Data Protection and Information Security Framework for Funded Partners

DPO, CISO, DSPR

July 2025, Version 1.2

Contents

INTRODUCTION AND SUMMARY

Background

UNHCR's Data Protection Office (DPO), the Chief Information Security Officer (CISO) in the Division of Information Systems and Telecommunications (DIST) and the Implementation Management and Assurance Service (IMAS) of the Division of Strategic Planning and Results (DSPR) have collaborated to provide an overview of UNHCR's key processes surrounding data protection and information security (DPIS) standards and requirements in funded partnerships. These processes contribute towards a unified data protection and privacy framework for the organization. As part of these efforts, UNHCR pursues best practices in data protection when processing personal data and aims to work in close collaboration with partners towards the same. UNHCR seeks to create an environment that enables the principled collection, use and sharing of personal data in furtherance of its mandate.

In line with UNHCR's personal data protection and privacy framework, before transferring personal data of forcibly displaced and stateless persons to a third party or engaging the services of a third party to process personal data on behalf of UNHCR, decision-makers in UNHCR must assess the data protection capacity of such third parties. Closely linked to this, an information security baseline assessment is required for partners under the UNHCR Policy on Information Security.

By implementing this combined framework, UNHCR aims to:

(1) safeguard UNHCR processes and systems end-to-end when information is collected and services are used by partners, and

(2) protect personal data when delivering services to forcibly displaced and stateless persons via partners.

For partners selected for 2024 implementation, please see the final section at the bottom of this overview for guidance.

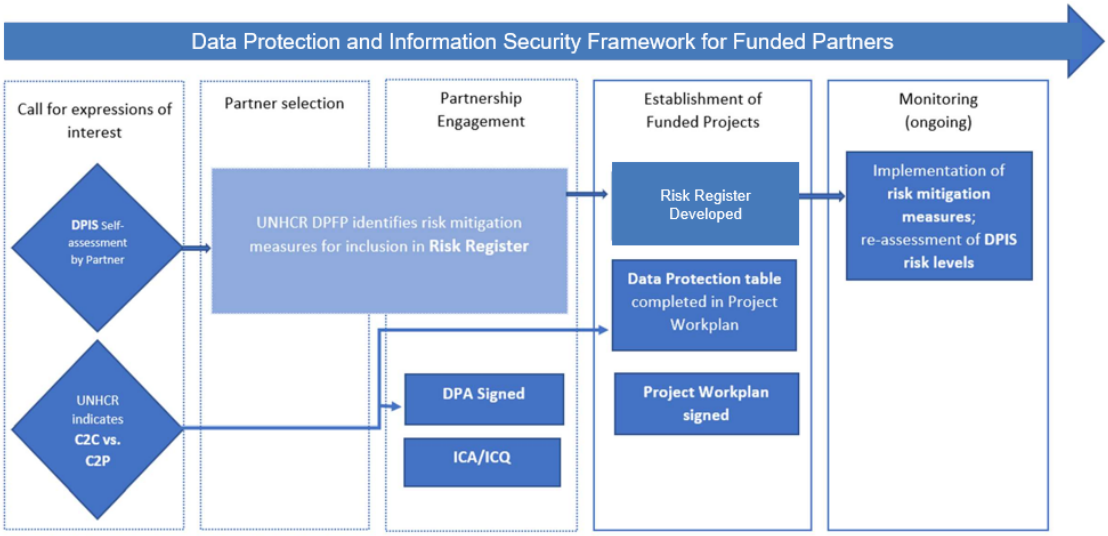

Figure 1 Process Summary

KEY ROLES AND DELIVERABLES

Partner roles

- Complete a Partner Data Protection and InfoSec Self-Assessment and answer the questions to the best of their knowledge (or indicate the lack of knowledge).
- Submit the self-assessment as part of their documentation for a competitive selection process, or when requested by a UNHCR operation.
- Submit the DPIS Capacity Assessment upon invitation from UNHCR.
- Incorporate the highest DPIS risks and mitigating measures as treatment plans within the project workplan risk register, where relevant.
- Commit to implement the recommendations made by UNHCR upon analyzing the responses to the DPIS questionnaire during the partnership engagement.
- Reflect the recommended mitigating measures in the choice of data processing tools and systems. This does not mean that UNHCR will finance or give partners solutions to meet the standards – however, this could be one option if agreed by both parties.
- Engage in and facilitate periodic audit and monitoring processes.

UNHCR roles

- Project control function leads the internal control assessment (ICA), with the Data Protection Focal Point (DPFP) advising on data protection and infosec questions.
- Programme function ensures the partner's DPIS self-assessment is completed during partnership selection.
- The DPFP, assisted by the Cybersecurity Focal Point (where appointed, or IT lead), conducts an initial DPIS review and an in-depth assessment of the partner's data protection and information security capacity, supported by the CISO's office as appropriate.
- The DPFP applies the same assessment framework to all partners engaged in projects involving the processing of personal data.
- The DPFP creates a Vendor profile on the UNHCR privacy management platform OneTrust and invites the partner to complete their DPIS Capacity Assessment on this platform.
- Project control function ensures that the highest identified risks from the DPIS Capacity Assessment will be incorporated in the project workplan risk register. A risk-based approach is applied so that low data protection capacity does not automatically disqualify a partner from processing personal data of forcibly displaced and stateless people.
- The DPFP, assisted by the cybersecurity focal point, commits to strengthening the partner's capacity in DPIS where required.
- The DPFP, assisted by the cybersecurity focal point, follows progress and provides support to monitor DPIS related issues as part of the Multi-Functional Team (MFT).
- The DPFP, assisted by the cybersecurity focal point, conducts targeted spot checks on the partner's DPIS processes, as part of the MFT verification exercises, for specific high-risk data protection and infosec partners, when necessary, and based on risks identified.
- The DPFP, assisted by the cybersecurity focal point, updates the DPIS Capacity Assessment on OneTrust with the residual risk level for relevant controls once the partner has successfully implemented the agreed mitigation measures. The DPFP also coordinates with project control to ensure that the project workplan risk register is updated once the treatment plans for the highest DPIS risks have been actioned.
- Project auditors conduct risk-based project audits.

PROCESS STEPS

1. Partner DPIS Self-Assessment

When relevant to the partnership, the UNHCR programme function requires partners to complete the Partner Data Protection and InfoSec Self-Assessment within Calls for Expression of Interest (CFEoI) on the UN Partner Portal (UNPP). Organizations therefore complete the Partner DPIS Self-Assessment when submitting a concept note in response to a CFEoI, or when requested separately by a UNHCR operation.

UNHCR will specify within the CfEoI whether the respective project involves a Controller to Controller (C2C) or Controller to Processor (C2P) model with respect to the processing of personal data in connection with the activities to be performed. There may be CfEoIs where the C2C/C2P model is not yet known as it depends on the scope of the proposals submitted by applicant organizations.

The Implementation Programme Management Committee (IPMC) **secretary** screens the UNPP partner profiles of organizations with the highest technical score to identify their UN Protection from Sexual Exploitation and Abuse (PSEA) capacity status, previous UN/UNHCR project audit internal control questionnaire (ICQ) ratings etc. The IPMC secretary shares the shortlist of screened organizations with the DPFP so that the DPFP can carry out the initial review of the Partner DPIS Self-Assessments.

2. DPIS Initial Review

The results of the Partner DPIS Self-Assessment are processed using a DPIS Initial Review form to gauge the initial indicative risk level for each applicant organization. For each individual DPIS control in the form (of which there are 22 in total), the indicative risk level is automatically determined based on the answers provided by the applicant organizations during the self-assessment. The DPFP assigns an overall indicative risk level of low, medium or high to each partner, taking into account the operational context and the nature of the project to enable meaningful prioritization. If one or more of the individual controls results in a high risk, the organization should be assigned an overall indicative risk level of medium or high.

The DPFP shares the results of the DPIS initial review with the IPMC for their consideration.

For partners recommended by the IPMC, the operation's DPFP creates a vendor profile on the privacy management platform OneTrust and invites the partners to complete their DPIS Capacity Assessment on this platform. See the **DPIS Capacity Assessment** section below for more details.

3. Internal Control Assessment/ Questionnaire

The Internal Control Assessment (ICA), coordinated by UNHCR project control, and the internal control questionnaire (ICQ), coordinated by project auditors, are built upon the harmonized internal control assessment / internal control questionnaire (ICA/ICQ) with other UN agencies. This provides a standardized assessment of the partner's programme, financial and operations management policies, procedures, systems and internal controls. The ICA/ICQ applies to all partners (except UN agencies and grant agreement partners). Baseline questions surrounding information security are embedded (in the additional UNHCR-specific 'guidance' column) within the ICA/ICQ in order to work with the partner to implement risk-based, minimum standards of information security.

Questions relevant to data protection and information security are included in the ICA/ICQ, the answers to which can be drawn upon when completing the DPIS Capacity Assessment. The ICA/ICQ is structured to determine whether partners have the processes and tools required to provide reasonable assurance about their capabilities to achieve project results. It focuses on assessing and strengthening operational capacities, policy and regulatory compliance, and reporting capacities, notably with respect to internal controls to monitor project delivery and the appropriateness of expenditures. The ICA/ICQ provides an overall risk rating of low, moderate, significant or high risk based on the various control measures and practices implemented by the partner organization. Project control/project auditors verify that the content of the ICA/ICQ (respectively) is aligned to the information presented in the supporting documents provided by the partner. Project control/project auditors share the draft ICA/ICQ report (respectively) with the partner for a final review and comments on the findings (via email or Aconex). UNHCR then finalizes the ICA/ICQ, taking into account any feedback from the partner. The final ICA/ICQ report is shared with the partner. With the coordination and support of UNHCR, the partner will implement any ICA/ICQ recommendations.

4. Data Protection and Information Security Capacity Assessment

For partners recommended by the IPMC and for whom the DPIS initial review has already been completed, the DPFP, assisted by the cybersecurity focal point, conducts the DPIS Capacity Assessment.

This in-depth capacity assessment is based on the same 22 questions used during the partner DPIS Self-Assessment and DPIS Initial Review. It is designed to measure partner capacity in three areas: the applicable regulatory framework, organizational practice, and systems and technology. The assessment framework is focused on practical, testable controls that UNHCR can check and verify when visiting partner offices, as well as a contextual protection analysis. The assessment builds on top of the UN-wide risks assessed during the ICA/ICQ (see above).

This process involves creating a Vendor profile for the recommended partner on the privacy management platform OneTrust and inviting them to complete their DPIS Capacity Assessment on this platform. In collaboration with the partner, the DPFP will identify appropriate mitigation measures and estimate the residual risk level expected to be achieved through the implementation of those measures. Implementation of the mitigation measures agreed with the partner becomes part of their obligations as per Art. 37 of the Data Protection Agreement (DPA). The highest data protection risk(s) and information security risk(s), with their corresponding treatment plans/mitigation measures, are incorporated in the project workplan **risk register**, prior to signature of the project workplan. If the DPFP considers the results of the DPIS Capacity Assessment for the recommended partner unsatisfactory, the assessment can be extended to the 2nd and 3rd choice of IPMC-recommended partners to better inform the decision on partnership selection.

For non-competitively selected partners, the partner must still complete the Partner Data Protection and InfoSec Self-Assessment, before signing the DPA, and the DPIS Capacity Assessment is completed by the DPFP on OneTrust.

The DPIS Capacity Assessment is valid for the duration for which the partner is selected for partnership with UNHCR.

Both the ICA/ICQ and the DPIS Capacity Assessment are designed as collaborative processes that emphasize dialogue between UNHCR and partners on the measures needed to improve areas of medium/moderate to high risk, identifying where UNHCR can provide the technical or other support to bring risks down within acceptable levels, and agreeing on the timing and nature of ongoing joint monitoring and project control activities.

Where operations consider it feasible, the DPFP, assisted by the local cybersecurity focal point (or IT lead), may conduct the DPIS Capacity Assessment for all applicants **ahead of the IPMC review process**. The DPFP should, in these cases, present all assessment findings to the IPMC ahead of their recommendation.

Emergency declaration
For a partnership agreement established during an UNHCR-declared Level 1/2/3 emergency, the DPIS Capacity Assessment is completed before the emergency declaration period expires if the project workplan is extended beyond the emergency declaration period (including any extensions).

Keep in mind: The partner's **DPIS Self-Assessment and the DPIS Initial Review are stored on the operation's SharePoint. The DPIS Capacity Assessment remains accessible on OneTrust.**

5. Data Protection Agreement

A Data Protection Agreement (DPA) is required for all funded partnerships where the personal data of individuals is processed under a Partnership Framework Agreement (PFA). The DPA is a legally binding document between UNHCR and a partner that establishes the terms and conditions of how personal data will be used. The DPA reflects the principles and standards set out by UNHCR's personal data protection and privacy framework established by the General Policy on Personal Data Protection and Privacy (2022).

The DPA makes reference to the DPIS capacity assessment under the 'General Obligations' where it states that the partner agrees to "*at a minimum, comply with the data protection and information security measures identified through the partner DPIS capacity assessment*".

Keep in mind: The DPFP is responsible for ensuring that partners (where relevant) have had their data protection and information security capacity assessed before the data protection agreement is signed.

The DPA includes standardized terms only and requires the completion of the corresponding 'Data Protection' table in the project workplan to outline the personal data processing particulars for the relevant project. This allows for specifying details relating to the processing of personal data such as the specific purposes, personal data elements, transfer methods and additional safeguards. The content and structure of the DPA are grounded in the principles of partnership and aim to reinforce mutual respect for the respective mandates, obligations, independence, constraints and commitments of UNHCR and the organizations with which it partners. Moreover, this DPA recognizes that many of the organizations with which UNHCR collaborates have their own data protection and privacy policies and are also subject to data protection laws in the jurisdictions where they work.

The DPA emphasizes determining the accurate roles and relationships of each party, which is the foundation for correctly attributing the **responsibility for implementation of data protection principles and ensuring respect for data subject rights**:

- In a Controller-to-Controller (C2C) relationship, UNHCR is a Data Controller, and the partner is a Data Controller. Both parties accept equal responsibility for these areas; the C2C model is applicable for most projects involving **case management** (notably including for programmes focused on the delivery of health, protection case management, protection monitoring, GBV programming, child protection interventions, etc.). In C2C relationships partners will normally take on responsibility for establishing

their own data subject request and complaint procedures, developing information notices, etc.

- In a Controller-to-Processor (C2P) relationship, UNHCR is the Data Controller, and the partner is the Data Processor. UNHCR assumes primary responsibility in these areas; the C2P model is appropriate for most other projects.

6. Project Workplan

The **project workplan** outlines the funded activities to be completed within a given implementation year and includes a table on data protection. An example of a project workplan for a Controller-to-Controller (C2C) relationship shows the data protection details a partner and UNHCR operation may incorporate.

7. Implementation Monitoring

The DPFP is responsible for ensuring that all DPIS risk mitigation measures have been implemented by regularly monitoring and verifying the partner's progress in strengthening their DPIS capacity. Based on the results of this monitoring, when a mitigation measure has been verified as successfully implemented, the corresponding risk level for each relevant control of the DPIS Capacity Assessment on OneTrust should be adjusted accordingly by the DPFP and the overall capacity risk rating updated.

The project workplan risk register is also revisited regularly throughout implementation monitoring and is used to update the status of the treatment plans for the highest DPIS risks identified. This is the same approach for all implementation monitoring recommendations raised by UNHCR and partners.

CURRENT PARTNERS AND NEWLY SELECTED PARTNERS FOR 2025 AND ONWARDS

Please refer to the table below for the DPIS assessment requirements in 2025 and onwards, depending on the context-specific scenario regarding partnership selection:

Scenario	Requirements
Multi-year PFA from 2024 onwards. Signed a 1 year transitional 'template a' for 2024 and need a new DPA for 2025 onwards.	All previously selected partners to sign the standard DPA for 2025 (with multi-year validity until end of PFA). **No DPIS capacity assessment process is required for previously selected partners** (including the partner's self-assessment). The requirements surrounding the capacity assessment therefore only target newly selected partners (whether competitively or not) for 2025 onwards.
Multi-year PFA from 2024 onwards. Signed a 1 year 'template b' (i.e. the standard) DPA for 2024 and need a new DPA for 2025 onwards.	
Multi-year PFA from 2024 onwards. Signed a multi-year 'template b' (i.e. the standard) DPA for duration for which the partner was selected.	
Newly selected partner for 2025 or future years, establishing new multi-year PFAs and project workplans for 2025 or future years.	All newly selected partners need to complete the DPIS self-assessment and UNHCR to carry out the capacity assessment before the standard DPA is signed**.**

END