Destruction of Data	[Instructions: If the Partner is collecting data in a UNICEF Filing System, then this row is not applicable. If the data is being collected in a non-UNICEF Filing system, then specify what happens to the data at the end of the Access Period.]

FINAL DRAFT 2023.1.25 (updated and adjusted to the new PCA template issued in Jan 2023)
For Information Only (DPA is filled by UNICEF and Share with Partner to complete)

ANNEX 2
Form of Consent to be provided by Data Subjects

ANNEX 3
Information Security

This Information Security Annex forms an integral part of the Agreement to which it is attached. Any capitalized terms not otherwise defined herein will have the meanings set forth in the Agreement.

In addition to requirements set forth in the Agreement, the Implementing Partner will:

1. Comply with UNICEF instructions on IT security and agrees to be subject to UNICEF information security reviews and/or audits, when requested.
2. Possess throughout the term of the Agreement:
 - 2.1. Incident detection measures and ensure incident response processes including its escalation to UNICEF.
 - 2.2. Information Security awareness process to train users according to their roles and responsibilities.
 - 2.3. Appropriate security controls for the processing of Personal Data, as well as sensitive non-personal data, and provide UNICEF upon the signature of the Agreement with a description of such security controls, which shall include at least
 - a) The pseudonymization of Personal Data, secure hosting and encryption of all data;
 - b) The ability to ensure the ongoing confidentiality, integrity, and availability of processing systems and services;
 - c) Basic email security controls to prevent own email domains being spoofed or communication altered in transit;
 - d) A process for regularly assessing vulnerabilities and evaluating the effectiveness of the security controls implemented;
 - e) The regular verification, evaluation and assessment of the security controls. Such measures shall at least include mechanisms to:
 1. Enforce multifactor authentication for any user access to Personal Data;
 2. Ensure encryption of data while in transit;
 3. Ensure organization-owned devices and systems are regularly updated;
 4. Ensure that all files and databases containing UNICEF data are backed up on a daily basis and paper-based information is duly secured in protected premises;
 5. Enforce system access controls, including secure credential management, granting user access while enforcing principle of least privilege, access recertification, revoking user access, administrative access and administrative user access management;
 6. Put physical access controls in place and ensure physical security measures specially targeted to protect paper based Personal Data are in place and aligned with the highest industry standards.