FAQ on DPA for UNHCR and Partners

v.1.1 12.02.2024

Section 1: Understanding the Data Protection Agreement (DPA)

Q1: What is the role of the Data Protection Agreement (DPA) in partnerships with UNHCR?
A1: 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.

Q2: Can the DPA be entered into separately from the Project Workplan, and does it remain valid for a multi-year term?
A2: 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.

Q3: Does a PFA always need to include a DPA?
A3: A PFA needs to include a DPA if the Project requires the processing of personal data of Forcibly Displaced and Stateless persons.

Q4: Do the data protection sections of a Project Workplan always need to be filled out?
A4: No, it needs to be filled out only if the Project requires the processing of personal data of Forcibly Displaced and Stateless persons, and if the template b is selected for 2024 implementation. This requirement ensures that data protection measures are agreed upon and in place before project activities commence. If the transitional DPA template (based on the previous Annex C) is used in 2024, the details are contained therein, and it is not necessary to fill in the data protection sections of the Project Workplan.

Q5: Who leads the assessments on data protection and information security?
A5: The Data Protection Focal Point (DPFP), as part of the UNHCR Multi-Functional Team (MFT), leads the assessment. Information security focal points should also be consulted as part of the process so as to ensure that the information security aspect of data protection

is thoroughly addressed. Country offices with insufficient capacity can be supported by the respective Regional Bureaux.

Q6: Is it possible to amend articles within the DPA (for example, omitting Article 6 on sub processing)?
A6: 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 Work Plan (PWP) if not relevant. Major modifications may require the development of tailored provisions and are subject to approval by UNHCR's Legal Affairs Service and Data Protection Office.

Q7: How frequently is the DPA reviewed and updated, and how are partners informed of changes?
A7: The DPA format 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 be agreed by UNHCR and the partner.

Section 2: Roles and Responsibilities

Q8: How is the relationship categorized as Controller to Controller (C2C) or Controller to Processor (C2P) in projects involving UNHCR?
A8: This distinction is vital for delineating precise roles and data protection responsibilities within the project. Data Controllership does not equate to data ownership but is defined by the accountabilities to 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 is a natural or legal person that processes personal data on behalf of the Data Controller following instructions of the latter. The categorization of the relationship as C2C or C2P will be indicated by UNHCR in the call for expressions of interest. As a rule, projects that involve case management and similar complex processing will be better served by a C2C framework, with partners establishing their own data subject request and complaint mechanisms, information notices, etc. Projects that involve less complex processing processes, for example, assistance distributions or surveys are better served by the C2P framework.

Section 3: Collaboration and Training

Q9: What is the function of Data Protection Focal Points (DPFP), and how can effective collaboration be facilitated?
A9: 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 Partners.

Q10: Are there plans for training project teams to understand their roles (C2C or C2P) and implement data protection provisions effectively?
A10: 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.

Section 4: Retention and Continuity of Services

Q11: How does the DPA address issues of personal data retention in relation to programs that continue beyond UNHCR funding?
A11: The DPA acknowledges the necessity of personal data retention 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.

Q12: How can partners ensure compliance with applicable laws when it comes to data retention, considering the varying requirements that may exist therein?
A12: The 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 the retention requirements arising from legislative frameworks applicable to the Partner. Specifying these retention requirements under the PWP permits a harmonization of the legal compliance requirements of the Partner with the DPA provisions.

Q13: In cases where the DPA needs to align with internal policies of partner organizations, such as record retention policies, how should this be approached?
A13: Processing of personal data by UNHCR and partners should comply with data protection standards. 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 5: Sensitive Data

Q14: The Project requires handling of anonymous but sensitive data relating to vulnerable groups. What can be done to safeguard this?
A14: Dealing with anonymous data related to vulnerable groups necessitates stringent measures. It's imperative to incorporate protective measures to 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.

Q15: What guidelines are in place for the delivery of personal data to UNHCR, particularly concerning sensitive information?
A15: 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 6: Data Processing

Q16: What are the requirements for obtaining consent from data subjects for data processing activities?
A16: 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 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.

Q17: 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?
Q17: 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 operation unrelated to the purposes and legal/legitimate bases that were agreed between us relayed to the data subjects. Obtaining consent does not render other data protection principles, such as purpose specification, inapplicable. Moreover consent can rarely be an appropriate basis in the context of delivering humanitarian assistance.

Q18: How should partners address data protection requirements in different jurisdictions?
A18: Partners should be aware of and comply with local data protection laws in addition to the DPA. This may involve adapting policies and procedures to meet specific legal requirements in the jurisdictions where they operate. Country offices can support partners by organizing capacity-building activities on broader data protection principles and offer guidance.

Section 7: Data Subject Rights

Q19: How should partners handle data subject rights in accordance with the DPA?
A19: 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.

Q20: 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?
A20: UNHCR should provide the Partner with material to fulfill the transparency requirements. These can be included in the project workplan as appendices or later on shared with the Partner in writing.

Section 8: Data Breach and Incident Response

Q21: Why is there a need to notify UNHCR within a set period of time in case of a data breach?
A21: notification to UNHCR is required within 48 hours, 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. Such notification requirement is not to be confused with the notification requirement to data protection authorities where this is required under applicable law. The purpose of the notification is to enable UNHCR to take mitigative measures when appropriate.

Section 9: Monitoring and Compliance

Q22: How is compliance with the DPA monitored by UNHCR and its partners?
A22: UNHCR and its partners should 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.