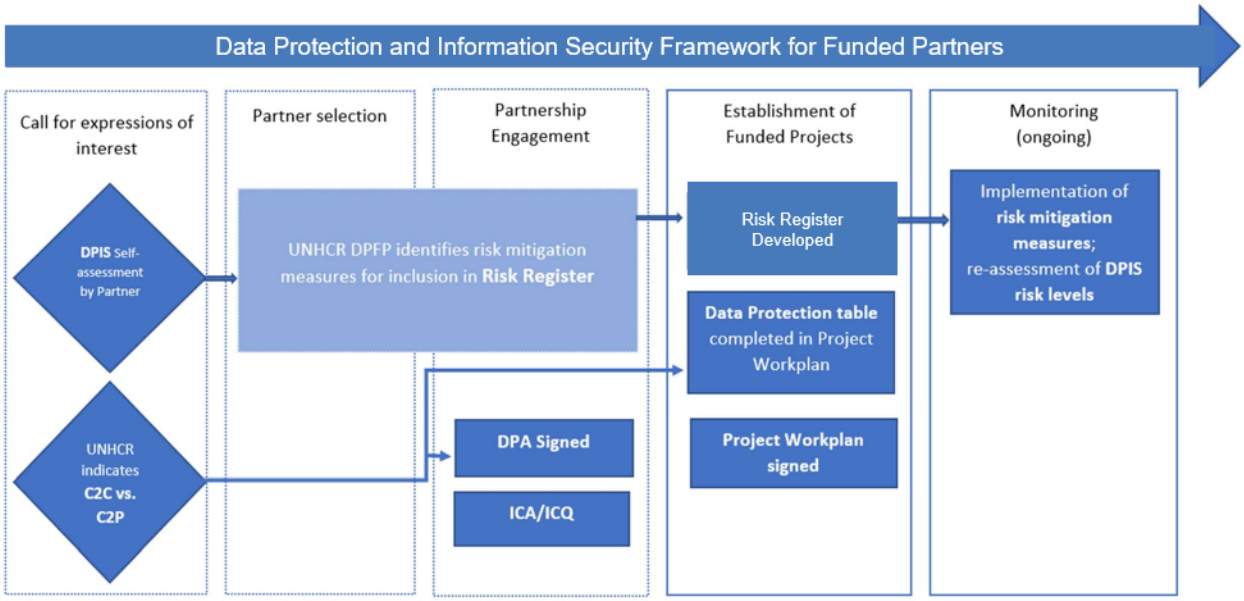
# FAQ on Data Protection and Information Security (DPIS) Framework for UNHCR and Partners

V.1.3 07.2025

## Section 1: End-to-end DPIS framework with partners

**Q1: What does the end-to-end DPIS framework comprise?**
**A1:** The end-to-end Data Protection and Information Security (DPIS) framework comprises a number of key processes that take place from when UNHCR launches a call for expression of interest for a new partnership that entails the processing of personal data of forcibly displaced and stateless people (FDSP), to the ongoing monitoring of these types of partnership agreements. The figure below summarizes the processes and resulting documents that fall under this framework.




**Q2: What does the partner need to do with respect to the DPIS framework?**
**A2:** When a partner submits a concept note for a partnership opportunity that includes the processing of personal data of FDSP, they must also fill out and submit the Partner Data Protection and InfoSec (DPIS) Self-Assessment by answering the questions to the best of their knowledge.

When a partner is selected for the partnership, they will be invited to complete the DPIS Capacity Assessment on the privacy management platform called OneTrust, and they must agree with UNHCR on the mitigation measures to be implemented for DPIS controls where the risk levels identified need to be reduced. The partner must also fill out the data protection section of the project workplan and must sign the Data Protection Agreement (see Section 2 below for more information). The partner will then collaborate with UNHCR to include the highest DPIS risk(s) in the project workplan risk register.

**Q3: Who leads the UNHCR DPIS Capacity Assessment?**
**A3:** The Data Protection Focal Point (DPFP), as part of the UNHCR Multi-Functional Team (MFT), leads the assessment. Information (cyber-) security focal points should also be consulted (where appointed) to ensure that the information security aspect is thoroughly addressed. Country offices with insufficient IT or DP capacity can be supported by the respective Regional Bureau.

**Q4: How to create a Vendor profile on OneTrust and how to launch a DPIS Capacity Assessment?**
**A4:** The DPFP, with support from the cybersecurity focal point where applicable, can create a Vendor profile using the Data Mapping Automation module in OneTrust. Once the Vendor is added, the DPIS Capacity Assessment can be initiated from the Assessments tab within the Vendor's profile.

A step-by-step guide to this process is available at: *[insert link]*

**Q5: Who can answer the DPIS Capacity Assessment?**
**A5:** When the DPIS Capacity Assessment is launched, the DPFP will include the Partner's email in the respondent field, which will trigger an invitation link to complete the assessment. On the assessment page, the Partner will have the option to add additional respondents from their organization by entering their email addresses using the "Add Participants" icon located in the top right corner of the page.

**Q6. What are the DPIS requirements in a UNHCR declared emergency?**
**A6.** For a partnership agreement established during a level 1, 2 or 3 emergency declared by UNHCR, the DPIS Capacity Assessment must be completed before the emergency declaration period expires if the project workplan is extended beyond the emergency declaration period (including any extensions). Otherwise, if the implementation of the project workplan ends before the emergency declaration expires, there is no need to complete the DPIS Capacity Assessment. The partner will then need to go through the formal selection process when UNHCR revisits its implementation modalities for the next year of implementation (after the emergency declaration has expired).

**Q7: How long is the DPIS Capacity Assessment valid for?**
**A7:** The DPIS Capacity Assessment is valid for the period for which the partner has been selected as a UNHCR partner under the Partnership Framework Agreement.

## Section 2: Understanding the Data Protection Agreement (DPA)

**Q8: What is the role of the Data Protection Agreement (DPA) in partnerships with UNHCR?**
**A8:** The DPA establishes a framework to ensure that both UNHCR and its partners adhere to stringent data protection standards. It details the responsibilities and obligations of both parties, emphasizing the critical nature of safeguarding personal data. By doing so, it replaces the former "Annex C" on personal data protection.

**Q9: Can the DPA be entered into separately from the Project Workplan, and does it remain valid for a multi-year term?**
**A9:** Yes, the DPA is entered into separately from the Project Workplan in that it forms part of a Project Framework Agreement that comes into force through the signature of a Partnership Framework Agreement (PFA) Cover Sheet. As a result, the DPA maintains its validity in alignment with the multi-year term under the PFA. General terms and conditions are stipulated in the DPA, while specific data processing details and roles of each party are documented in the Project Workplan which references the DPA.

**Q10: Does a PFA always need to include a DPA?**
**A10:** A PFA needs to include a DPA if the Project requires the processing of personal data.

**Q11: Do the data protection sections of a Project Workplan always need to be filled out?**
**A11:** Yes, they need to be filled out when the Project requires the processing of personal data. This requirement ensures that data protection measures are agreed upon and in place before project activities commence.

**Q12: Do government entities need to sign a DPA?**
**A12.** The DPA is mandatory for all funded partners processing personal data, including government entities.

**Q13: Is it possible to amend articles within the DPA (for example, omitting Article 6 on sub processing)?**
**A13:** The DPA is designed to be a standard agreement to ensure consistency with UNHCR's Data Protection Framework and internationally accepted data protection principles and standards. Specific articles can be deemed inapplicable in the Project

Workplan (PW) if not relevant. Major modifications to the DPA may require the development of tailored provisions and are subject to approval by UNHCR's Legal Affairs Service and Data Protection Office.

**Q14: How frequently is the DPA reviewed and updated, and how are partners informed of changes?**
**A14:** The DPA template is reviewed periodically to ensure it remains in line with evolving data protection standards and legal requirements and incorporates feedback from UNHCR operations and partners. When changes are required to a DPA that had already been signed, such changes will need to be mutually agreed by UNHCR and the partner.

## Section 3: Roles and Responsibilities

**Q15: How is the relationship categorized as Controller to Controller (C2C) or Controller to Processor (C2P) in projects involving UNHCR?**
**A15:** This distinction is vital for delineating precise roles and data protection responsibilities within the project. Data controllership does not equate to data ownership but rather accountability toward the data subjects. The party or the parties that determine(s) the purposes and essential means of processing personal data are Data Controllers, whereas a Data Processor acts on behalf of the Data Controller and processes personal data only according to the Controller's instructions. The categorization of the relationship as C2C or C2P will be indicated by UNHCR in the call for expressions of interest. Projects involving case management or other complex data processing activities are typically categorized as Controller-to-Controller (C2C). In these cases, partners are expected to establish their own mechanisms for handling data subject requests, complaints, and information notices.

Projects involving simpler processing, such as assistance distributions or surveys, are generally categorized as Controller-to-Processor (C2P), where the partner acts under UNHCR's instructions.

**Q16. What if one project workplan comprises activities that require both a C2C and C2P relationship with the partner? How should the project workplan data protection section be filled out?**
**A16.** Firstly, only one DPA need ever be signed because it specifies the terms for both C2P and C2C relationships, therefore covering both bases with such a partner.

Secondly, in the project workplan data protection section, it would be necessary to check both the C2P and the C2C boxes when selecting the 'roles of the parties'. After that, each and every row in the data processing particulars must be filled out, given that both C2P and C2C apply. When all applicable areas (for both C2P and C2C) are selected under 'nature and purpose of processing', it is important to indicate which 'nature and purpose' applies to which rule under the "Other" free text. For example, if C2C has fewer activities associated with this relationship, simply list all the C2C activities under the 'other' to help distinguish and clarify which relationship applies to which 'nature and purpose'.

## Section 4: Collaboration and Training

**Q17: What is the function of Data Protection Focal Points (DPFP), and how can effective collaboration be facilitated?**
**A17:** DPFPs play a pivotal role in fostering collaboration and ensuring cohesive data protection practices. They are instrumental in guiding through data protection provisions in consultation with the DPO and streamlining discussions to avoid protracted negotiations at regional or country levels. Ideally, the DPFPs shall establish and maintain contact with their counterparts within the partner organizations.

**Q18: Are there plans to train project teams to understand their roles (C2C or C2P) and implement data protection provisions effectively?**
**A18:** UNHCR has a data protection learning module, which is internally available. UNHCR is committed to capacity building and is developing a data academy to offer further sessions including to external users. Moreover, data protection focal points may offer training sessions for partners to ensure a mutual understanding and application of data protection measures. Partners are encouraged to utilize these resources and integrate data protection training into their regular staff development programs.

In the IT space, UNHCR is developing a standalone training pack which will provide guidance for project teams and partners themselves on what we expect and how to look after their IT security.

## Section 5: Retention and Continuity of Services

**Q19: How does the DPA address issues of personal data retention in relation to programs that continue beyond UNHCR funding?**
**A19:** The DPA acknowledges the need to retain personal data for service continuity, particularly in the context of a C2C relationship. If personal data retention is intended for

specific purposes for which such data was collected or shared in connection with the Project and processing for these purposes will continue beyond UNHCR funding, then these purposes should be explicitly outlined from the onset. In line with obligations relating to information under Article 8.1, relevant information notices should be provided to data subjects.

The partner's obligations with respect to data subject requests under Article 11 will survive the expiration of the partnership arrangement with UNHCR.

**Q20: How can partners ensure compliance with applicable laws when it comes to data retention, considering the varying requirements that may exist therein?**
**A20:** The model DPA allows for retention in compliance with applicable law, which broadly covers legal obligations falling upon the partner in connection with processing personal data. Partners should inform UNHCR of any retention requirements arising from legislative frameworks applicable to the partner. Specifying these retention requirements under the PW permits a harmonization of the legal compliance requirements of the partner with the DPA provisions.

**Q21: In cases where the DPA needs to align with the internal policies of partner organizations, such as record retention policies, how should this be approached?**
**A21:** Processing of personal data by UNHCR and partners should comply with UNHCR Data Protection Standards, as indicated under Article 2.11 of the DPA. This involves defining the purposes of data retention clearly, providing necessary information to data subjects, respecting their rights, and adhering to data protection principles. Compliance with internal rules should be achieved while respecting these principles and the rights of data subjects.

## Section 6: Sensitive Data

**Q22: The Project requires handling of anonymous but sensitive data relating to vulnerable groups. What can be done to safeguard this?**
**A22:** Dealing with anonymous data related to vulnerable groups necessitates stringent measures. It's imperative to incorporate protective measures such as, but not limited to, data minimization, access controls, encryption, data retention policies, regular reviews and continuous monitoring of data processing activities, and training and awareness programs. These measures help treat and mitigate disclosure risks for individuals and groups which

can result in stigma or retaliation. In such scenarios, collaborative efforts with UNHCR to implement appropriate safeguards and standards are essential.

**Q23: What guidelines are in place for the delivery of personal data to UNHCR, particularly concerning sensitive information?**
**A23:** The delivery of personal data to UNHCR must be in accordance with the PFA, the DPA and applicable data protection principles and standards. It is crucial to follow the conditions outlined in the DPA, which involve secure data transfer mechanisms and compliance with data protection principles, especially for sensitive information.

## Section 7: Data Processing

**Q24: What are the requirements for obtaining consent from data subjects for data processing activities?**
**A24:** Consent must be freely given, specific, informed, and unambiguous. Partners should provide clear information about the purpose of data processing and ensure that consent can be withdrawn easily. Documentation of consent and its scope is essential for compliance. Consent will not be valid where the data subject is unable to withdraw or withhold consent without detrimental impacts.

In view of this, **consent will not normally be a valid legitimate/legal basis** for most of the project activities that involve provision of protection, assistance, and facilitation of solutions. This is because consent would not be freely given if these activities were conditional upon obtaining consent.

**Q25: Can a Data Processor process personal data for purposes not compatible with the ones listed under the DPA if they seek consent of the data subject?**
**Q25:** In a partnership relationship, it is paramount to be clear who bears the accountability for compliance with data protection principles, including purpose specification, proportionality and lawfulness, and who is responsible for setting up systems and mechanisms to ensure data subjects can effectively exercise their rights.

In a C2P relationship, this is borne by UNHCR. It would not be appropriate for a partner to initiate a new data processing activity that is unrelated to the purposes and legal or legitimate bases previously agreed upon and communicated to data subjects. Obtaining consent does not override other fundamental data protection principles, such as purpose

specification. Moreover, in the context of humanitarian assistance, consent can rarely be an appropriate basis due to concerns about voluntariness and power imbalance.

In a C2C relationship, the accountability for compliance with data protection principles is shared between both parties. Both UNHCR and the partner must ensure that data processing activities are aligned with the agreed purposes and legal bases. Each party is responsible for setting up systems and mechanisms to enable data subjects to exercise their rights effectively.

**Q26: How should partners address data protection requirements in different jurisdictions?**
**A26:** Partners should be aware of and comply with local data protection laws in addition to the DPA, with due consideration for UNHCR's privileges and immunities, which extend to its data. This may involve adapting policies and procedures to meet specific legal requirements in the jurisdictions where they operate.

UNHCR Country offices can support partners by organizing capacity-building activities on broader data protection principles and offer guidance.

**Q27. How should UNHCR exchange personal data of FDSP with partners?**
**A27.** All FDSP data exchange should be encrypted so it can't be read by "strangers" en route.

## Section 8: Data Subject Rights

**Q28: How should partners handle data subject rights in accordance with the DPA?**
**A28:** Partners must ensure that data subjects are informed about their rights, including the right to access, rectify, or erase their personal data. Processes should be in place to respond to data subject requests promptly and in accordance with the DPA and applicable data protection laws.

**Q29: In situations where there is a C2P relationship, will UNHCR provide the partner with information notices or counseling notes to be used for purposes of implementing the data subject's right to information?**
**A29:** UNHCR should provide the partner with material to fulfill the transparency requirements. These can be included in the project workplan as appendices or later shared with the partner in writing.

## Section 9: Data Breach and Incident Response

**Q30: Why is there a need to notify UNHCR within a set period of time in case of a data breach?**
**A30:** Notification of a data breach to UNHCR is required within 48 hours under the DPA, along with documentation of the incident and measures taken. This notification period is the standard time that is included in UNHCR's data-sharing arrangements with third parties. The purpose of the notification is to enable UNHCR to take mitigative measures when appropriate.

This notification requirement is not to be confused with the notification requirement to data protection authorities where this is required under applicable law.

## Section 10: Information Security

**Q31: Is an open-source Operating System allowed to be used by partners?**
**A31:** Yes, this is allowed if the partner has a secure configuration and it is updated regularly (i.e. monthly) with security patches.

The use of an open-source operating system by partners can be allowed. However, it is vital to conduct thorough due diligence and ensure compliance with all applicable legal, regulatory, and organizational standards.

1. Licensing Compliance: Open-source software is distributed under various licenses (e.g., GPL, MIT, Apache). Each license has specific terms and conditions regarding usage, modification, and redistribution. Partners must comply with these terms to avoid potential legal issues.
2. Security and Risk Management: Open-source software can pose security risks if not properly vetted. It is crucial to assess the security posture of the operating system and ensure that partners implement appropriate security measures to mitigate risks.

3. Data Protection and Privacy: If the open-source operating system will handle personal or sensitive data, compliance with data protection regulations (e.g., GDPR, HIPAA, local legislation) is mandatory. Partners need to understand their obligations regarding data handling and storage.
4. Support and Maintenance: Unlike proprietary software, open-source systems may not have formal support channels. Partners should have the capability to maintain and support the operating system to minimize operational risks.
5. Documentation and Audit Trails: Maintain thorough documentation regarding the use of the open-source operating system, including licensing agreements and compliance checks. This can be critical for audits and demonstrating compliance.
6. Vulnerability Management: Open-source operating systems can be more susceptible to vulnerabilities if not regularly updated. Partners must have a robust process in place for monitoring, identifying, and patching vulnerabilities.
7. Configuration Management: Proper configuration is critical for security. Partners must ensure that the open-source system is securely configured according to best practices.

**Q32. What if the partner does not have their own organization email domain and their staff are using a commercial email provider (e.g. gmail, hotmail)?**
**A32:** Partners are required to use only approved, organization-owned email accounts for the transfer of personal data and refrain from using personal email accounts (e.g. gmail, yahoo). Gmail, Hotmail, Outlook and Yahoo accounts are the personal property of the staff who set them up and everything sent to these accounts is not sent to a legal entity but to the person. When they leave the organization, they will take all this with them, and it is unlikely that the partner will even have access to the data we transferred via such channels. We recognise that this has happened many times before, but we hope to minimise new cases and phase it out gradually.

In addition, partners should (of course) set up multifactor authentication (MFA), anti-phishing and anti-malware services on their corporate mail systems.

## Section 11: Monitoring and Compliance

**Q33: How is compliance with the DPA monitored by UNHCR and its partners?**
**A33:** UNHCR and its partners shall incorporate adherence to the DPA into their regular ongoing monitoring of the project. Any identified gaps or non-compliance issues should be addressed promptly, with corrective actions documented and implemented.

Where there is a C2P relationship, an annual data protection audit is foreseen to assess the level of compliance with the DPA provisions.

** END **