GUIDANCE ON THE PROTECTION OF PERSONAL DATA OF PERSONS OF CONCERN TO UNHCR

2018

DATA PROTECTION POLICY

Contents

1. General Provisions

1.1. Purpose

The purpose of this *Guidance on the Protection of Personal Data of Persons of Concern* is to assist UNHCR personnel in the application and interpretation of the Policy on the Protection of Personal Data of Persons of Concern (DPP), adopted in May 2015.[1] It promotes the principled and practical implementation across all UNHCR operations.

1.2. Rationale

The Data Protection Policy foresees in para. 1.1 that it will be complemented by Operational Guidelines. While the Policy established the overarching framework including the basic principles of personal data processing (para. 2.1 of the DPP), a number of key concepts (e.g. personal data, privacy by design), tools (e.g. impact assessments) and procedures (e.g. breach notification and clearance of data transfer agreements), the Guidance is a tool which develops and elaborates on these principles, concepts and procedures in order to facilitate their implementation. The Guidance also responds to requests from the field and auditors.

1.3. Scope

The scope of this Guidance corresponds with the scope of the Data Protection Policy, i.e. it applies to all processing of personal data of persons of concern to UNHCR (para. 1.3.1 and 1.3.2 of the DPP). This Guidance applies to all UNHCR personnel. It is particularly relevant for data controllers, data protection focal points and data processors.

1.4. Terms and definition

In addition to those defined in the Data Protection Policy, this Guidance introduces a number of additional terms and definitions. The definitions marked as (*) correspond with the definitions established in para. 1.4 of the Data Protection Policy.

[1] UNHCR, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR ("Data Protection Policy")*, 27 May 2015, available at: www.refworld.org/docid/55643c1d4.html.

"Aggregate data" means data is combined in a way to show values or trends without including the records of individual data subjects or data that would render an individual data subject identifiable.

"Anonymization" is the process of removing or modifying all personal identifiers and codes in such a way that individual data subjects cannot be identified and there is no reasonable likelihood that identification could take place based on the data, alone or in combination with other data.

"Assent" is the expressed willingness and views of a child to participate in assistance or protection activities and services in situations where he/she cannot legally provide formal consent to the processing of personal data due to age, level of maturity and/or other factors.

"Consent" means any freely given and informed indication of an agreement by the data subject to the processing of his/her personal data, which may be given either by a written or oral statement or by a clear affirmative action. (*)

"Data Controller" means the UNHCR staff member, usually the Representative in a UNHCR country office or operation, who has the authority and accountability for overseeing the management of, and to determine the purposes for, the processing of personal data. (*)

"Data minimization" means a standard procedure to minimize data protection risks and ensure that the data collected, shared or otherwise processed is necessary and relevant to achieve a specified purpose.

"Data Processor" means any UNHCR staff member or other natural person or organization, including an Implementing Partner or third party that carries out processing of personal data on behalf of the data controller. (*)

"Data Protection Focal Point" means, in principle, the most senior UNHCR protection staff member in a UNHCR country office or operation, who has been designated by the data controller to assist in carrying out his or her responsibilities regarding this Policy. (*)

"Data Protection Impact Assessment" is a tool and a process to assess the protection impacts on data subjects in processing their data, and for identifying remedial actions to avoid or minimize such impacts. (*)

"Data Protection Officer" means the UNHCR staff member in the Division of International Protection, who supervises, monitors and reports on global compliance with the Policy. (*)

"Data Sharing" means any act of transferring or otherwise making personal data of persons of concern accessible within or between UNHCR offices, or to a UNHCR partner or third party.

"Data subject" means any individual falling within the scope of the Data Protection Policy whose personal data is subject to processing by UNHCR. (*)

"Data Transfer Agreement" is an agreement between UNHCR and a third party which states the terms and conditions of the use of personal data, including the specific data sets to be shared, the mode of data transfer, for what purposes the data may be used, data security measures, and related issues. (*)

"Individual case file" is the central repository for data related to a specific person of concern, whether in hardcopy or electronic format, including all relevant correspondence created and received by UNHCR. This includes, i.e.: asylum application forms; protection needs assessments; registration forms; Refugee Status Determination (RSD) application forms; signed consent and/or disclosure forms; interview transcripts and counselling notes; documents produced by the Persons Of Concern (POC) and dependent family members; home visit requests and reports; medical documents (such as medical assessment forms); subsistence allowance documents; copies of Best Interest Assessments and Best Interest Determinations and related procedural steps; Resettlement Registration Forms (RRF); correspondence with partners, including government authorities and resettlement countries; any printed email or other correspondence pertaining to the case.

"Implementing Partner" means an organization established as an autonomous and independent entity from UNHCR that UNHCR engages through a Project Partnership Agreement (PPA) to undertake the implementation of programmatic activities within its mandate. (*)

"Operational Partner" means an organization which does not receive funding from UNHCR but with which UNHCR cooperates and collaborates to provide protection and assistance to POCs, which could include the sharing of aggregate/statistical and/or personal data to facilitate efficient assistance and service delivery and avoid duplication of humanitarian efforts.

"Personal data" means any data related to an individual who can be identified from that data; from that data and other information; or by means reasonably likely to be used related to that data. Personal data includes biographical data (biodata) such as name, sex, marital status, date and place of birth, country of origin, country of asylum, individual registration number, occupation, religion and ethnicity, biometric data such as a photograph, fingerprint, facial or iris image, as well as any expression of opinion about the individual, such as assessments of the status and/or specific needs. (*)

"Personal data breach" means a breach of data security leading to the accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transferred, stored or otherwise processed. (*)

"Person of concern" means a person whose protection and assistance needs are of interest to UNHCR. This includes refugees, asylum-seekers, stateless persons, internally displaced persons and returnees. (*)

"Processing of personal data" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available to any party, alignment or combination, restriction, erasure or destruction. (*)

"Pseudonymization" means modifying data so that it remains associated to a particular individual data subject without that individual being identified. This is done by assigning reference codes or pseudonyms to individual data subjects in lieu of their personally identifying data. These codes are kept separately and are subject to technical and organizational measures to ensure that data is not attributable to an identified or identifiable data subject

"Subject access request" means a request from a person of concern, or their legal representative, to obtain information from UNHCR about the personal data that it holds on them, and any associated requests to amend or delete such data. Subject access requests may also be received from family members in respect to data held in UNHCR's archives.

"Third party" means any natural or legal person other than the data subject, UNHCR or an Implementing Partner. Examples of third parties include national governments, international governmental and non-governmental organizations, private sector entities or individuals. (*)

"UNHCR personnel" means all individuals working for UNHCR, including staff members, affiliate workforce (consultants, deployees, UN Volunteers etc.), and interns.

1.5. Abbreviations

This Guidance also uses the following abbreviations:

BIMS	Biometric Identity Management System
DIP	Division of International Protection
DIST	Division of Information Systems and Telecommunications
DPP	Data Protection Policy
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDPB	European Data Protection Board
FICSS	Field Information and Coordination Support Section
FSS	Field Security Service
GDPR	General Data Protection Regulation of the European Union
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICT	Information and Communication Technology
IGO	Office of the Inspector General
IMRS	Identity Management and Registration Section
IPMS	Implementing Partner Management Service
ISO	International Organization for Standardization
LAS	Legal Affairs Service
POC	Persons of Concern
PNSS	Protection and National Security Section
PPA	Project Partnership Agreement
RAS	Records and Archives Section
RSD	Refugee Status Determination
SGBV	Sexual and Gender Based Violence

1.6. Structure of the Guidance

This Guidance follows essentially the structure of the Data Protection Policy in the order in which the basic data protection principles are dealt with. Some basic principles require more explanation and take more space than others, i.e. legitimate and fair processing, the rights of data subjects, data security and accountability. The Guidance therefore deals with them in separate sections. Other Principles are jointly dealt with in one section. In addition, several concepts and types of data processing are, due to their importance, also elaborated in separate sections, i.e. personal data, data breaches, impact assessments and data transfers. Throughout the Guidance, reference is made to the Data Protection Policy in order to show the close link between both documents and highlight which aspects are covered by the mandatory Policy. Other sources are referred to in footnotes.

2. On personal data, anonymized and pseudonymized data

2.1. Personal data

2.1.1 By limiting its scope to **personal data**, the DPP deliberately follows a concept and notion established in international and regional data protection law. The definition of personal data in the DPP (para. 1.4) ought to be equivalent to the common definition of "any information relating to an identified or identifiable natural person ('data subject')".[2] The authoritative guidance and interpretation provided on this definition, for instance by the European Court on Human Rights, the European Data Protection Board (EDPB) and the former Article 29 Working Party, is therefore relevant also for the interpretation of UNHCR's DPP.

2.1.2 To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out to identify a person directly or indirectly. **Identification** requires elements which describe a person in such a way that he or she is distinguishable from all other persons and recognizable as an individual. A person's name is a prime example. However, in certain environments, reference to a position (e.g. head of an organization) may be sufficient and qualify as personal data. In other environments, names may not suffice to establish the identity of a person and additional identifiers are needed such as date and place of birth, personalized numbers or, increasingly, biometric data.

2.2. Anonymization

2.2.1 In para. 1.3.1, the DPP mentions aggregated or anonymized data as examples that do **not fall within the scope of the Policy** but does not develop the notion; pseudonymization is not mentioned in the Policy. This Guidance offers a definition of both, anonymization and pseudonymization, and additional explanation below.

[2] See Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, CETS No. 108, as it will be amended by its Protocol, 25 June 2018, CETS No. 223 (Modernized Convention 108), available at: https://rm.coe.int/16808ade9d, Article 2 (a); European Union, *Regulation (EU) 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, 27 April 2016, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, Article 4 (1); and International Conference of Data Protection and Privacy Commissioners (ICDPPC), *International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution)*, 5 November 2009, available at: https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf, Part I 2.a.

2.2.2 The point and characteristic of anonymization is that a set of personal data has been **irreversibly modified in such a way that the data subject is no longer identifiable**. No element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person concerned. Where data have been **successfully anonymized, they are no longer personal data**. With regard to anonymization techniques, UNHCR data controllers and data processors need to verify that they produce the desired result.[3] Where the necessary expertise is lacking, responsible staff members are encouraged to contact DIST and/or seek further advice with the DPO.

2.3. Pseudonymization

2.3.1 Anonymization needs to be distinguished from pseudonymization, which disables the identification by **replacing identifiers by a pseudonym**. Pseudonymization is achieved, for instance, by encryption of the identifiers in personal data; a common example in UNHCR is the use of registration or identity numbers instead of names of POCs. **Pseudonymized data remains personal data for those who are entitled to use the decryption key**, which allows re-identification. For everyone who is not in possession of the decryption key, pseudonymized may still be identifiable but with difficulty, i.e. not with means reasonably likely to be used. Pseudonymization is however still often good practice in that it offers a certain level of data protection depending on the concrete operational circumstances.

2.4. Aggregate data

2.4.1 With regard to aggregate data that is derived from personal data, improper handling could in certain circumstances pose risks to persons of concern to UNHCR. This is the case for, example, where aggregate data is **combined with other data sets or submitted to data matching** or other techniques that transform anonymized data into personal data, so that individuals become identifiable. This should be equated with the naming of an individual. For identification, it can be enough to be able to establish a reliable connection between particular data elements and a known individual.

2.4.2 However, even where anonymization is carried out effectively, and the data protection policy is no longer applicable, UNHCR staff is reminded of **inherent protection risks of using, and in particular sharing and publishing, aggregate data**. For instance, there is the risk that datasets divulge the actual location of small or 'at risk' groups, for

[3] See, e.g., Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymization Techniques*, Working Paper 216, adopted on 10 April 2014, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf; and UK Information Commissioner's Office, *Anonymization: Managing data protection risk - code of practice*, November 2012, available at: https://ico.org.uk/media/1061/anonymisation-code.pdf.

example by mapping data such as country of origin, religion or specific vulnerabilities to the geographical coordinates. Closely related is the aspect that aggregate data, e.g. on SGBV or other protection incidents, should only be shared if there is a sufficient number of total incidents (usually over 50) and should not be disaggregated by age, sex, geographical area, or any other data points where there is not a sufficient volume of incidents to ensure that they cannot be traced back to individuals or geographical locations.[4] These considerations are driven by general protection imperatives related to avoidance of physical harm, stigmatization, discrimination, intimidation or xenophobic practices to groups or individuals, criminalization, racism or jeopardizing relations with host communities.

2.4.3 If the sharing or publication of anonymized data could pose protection risks, UNHCR may enter into a formal **agreement with partners or research organizations** with whom the data is shared, setting out the terms and conditions for the use of the data, including an obligation to maintain the confidentiality of the dataset and prevent unauthorized access. Provisions may also be included for UNHCR to review material prior to publication. Operations should seek support from regional Information Management Officers, where available, or from FICSS and the DPO in Headquarters, when needed.

3. Legitimate and fair processing

In this Section, the Guidance provides short explanations of the principle of legitimate and fair processing, guidance for the understanding of each legitimate basis, examples from typical UNHCR contexts and guidance for the choice of the appropriate legitimate basis. Seeking consent/assent from children and from individuals with mental health conditions and intellectual disabilities are addressed separately at the end of this section.

[4] See on this and other aspects in this section: UNHCR, *Statistical Yearbook 2015, Chapter 6: From Data Protection to Statistics*, available at: http://www.unhcr.org/56655f4c21.html; see also United Nations Development Group (UNDG), *Data Privacy, Ethics and Protection, Guidance Note on Big Data for Achievement of the 2030 Agenda*, 2017, available at: https://undg.org/wp-content/uploads/2017/03/UNDG-Big-Data-Guidance-Note.pdf and Office of the High Commissioner for Human Rights , *A Human Rights-Based Approach to Data: Leaving No One Behind in the 2030 Development Agenda, Guidance Note to Data Collection and Disaggregation*, 2018, available at: https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf.

3.1. Introduction

3.1.1 According to para. 2.2 of the DPP, processing personal data may only be carried out on a legitimate basis and in a fair and transparent manner. The need for a **legitimate basis**, also known as lawful processing, has its origin in Human Rights law requiring a legal basis for any interference with the right to respect for private life of the data subject.[5] Considering the nature of UNHCR as a UN entity that benefits from privileges and immunities, the term 'legitimate basis' was chosen instead of legal basis or lawfulness. For the purpose of the processing of personal data by UNHCR, the DPP as a High Commissioner's Policy is the appropriate source document to identify the legitimate bases.

3.1.2 The DPP also clarifies that UNHCR may (only) process personal data based on one or more of the above-mentioned legitimate bases. For example, processing personal data in the vital or best interest of POCs would also be covered by UNHCR's mandate. The Policy does however **not establish an explicit hierarchy of legitimate bases** although the relevance of each may be deducted from the order in which they are listed in para. 2.2 of the DPP: (i) consent – (ii) vital or best interest – (iii) UNHCR's mandate – (iv) beyond UNHCR's mandate the safety and security of persons. The Policy also does not provide guidance as to which legitimate basis applies in which situation. Only para. 2.2 (iv) of the DPP ("Beyond UNHCR's mandate, to ensure the safety and security of persons …") indicates that the other legitimate bases (consent and vital or best interest) are meant to cover activities of personal data processing *within* UNHCR's mandate.

3.1.3 The **fairness** element generally requires UNHCR to be transparent, meaning clear and open with POCs as data subjects about how their information will be used. This aspect, also referred to as the transparency principle, is essentially covered in the UNHCR DPP in the data subject's right to information (para. 3.1 of the DPP). In this paragraph, the DPP lists in points (i) to (viii) all relevant information which needs to be provided when collecting personal data. Respecting the right to information is therefore commensurate with the transparency principle. Other aspects of fairness concern the processing of personal data only in ways that POCs would reasonably expect of UNHCR, not using data in ways that could have an unjustifiably adverse or discriminatory impact on them and paying particular attention when processing particularly sensitive data (such as medical data, data concerning the conviction or suspicion of criminal offenses, the identity of witnesses, persons living

[5] See UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, available at: http://www.refworld.org/docid/453883f922.html, para. 3 and 8.

in hiding due to threats to their safety, or information related to sexual orientation or membership of a minority religious or ethnic community).

3.2. Consent

3.2.4 **Consent** is the most frequently used and often the preferred legal basis for personal data processing. However, given the vulnerability of most beneficiaries and the nature of humanitarian emergencies, many humanitarian organizations will not be in a position to rely on consent for most of their personal data processing[6]. Whether consent is the appropriate legitimate basis depends on a careful analysis and thorough understanding of each situation. The fairness towards and respect for the rights of individuals requires UNHCR to apply consent whenever the situation allows the individual to exercise his or her choice freely and informed. Typical examples from UNHCR's work for procedures requiring consent of the individual are: registration (see however below under UNHCR's mandate), RSD, voluntary repatriation, resettlement, assistance, needs assessments, tracing, SGBV case management.

3.2.5 Based on the definition in para. 1.4 of the DPP, for consent to constitute a viable legitimate basis, it needs to be freely given and informed. **Freely given** means that the individual has a genuine choice and is able to refuse or withdraw consent without adverse consequences. In emergency situations, but also with regard to access to assistance (food, cash) and in the absence of other viable sources of income, this condition may not be fulfilled because refugees or other POCs may see no alternative to agreeing to accept that their data is collected and shared with partners. Any coercion or unduly influence is incompatible with the condition of freely given consent.

3.2.6 **Informed** consent requires that the data subject receives explanations, which allows for full appreciation and understanding of the circumstances, risks and benefits of processing. Factors such as age, gender, the level of education, health or disability may affect an individual's ability to understand the consequences of data processing and need to be taken into account in the way information is provided (see also below: Seeking consent/assent from children and from individuals with mental health conditions and intellectual disabilities). The information needs to be provided in simple jargon-free language, yet complete, with a sufficient level of detail to enable the data subject to clearly appreciate the future data flows, including risks and consequences as much as known to UNHCR. In order to be complete, the information should cover all of the envisaged data processing activities to be carried out, especially what data sets or elements will be shared or transferred with the host Government, implementing partners or other third parties.

[6] International Committee of the Red Cross (ICRC), *Handbook on Data Protection in Humanitarian Action*, June 2017, available at: https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action, Chapter 3, page 45, para 3.2.

3.2.7 The definition of consent in the DPP also clarifies that consent may be given either by a **written or oral statement or by a clear affirmative action**. Examples for written consent are the Voluntary Repatriation Form and the Resettlement Registration Form (Section 8 of the RRF: Declaration). Apart from established processes, such as registration, RSD, resettlement, voluntary repatriation, and SGBV case management, the responsibility for establishing appropriate consent procedures remains with the data controller. Whatever the method for providing consent, this Guidance encourages proper recording of consent, for instance in an interview transcript, as a note for the file or in audio recording.

3.3. Vital or best interest

3.3.1 When consent cannot be validly obtained, personal data may still be processed if it is in the vital interest of the data subject, i.e. where data processing is **necessary in order to protect an interest which is essential for the data subject's life, integrity, health, dignity, or security**[7]. The best interest refers to the principle set out in Article 3 (1) of the Convention on the Rights of the Child and can be used as a legitimate basis where the processing of children's personal data is in their best interest. For UNHCR, this would require the proper conduct of a best interest procedure (see also below: seeking consent/assent from children).

3.3.2 **Examples** are: urgent and lifesaving assistance in the preliminary stages of a large scale/emergency response, processing of data of POCs who are unable to provide consent due to their state of health (including unconsciousness), or do not have the capacity (including due to mental health conditions and intellectual disabilities), to secure the release of a POC from detention, or similar facility, where UNHCR does not have access to obtain consent directly from the individual and processing of personal data relating to unaccompanied or separated children in their best interest.

3.4. To enable UNHCR to carry out its mandate

3.4.1 For the purpose of processing personal data of POCs, the mandate of UNHCR as set out in its Statute and amended in subsequent resolutions of the UN General Assembly[8] can be considered a legitimate basis. The general notion of this category of legitimate basis

[7] See ICRC, *Handbook on Data Protection in Humanitarian Action*, Chapter 3, page 48, para. 3.3.

[8] See UNHCR, *Note on the Mandate of the High Commissioner for Refugees and his Office*, October 2013, available at: http://www.unhcr.org/uk/526a22cb6.pdf.

is 'important grounds of public interest'[9]. Important grounds of public interest are triggered **when the activity in question is part of a humanitarian mandate established under international law**[10]. Cases where this legitimate basis may be relevant include distribution of assistance, where it may not be practicable to obtain consent of all the possible beneficiaries, and where it may not be clear whether the life, security, dignity and integrity of POCs is at stake, i.e. where the vital or best interest basis would not apply.

3.4.2 **Examples** for relying on this legitimate basis are: registration and mandate RSD, when this is a prerequisite for UNHCR´s work in delivering protection and assistance to POCs; the routine transfer of basic biographical data to host governments, when required by a host country agreement or MOU; processing data for anonymizing or pseudonymizing; processing data to combat fraud committed by POCs, or when POCs are implicated in a case of possible misconduct by any person or entity with a contractual link to UNHCR; maintenance of the information security of UNHCR databases and ICT infrastructure; when data is provided to UNHCR from partners or third parties for the purposes of protection or assistance; or processing data for the purposes of archiving.

3.5. Beyond UNHCR's mandate, to ensure the safety and security of persons of concern or other individuals

3.5.1 This legal basis stands **in direct correlation with para. 6.3 and 6.4 of the DPP** concerning the transfer of personal data to national and international law enforcement agencies, tribunals and courts. Other examples could concern: measures taken in order for UNHCR to respond effectively to personal data breaches (if the measures would go beyond the mandate); implementation of security management procedures that are necessary to ensure the safety of POCs, UNHCR personnel and others, in particular in the context of an ongoing and serious security threat; and measures taken in the context of formal investigations into possible misconduct by anyone contractually linked to the UN, including into possible sexual exploitation and abuse, in particular if seeking consent could compromise the integrity of the investigation and/or expose victims or others to harm.

3.6. Determining the appropriate legitimate basis

3.6.1 According to para 7.2.2 (i) of the DPP, the responsibility to determine the applicable legitimate basis for the specific and legitimate purpose(s) of data processing lies with the data controller, assisted by the data protection focal point. In case of questions, the DPO may be consulted (para. 7.2.3). Apart from the **principled need** to process personal data

[9] See, e.g., Article 6 (1) (e) of the GDPR that recognizes as lawful processing when it is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

[10] See ICRC, *Handbook on Data Protection in Humanitarian Action*, Chapter 3, page 49, para. 3.4.

based on the appropriate legitimate basis, the **practical relevance** of its determination will often lie in deciding whether or not to require consent. Where consent is the relevant legitimate basis, the consequence of withholding or withdrawing consent is that personal data ought not to be processed. Moreover, where consent is determined not to be the appropriate legitimate basis, UNHCR will be required to take more responsibility for the assessment of risks and benefits or processing, not least when new technologies are involved and in situations characterized by complex data flows and multiple stakeholders[11]. UNHCR is furthermore still bound to exercise due diligence and assessing the impact of data processing once consent is obtained as a general requirement of UNHCR's protection mandate.

3.6.2 It should also be noted that obtaining **consent is not the same as providing information** about data processing. The former is a legitimate basis, the latter an individual right of the data subject and the consequence of the transparency principle that needs to be respected irrespective of the legitimate basis for processing. Finally, the right to object per para. 3.4 of the DPP needs to be respected also where the processing of personal data is based on legitimate bases other than consent – however within the limits set out in para. 3.4 and 3.7 of the DPP.

3.7. Seeking consent/assent from children

3.7.1 **Children** require specific protection and they are a particularly vulnerable category of data subjects. They may be less aware of the risks and consequences, as well as safeguards and rights, related to the processing of their data. With regard to the legitimate basis for processing children's personal data, in most situations, consent can and should be obtained from the child's parent, family member with parental responsibility, or legal or customary caregiver.

3.7.2 However, in the case of unaccompanied or separated children, or where the child's parents and/or caregiver might be at the origin of risks or harm to the child, UNHCR, and partners, are in a situation where certain actions, notably best interest procedures, require the processing of the child's personal data. In such situations, consent by the child may still be the appropriate legitimate basis provided he/she has the capacity to understand the process and its ensuing rights and obligations. Using **consent by the child** requires therefore an assessment of the evolving capacity, including age, level of maturity and development, and/or other factors. Applicable national legal standards may also need to be taken into account, for instance when working with national authorities or their approval is required.

[11] ICRC, *Handbook on Data Protection in Humanitarian Action*, Chapter 3, page 45, Section 3.2.

3.7.3 In the case of children who are not able to give consent, UNHCR may process the child's personal data based on the "the vital or best interest of the data subject" (para. 2.2 (ii) of the DPP). However, and irrespective of this legitimate basis, where a child can understand and agree to participate in services or activities, his or her informed assent should be sought. **Assent** is the expressed willingness and views of a child to participate in services or activities, for example to take part in a child protection activity, receive medical care, or benefit from assistance.

3.7.4 When collecting personal data from children, UNHCR personnel should strive to ensure it takes place in a **child-friendly environment and procedures** and be conducted by personnel with knowledge of and experience in working with children. Interviews should be conducted in an age-appropriate and gender-sensitive manner, taking into account the developmental and maturity level, as well as individual and contextual circumstances and needs of the child. Any communication about data processing should be in clear and plain language and preferably in multiple formats (e.g. visual, audio and easy to read).

3.8. Seeking consent from individuals with mental health conditions and intellectual disabilities

3.8.1 Persons of concern with disabilities, including those with mental health conditions and intellectual disabilities, have the same rights to make decisions in respect to the use of their personal data as other persons. UNHCR personnel should assume, subject to any indications to the contrary, that such persons do have the **capacity to provide consent** and follow its regular procedures for obtaining and recording consent, adapted to an individual's communication needs and preferences, and other support needs.

3.8.2 **Communication methods** may need to be adapted for persons with disabilities, depending on their communication preferences. Some may require additional support and assistance in situations when personal data is being collected. When UNHCR personnel are unsure about an individual's capacity to understand the process, and its ensuing rights and obligations, they should involve a supervisor (or another colleague with relevant expertise) to consider additional supports and be able to determine the person's will and preferences. UNHCR may seek the individual's permission to include a caregiver, or other support person, if this is considered safe. Such a person can facilitate understanding or communication and should be used to support his/her ability to understand and provide consent (rather than a form of substitute decision-making). If it is determined that an individual is not able to adequately understand the process, and its ensuing rights and obligations, UNHCR personnel may decide to process the data on an **alternative legitimate basis, such as vital and best interests**.

4. Other data protection principles

4.1. Purpose specification

4.1.1 The purpose specification principle, also referred to as purpose limitation principle, is **one of the key principles** in the field of data protection. It is linked to several other principles notably to the legitimate basis, necessity and proportionality, the right to information, the data security and the accountability principle. **Without clarity about the specific purpose(s) for data processing** it is difficult or impossible to determine the appropriate legitimate basis, the minimum necessary data elements to be processed, fully inform the data subject, set up the necessary data security measures and for data controllers to take responsible decisions.

4.1.2 The Data Protection Policy only deals in one paragraph with the principle. In para. 2.3 of the DPP, reference is made to the need for the purpose(s) for the collection to be (i) specific, and (ii) legitimate. Furthermore, there should be **no processing incompatible with such purpose(s)**. The Policy also states that it is up to the data controller, assisted by the data protection focal point, to determine the specific and legitimate purpose(s) of data processing (para. 7.2.2 of the DPP). In the following, additional guidance is provided for the proper understanding of this principle including some practical examples.

4.1.3 Data controllers need to determine and manifest the specific purpose(s) **before** the collection of personal data[12]. In particular in case of large population groups where direct contact to POCs is rare and difficult, country operations are advised to carefully reflect upon all specific purposes, especially transfers to partners and third parties well ahead in order to provide this information to the data subjects, e.g. at the time of registration.

4.1.4 With regard to the level of specificity, the advice is to be **as specific as reasonably possible**. For example, instead of referring to the protection of refugees, the precise activities need to be clearly stated, such as the issuance of asylum-seeker certificates, conducting needs assessments or monitoring the situation of asylum-seekers in detention. Equally, instead of referring to general types of assistance (e.g. cash or food), data controllers are encouraged to specify the purposes such as authentication at the point of food or cash collection or post distribution monitoring. This is not only important for the purpose of complying with the informed consent requirement and the right to be informed (para. 3.1 (i) of the DPP) but also in order to reflect the specific purpose(s) in data transfer agreements (as required in para. 6.2.2 (i) and 6.1.2 (ii) of the DPP).

[12] See Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, Working Paper 203, adopted on 2 April 2013, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

4.1.5 The legitimacy of the purpose(s), should not be equated with the legitimate basis principle. Legitimate purpose(s) for UNHCR are those that are **compatible with its mandate** in the broad sense, including, e.g. the providing of good offices. Moreover, what is legitimate for a third party may not be legitimate for UNHCR.

4.1.6 Further processing needs to be compatible with the initial purpose(s). This logically follows from the Policy. New purposes require a new legitimate basis. "Function creep", or a situation where the same systems and/or data sets are used for other purposes than the ones originally designated, would be incompatible with the purpose specification principle. Typical **examples for compatible purposes** are the use of personal data by the data controller for statistics, archiving and scientific or historical research[13]. In the specific UNHCR context, processing personal data for a solution such as resettlement or voluntary repatriation not previously communicated to the data subject requires a new legitimate basis, i.e. consent. Offering a new type of assistance or service would also be a new purpose requiring a new legitimate basis, even though not necessarily consent. However, replacing an existing project partner by a new partner for an identical project could be considered a compatible purpose. It would be **within "reasonable expectations" of POCs** that UNHCR proceeds that way provided there are no valid concerns about the acceptance of the partner. In such scenarios, UNHCR is encouraged to update the information it provides to POCs and communicate the programmatic changes through committees and other fora of communication to ensure that POCs are informed of the change and may opt-out of data sharing if they wish to.

4.2. Necessity and proportionality

4.2.1 The necessity and proportionality principle is **closely linked with the purpose specification principle**. What is necessary and proportionate in terms of data processing needs to be judged against the specific and legitimate purpose(s). The Policy clarifies that "data that is processed should be adequate and relevant to the identified purpose, and not exceed that purpose" (para. 2.4 of the DPP). The principle is also known as '**data minimization**' principle.[14]

4.2.2 Whether for internal data collection purposes or when deciding what data can be transferred to third parties, UNHCR personnel should always seek to limit or minimize the

[13] See Article 5 (b) of the GDPR.

[14] See Article 5 (4) (c) Modernized Convention 108 and Article 5 (c) of the GDPR. See also European Union Agency for Fundamental Rights (FRA) and Council of Europe, *Handbook on European data protection law*, 2018 edition, available at: http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law, Section 3.3 page 125.

personal data elements to those which are necessary for the specific purpose(s). The principle needs to be respected **by data controllers and data processors**. Unlike for other principles, para. 7.2.2 of the DPP does not explicitly allocate the responsibility to one of them. There are numerous examples of this joint responsibility in UNHCR's practice, in particular in activities that require interviewing or counselling POCs. While guidance on how to conduct counselling during registration, RSD interviews, BID procedures, needs or participatory assessments may have been developed or provided by data controllers (as part of their responsibility to ensure overall compliance with the Policy, para. 7.2.1 of the DPP), data processors need to implement general guidance and apply it when communicating with POCs.

4.2.3 In other examples, where the specific data elements that need to be collected are predetermined in internal guidance material supported by electronic systems or forms, e.g. registration levels in UNHCR's proGres data base, or in data transfer agreements (see in this respect para. 6.1.2 (iii) and 6.2.2 of the DPP), the responsibility for the respect of the necessity and proportionality principle would have been entirely shifted to the data controller. In situations where data processors have a certain margin of discretion, for instance in RSD interviews or during assessments, they should not feel unduly restricted in their exercise of data collection, but rather be guided by a clear understanding of the (specific and legitimate) purpose(s) of their activity. Another example concerns the designing of surveys, where UNHCR personnel are advised to distinguish carefully between what is necessary and what might only be "nice to know"[15].

4.3. Data accuracy

4.3.1 The data accuracy principle, at times also referred to **data quality principle**[16], is described in para. 2.5 of the DPP as the need to record personal data as accurately as possible to ensure they fulfil the purpose(s) for which they are processed. Every reasonable step should be taken to ensure that inaccurate personal data are deleted or corrected without undue delay, taking into account the purposes for which they are processed[17]. Data accuracy is closely linked to the ongoing **need for verification** of registration data and the need to **resolve inconsistencies** in the anti-fraud context[18].

[15] See on this aspect ICRC, *Handbook on Data protection in Humanitarian action*, Chapter 2, page 26, para. 2.5.3.

[16] See, e.g., ICDPPC, *The Madrid Resolution*, Principle 9.

[17] See also Article 5 (1) (d) of the EU GDPR.

[18] See UNHCR, *Handbook for Registration*, Part 1, Chapter 4 (para. 4.4 - Verification) and Part 2, Chapter 20 (Verification techniques), available at: http://www.refworld.org/pdfid/3f967dc14.pdf and UNHCR, *Policy on Addressing Fraud committed by persons of concern*, October 2017, para. 4.6.

4.3.2 UNHCR faces challenges in ensuring data accuracy, which are inherent in the nature of its work in situations of humanitarian crisis. For instance, when registering POCs, it may only rely on oral information provided by the individual without the possibility to verify such information with national civil registration authorities, notably in the country or area of origin. Depending on the purpose for data collection, or **the more important the data is, the greater the effort needed to ensure its accuracy**. An example in point concerns the establishment and evidence of identity and the increasing collection and use of biometric data for verification, authentication and authorization purposes.

4.3.3 In practical terms, the data accuracy principle can be implemented by the following measures:

(i) When informing POCs of their rights, stress the importance of **data subjects providing accurate and complete information**, the consequences of not doing so, as well as the requirement to notify UNHCR or partners of any changes in their personal situation (see para. 3.1 (iii) to (v) of the DPP);

(ii) Within logistical and security constraints, **periodically review, verify and update personal data sets**, e.g. through continuous registration and verification exercises (see para. 4.3.2 of the DPP);

(iii) that data which has been challenged, or which UNHCR has reason to believe is not accurate is **marked as such**, and steps are taken to follow up on potential inaccuracies, whenever feasible, e.g. in RSD procedures;

(iv) that the **source of data** as well as amendments or deletions are **recorded**.

4.4. Retention, disposal and return of data

4.4.1 Data retention has close links with the principles of necessity and proportionality; it is also considered as **storage limitation principle**[19]. In UNHCR's Data Protection Policy, it is dealt with in the section on data processing where it is stated that personal data is not to be retained longer than necessary for the purposes for which it was collected (para. 4.6.1).

4.4.2 This principle and its relevance in UNHCR is however limited because individual case files of POCs[20], whether open or closed, are considered **permanent records** (see

[19] See, Article 5 (1) (e) of the GDPR and Article 5 (4) (e) of Modernized Convention 108; see also FRA and Council of Europe, *Handbook on European data protection law*, Section 3.5, page 129.

[20] For the definition of 'individual case file', see above under Section 1.4 of this Guidance.

para. 4.6.2 of the DPP)[21]. The Archives of UNHCR exist to make the experience of UNHCR available to guide and assist UNHCR in planning and conducting its activities, and to provide information to meet the research needs of persons of interest to UNHCR, the scholarly community and the general public[22]. Similarly, it is generally recognized in data protection law that further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes is considered compatible with initial data collection purposes[23]. In UNHCR, country operations are encouraged to transfer permanent records to the Records and Archives Section (RAS) at any time when they are no longer needed for the day-to-day work to ensure safe and secure preservation[24].

4.4.3 With regard to personal data of POCs contained in other records or documents that are not part of an individual case file and hence **temporary records**, the respect of the retention limitation generally implies their destruction. For example, when it is found no longer necessary to retain distribution lists for assistance, transport manifests or household surveys, these records (and any backups) may be destroyed[25]. The destruction of temporary records needs to be formally authorized by senior management of the Country Office and the latter should contact RAS in advance of sending permanent records. In case of doubt whether records can be destroyed, operations should contact RAS for advice[26].

4.4.4 Pursuant to the Archives Policy, the **destruction of temporary records** should be done in a secure manner. Destruction means that retrieval is impossible. Safe disposal methods for hard copies include: the use of cross-cut shredders, the safe burning of papers or, in the case of large volumes, the outsourcing of physical document disposal to a specialized service provider. In this case, the contractual obligations should ensure that confidentiality is respected throughout the chain of custody and provide for the submission of disposal records and certification of destruction. For electronic records, it should be noted that the 'delete' functions on the vast majority of computer systems do not destroy infor-

[21] UNHCR, *Policy on the Management of UNHCR Records and Archives*, Annex B: UNHCR Summary of Records Schedules, December 2017, Section 2 (Identifying permanent records in the field), para. 3.

[22] UNHCR, *Policy on the Management of UNHCR Records and Archives*, Annex C, page 1, available at: http://www.unhcr.org/research/archives/3b03896a4/unhcr-archives-access-policy.html.

[23] See Article 5 (1) (b) and 89 of the GDPR.

[24] UNHCR, *Policy on the Management of UNHCR Records and Archives*, Annex B: UNHCR Summary of Records Schedules, Section 1 (Introduction).

[25] Ibid.

[26] Ibid.

mation from the hard disk, but only delete the address reference while leaving actual information on the computer. Data controller are advised to seek guidance from the IT Officer on secure data destruction or disk erasure tools that adhere to industry best practice. The IT Officer should oversee the physical destruction of any media containing electronic records, including audio and video and portable devices, and duly advice personnel not to throw away computers, laptops, tablets or smartphones that may contain personal data before wiping the hard disk. **Disposal records** indicating the time and method of destruction, as well as the nature of the records destroyed, should be maintained and may be requested by UNHCR, as part of project or evaluation reports[27].

4.4.5 Where **implementing partners** process personal data on UNHCR's behalf, partner organizations should either **return or destroy** such personal data in order to respect the limited retention principle. In line with para. 5.5 of the DPP, all Project Partnership Agreements (PPA) include provisions for the return and/or destruction of personal data of persons of concern after termination of the agreement[28]. In principle, all personal data relating to refugees and other persons of concern to UNHCR shall be physically returned to the Data controller and the partner is required to **certify in writing** that all copies have been destroyed, including any personal data disclosed to its sub-contractors. There are two exceptional situations to this general rule:

4.4.6 First, where a **partner is subject to an obligation to retain data** provided by or processed on behalf of UNHCR in accordance with a legal requirement, an established auditing procedure or other procedure agreed upon beforehand with UNHCR, it should certify in writing that (i) a data minimization review has taken place (only data which is needed is retained), (ii) that the data will no longer be actively processed and is stored in such a way that it can only be accessed or used for the purposes for which it is being retained; and (iii) that the data will be duly destroyed when the retention period (which should be clearly indicated by the partner) has elapsed.

4.4.7 Second, the **data controller may determine that destruction is not necessary**, for example where the implementing partner continues the service provision with other sources of funding. In such cases, the data controller should be satisfied that the partner seeks explicit consent from data subjects concerned and may request a copy of the data from the partner for further case management and/or archiving purposes.

[27] Ibid.

[28] UNHCR, *Standard Format Bipartite Project Partnership Agreement (UNHCR with non-governmental and other not-for-profit partners)*, available at: https://cms.emergency.unhcr.org/documents/11982/47020/Bipartite+PPA+-+NGO/2ac3aacc-adf6-492c-9ddc-1b8f242f1334, para. 13.25.

4.5. Confidentiality

4.5.1 According to para. 4.1.1 of the DPP, personal data is **by definition classified** as confidential[29]. Based on its content, certain personal data may also be classified as "Strictly confidential" if unauthorized disclosure could reasonably be expected to cause exceptionally grave damage[30]. The duty of confidentiality extends to all communications with persons of concern, and all data provided by them or obtained on their behalf by personnel and partners in the course of UNHCR's activities. It is also part of UNHCR's Code of conduct (Principle 6) and the UN Staff Rules (see Regulation 1.2 (i))[31].

4.5.2 Pursuant to para. 7.2.2 of the DPP, data controllers, assisted by the data protection focal point, need to implement, inter alia, measures aimed at ensuring data confidentiality and security. In para. 4.1.2, the DPP explains, in order to ensure and respect confidentiality, personal data must be filed and stored in a way that it is **accessible only to authorized personnel** and transferred only through the use of protected means of communication. As a consequence, data controllers are advised to ensure that such **authorized personnel is identified, on a "need to know basis"**, e.g. in Standard Operating Procedures, and kept up to date, bearing in mind regular staff rotation. With regard to data transfers, whether or not a data transfer agreement has been signed between UNHCR and the third party, UNHCR must seek written agreement from the third party that the personal data will be kept confidential (para. 6.1.2 (v) of the DPP).

4.5.3 UNHCR personnel should be aware that States are under an international legal obligation to respect the privileges and immunities of the United Nations Organization[32], of which UNHCR as a subsidiary organ to the General Assembly is part. Privileges and immunities are also a standard element of UNHCR's host country agreements; they serve the organization to fulfil its mandate in an independent manner. The immunity of UNHCR includes the inviolability of its records and archives, including the personal data it holds on POCs[33]. Any acts of search, requisition, confiscation, expropriation or other interference by

[29] See UNHCR, *Information Classification, Handling and Disclosure Policy*, December 2010, para. IV (1) (a) and (b), based on United Nations, *Secretary-General's Bulletin on Information sensitivity, classification and handling*, ST/SGB/2007/6 of 12 February 2007, available at: https://archives.un.org/sites/archives.un.org/files/ST_SGB_2007_6_eng.pdf, Section 1, para. 1.2 (a) and (b).

[30] Ibid, para. III (4) and ST/SGB/2007/6, Section 2, para. 2.3.

[31] UNHCR, *Code of conduct*, available at: http://www.unhcr.org/admin/policies/422dbc89a/unhcr-code-conduct-explanatory-notes.html, United Nations, *Staff Regulations*, available at: https://hr.un.org/content/staff-rules-and-staff-regulations-united-nations.

[32] See Article 105 of the UN Charter and the *Convention on the Privileges and Immunities of the United Nations,* adopted by the General Assembly of the United Nations on 13 February 1946, available at: http://www.un.org/en/ethics/pdf/convention.pdf.

[33] Article II Section 3 of the 1946 Convention.

national authorities, whether based on executive, administrative, judicial or legislative action (including orders of disclosure from national courts), constitute a violation of UNHCR's immunities, and should be brought to the immediate attention of the Legal Affairs Services (LAS) in Headquarters.

5. Rights of persons of concern as data subjects

5.1. Introduction

5.1.1 Applying a right-based approach, UNHCR is committed, through the Data Protection Policy, to respect a set of rights of persons of concern, as data subjects, namely:

(i) the right to **receive information** about data processing by UNHCR and its partners;
(ii) the right to **request access** to data held by UNHCR and its partners;
(iii) the right to **request the correction and/or deletion** of that data; and
(iv) the right to **object** to the processing of their data

5.1.2 The right to information is also referred as **transparency or openness principle** and data subject's rights accordingly only include points (ii) to (iv)[34]. Elsewhere, a broader transparency principle appears alongside the right to information[35] or the latter is combined with the right to access[36]. The formulation of para. 3.1 of the DPP provides for a **pro-active obligation on the part of UNHCR to inform data subjects**, while the other rights are subject to a request. The different approaches should therefore not lead to differences in the treatment of data subjects. The rights as set out in UNHCR's Policy are all rooted in the universal right to privacy and reflected in General Comment No. 16 of the Human Rights Committee[37].

[34] See, e.g., ICDPPC, *The Madrid Resolution*, Part II, para. 10 and Part IV, para. 16 to 18.

[35] Chapter III, Section 2, Articles 12 to 15 of the GDPR.

[36] For instance, in Article 8 (b) Modernized Convention 108.

[37] UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, available at: http://www.refworld.org/docid/453883f922.html, para. 10.

5.2. The right to information

5.2.1 The UNHCR Data Protection Policy combines **several types of information** about which UNHCR should inform an individual when collecting personal data, including information about the intended data processing and its purposes, as well as the data subject's rights, how to file a request and the importance of providing accurate information (see the full list in para. 3.1 (i) to (viii) of the DPP). In addition, UNHCR personnel should stress that data will be kept confidential, not shared with the country of origin and explain, to the extent practical, the benefits and risks of data processing and transfers in the specific operational environment including anti-fraud messaging appropriate to the operational context[38]. Where it is not possible to provide persons of concern with all the requisite information about UNHCR's data processing at the first point of data collection, for example due to the scale of an emergency, this information should be provided at the next practical opportunity.

5.2.2 Access to information about data processing is a pre-requisite to informed decision-making by persons of concern in respect to their personal data, including the possibility of exercising their rights to access, correction and deletion or objection. As a rule, **information should be provided before personal data are processed**, orally or in writing, as transparently as circumstances allow and, if possible, directly to the individual concerned[39]. In addition, and where this is not possible due to the size of the population of POCs, UNHCR operations are recommended to integrate the provision of information about data processing into their communication strategies with POCs, for example through mass information campaigns, websites, community outreach initiatives, meetings with community leaders and committees, leaflets and information notices. **Information should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language**, and should be communicated through appropriate means (e.g. visual, audio and easy to read) to improve access for persons with visual, hearing and intellectual impairments.

5.3. The right to access personal data

5.3.1 In para. 3.2, the Data Protection Policy provides that data subjects may receive from UNHCR (i) confirmation as to whether UNHCR processes any personal data on them and (ii) information on the personal data being processed, the purpose(s) for processing such data and the partner(s) and/or third parties to whom such data has been, is being or will be transferred. While each request should be considered on a case-by-case basis,

[38] UNHCR, *Policy on Addressing Fraud committed by persons of concern*, para. 4.2 a).

[39] ICRC, *Handbook on Data Protection in Humanitarian Action*, Chapter 2, para. 2.10, page 36.

having regard to the legitimate interest of the data subject in accessing his or her personal data, data controllers are generally advised to adopt an **approach whereby granting access should be the principle and refusal the exception**.

5.3.2 This applies to personal data that is included in documents POCs have provided to UNHCR. Examples are passports, identity documents, marriage or birth certificates, education records, photos, medical records, or any documentary evidence of activities or incidents in the country of origin provided in support of a refugee status application. **Access to copies of documents provided by POCs**, e.g. in case of loss of the original by the POC, **should in principle be unrestricted**. UNHCR should not keep originals of documents provided by POCs.

5.3.3 The situation differs when it comes to **personal data in documents or records generated by UNHCR ("internal work products")**, or by an implementing partner on UNHCR's behalf, such as interview records or case processing assessments. While data controllers are advised to strive to ensure a **high degree of transparency** towards persons of concern, they also need to exercise his/her discretion and may withhold specific documents or records, in part or in full, for instance where this would reveal personal data of others or where documents are classified as "confidential" or "strictly confidential". The RSD Procedural Standards and the Resettlement Handbook contain more detailed advice with regard to respective procedures[40].

5.3.4 Where UNHCR has received **personal data of POCs from a project partner or third party**, UNHCR may provide the individual with information about the source of the personal data it has received with the exception of information that was provided on condition of (or with a reasonable expectation of) confidentiality, or which would otherwise harm UNHCR's operations or third-party relations. If personal data is held by a partner or third party, UNHCR should explain the specific purpose(s) of the transfer from UNHCR to that partner/ third party and refer the data subject to the partner or third-party data for any further information about the data processing.

[40] UNHCR, *RSD Procedural Standards - Legal Representation in UNHCR RSD Procedures*, 2016, ("RSD Procedural Standards"), available at: http://www.refworld.org/docid/56baf2c84.html, Section 2.7.4 (b) and UNHCR, *Resettlement Handbook*, 2011, available at: http://www.unhcr.org/46f7c0ee2.pdf, Section 7.5.7.

5.4. The right to request correction or deletion of personal data

5.4.1 The Data Protection Policy grants refugees and other persons of concern the right to request the correction or deletion of their **own personal data which is inaccurate, incomplete, unnecessary or excessive** (para. 3.2.1). Whether personal data is indeed inaccurate or incomplete needs to be verified. For this reason, para. 3.2.2 of the DPP requires UNHCR to request proof relating to the inaccuracy or incompleteness. However, it is acknowledged that proof is not always available in the context of forced displacement. UNHCR personnel is therefore advised to **apply appropriate verification techniques** as developed in the registration context in order to assess requests[41].

5.4.2 Requests for correction may often occur in the course of routine case processing, for example when an individual is handed an attestation letter and notices that his/her basic biodata is recorded incorrectly. Some may be obvious and be handled quickly, others may require thorough verification of the proof or other information supporting the request. In general, upon receipt of a request, responsible UNHCR personnel is therefore advised to:

(i) **request proof** relating to the inaccuracy/incompleteness of data (if relevant), and

(ii) **assess the legitimacy** of the request and the credibility of the proof or information provided in support of the request, using for instance verification techniques in the context of registration procedures.

If the responsible staff member (based on his/her function or assigned responsibilities) finds the request credible, the data should be amended. In accordance with UNHCR's obligations to maintain records (see Section 8.1), personnel is advised to record the fact that a POC has requested a correction and UNHCR accepted or not such requests in the individual's file.

5.4.3 Where the responsible staff member has **grounds for believing that a request is manifestly abusive, fraudulent or obstructive**, for example, a request to correct parts of an interview transcript, or change information that could impact eligibility for refugee status or resettlement without justification, it may be subject to the restrictions set out in para. 3.7 (ii) of the DPP. Such requests should be declined and, in addition, may necessitate fraud detection procedures[42].

[41] See UNHCR, *Handbook for Registration*, available at: http://www.refworld.org/pdfid/3f967dc14.pdf, Part 2, Chapter 20.

[42] On the detection and response to fraud, see UNHCR, *Policy on Addressing Fraud Committed by Persons of Concern*, para. 4.3.

5.5. The right to object to processing of personal data

5.5.1 Data subjects are entitled to object to data processing, based on the condition that there are **legitimate grounds related to his or her specific personal situation**. The key issue with the right to object is to assess the legitimacy of the grounds put forward by the data subject related to his or her specific situation. For example, an asylum-seeker may request that his or her personal data are not transferred to the host country or to a particular partner over concerns, due to his or her particular profile, for his or her safety or security or that of family members.

5.5.2 If the objection is deemed to be justified, **processing should be limited to the remaining legitimate purpose(s)**, for instance registration or archiving. If the objection concerns the transfer of personal data to a third party, the relevant data elements may be removed from UNHCR systems and tools or reducing access rights, thereby rendering it inaccessible to third parties. Some requests may however also be resolved by thorough counselling, alternative forms of assistance or protection or raising the underlying issue with a partner without referring to the individual case. Where an alternative form of assistance is not feasible, the individual should be counselled to that effect.

5.5.3 In assessing objections, UNHCR personnel is also advised to (i) verify the original legitimate basis because, if it is consent, objection would normally imply the withdrawal of consent, (ii) whether there is an alternative legitimate basis for continued, albeit restricted processing, for example to maintain records (including for archiving) and (iii) whether the processing is still necessary and proportionate to the purpose. **The right to object is not another form of the right to deletion**. Finally, a request for withdrawal of a refugee status application would not be considered as an objection but rather as a specific procedure within RSD that would lead, following counselling, to file closure[43].

5.6. Restrictions of the rights of data subjects

5.6.1 The right to privacy is not an absolute right and needs to be weighed against other fundamental rights and public interests, in accordance with the principle of proportionality. In para. 3.7 (i), the Data Protection Policy refers to necessary and proportionate measures to safeguard the safety and security of UNHCR, its personnel or the personnel of its partners or the overriding operational needs and priorities of UNHCR in pursuing its mandate. In line with other policies[44], this may be interpreted as information the disclosure of which

[43] See UNHCR, *Procedural Standards for RSD, Unit 9 - Procedures for File Closure,* available at: http://www.refworld.org/rsdproceduralstandards.html, Section 9.1.

[44] For instance, UNHCR, *Policy on Addressing Fraud Committed by Persons of Concern*, *Information Classification, Handling and Disclosure Policy* and *The Role, functions and modus operandi of the Inspector General's Office*.

could jeopardize the rights of other individuals or cause damage to the work of UNHCR and therefore is, or ought to be, classified as “confidential” or “strictly confidential”.

5.6.2 In practice, this may include **Information on the physical or mental health** of the individual, or other persons, where disclosure is likely to cause serious harm or undermine the provision of essential services; the **privacy** of other persons of concern, their family members or persons with whom they are associated, unless they have given their consent, **criminal investigations** or prosecutions where UNHCR has processed personal data on its own initiative or in response to a legitimate request from national authorities, UNHCR’s **anti-fraud or integrity efforts** where disclosure could undermine specific investigations or the functioning of its detection and investigation procedures, **investigations by the IGO** in respect to staff misconduct vis-à-vis POCs, **information provided by a third party** on condition of, or with a reasonable expectation of confidentiality.

5.6.3 Moreover, UNHCR may refuse requests for any of the data subject’s rights if there are grounds for believing that the request is manifestly abusive, fraudulent or obstructive to the purpose of processing (para. 3.7 (ii) of the DPP). **Abusive requests** include, but are not limited to, repeated identical or similar requests from the same individual (unless a reasonable interval has elapsed), or requests that constitute an obvious attempt at abuse of process**. Fraudulent requests** include, but are not limited to, situations in which the identity of the person or the authority of their legal representative cannot be verified or is in doubt. Requests that raise inconsistencies that cannot be resolved by the functional UNHCR unit or that are deemed to be significant in nature are to be referred to the operation’s Anti-Fraud Focal Point[45]. **Obstructive requests** include, but are not limited to, requests or objections that have no reasonable foundation and ‘bulk requests‘ that are clearly designed to frustrate or obstruct the effective implementation of UNHCR’s mandate.

5.7. Procedural aspects

5.7.1 Under para. 7.2.2 (iii) of the DPP, it is the responsibility of the data controller to establish internal procedures, in particular regarding the respect for the rights of the data subject. In para. 3.5 (modalities of requests) and 3.6 (recording and response), the Data Protection Policy provides some guidance with regard to procedural aspects. This is however not exhaustive. In the following, further guidance and proposals are provided regarding how such procedures could be designed and which points they should include. In line with the purpose and rationale of the Policy, such procedures should be **fair and efficient** with a view to **enable data subjects that their rights are respected**.

[45] UNHCR, *Policy on Addressing Fraud Committed by Persons of Concern*, para 4.7.

5.7.2 Procedures for the rights of data subjects could be set out in **Standard Operating Procedures** (para. 7.2.2 (iii) of the DPP). Such SOPs could cover, as suggested in the Policy, all relevant data protection aspects, including data security and data transfers. Alternatively, the procedure(s) for requests of data subjects could be integrated in existing SOPs, for instance on registration, RSD and/or resettlement. They should however **not be confused with general complaint procedures** foreseen in these areas[46]. While there may be overlaps, e.g. an asylum seeker may complain about a registration clerk who refuses to correct certain personal data elements in his or her file, both pursue different objectives: The complaint about the staff concerns a certain behavior, potentially misconduct, and the way services are delivered while the request for correction concerns the respect of a specific right related to the processing of the data subject's personal data. Also, the person responsible for dealing with general complaints may not necessarily be responsible for dealing with a request related to personal data processing.

5.7.3 Procedures for requests for the rights of the data subject could usefully address the aspects of: (1) how data subjects are informed of their rights, (2) who is entitled to file a request, (3) how to make a request, and (4) aspects on the handling of and the response to requests, including the designated responsible person for dealing with requests. These four aspects are elaborated further below listing points that could be included in SOPs.

5.7.4 On the **information of data subjects** of their rights (see also para. 3.1 (viii) of the DPP):

(i) Where UNHCR conducts registration, RSD and/or resettlement, information related to the rights of the individual as data subject, i.e. access, correct, delete or object, are usefully integrated in such procedures and provided individually, e.g. ahead of respective interviews.

(ii) Where UNHCR does not carry out any of the above-mentioned procedures but nevertheless processes personal data, for instance in the context of monitoring activities, the data subject should, wherever possible be counselled and advised individually.

(iii) In large operations, whether camp-based or in urban contexts, data controllers are advised to provide relevant information also through other ways of communication that are appropriate in their respective operational environment(s). Reference is made to para. 8.1.2 above.

[46] See UNHCR, *Handbook for Registration*, available at: http://www.refworld.org/pdfid/3f967dc14.pdf, Part 2, Chapter 13, Section 13.3 ('Establish complaint procedures'), *Procedural standards for RSD*, available at: http://www.refworld.org/docid/42d66dd84.html, Section 2.6, page 2-22 ('Complaint procedures') and *Resettlement Handbook*, available at: http://www.unhcr.org/46f7c0ee2.pdf, Chapter 4, page 133 ('Complaint mechanism').

5.7.5 The following persons are **entitled to file a request**:

(i) The data subject;

(ii) Legal representatives, parents or legal guardians on behalf of the data subject whom they represent (para. 3.5.1 of the DPP). In the case of parents and legal guardians, the responsible UNHCR staff member should verify whether there are reasons to believe that it is not in the best interest of the child to release such data to a parent or legal guardian;

(iii) Children themselves who are able to express their consent or assent to data processing may also submit requests in their own right (for more details, see below). Although family members may have a legitimate interest in seeking to access data related to their relatives, these are not entitled to make requests on behalf of data subjects; such requests should be dealt with in accordance with the conditions for data sharing with third parties;

(iv) Legal representatives should present a designation of legal representation (power of attorney). 'Bulk requests', where a legal representative submits requests on behalf on several POCs, should, to the extent possible be handled in the same way as individual requests (taking into consideration available capacity and resources).

5.7.6 On the ways and conditions for **filing a request**:

(i) Requests can be made orally or in writing (para. 3.5.1 of the DPP);

(ii) Requests are to be submitted to the UNHCR office in the country where the data is being processed (para. 3.5.1 of the DPP). However, data controllers are advised not to conceive this as a formal requirement. The idea is to bring requests quickly to the attention of the person responsible for responding to them. Oral requests or requests addressed to an implementing partner should be re-directed to the responsible person in the UNHCR office in which the individual's data is being held, including UNHCR's RAS.

(iii) Requests and their response are always free of charge;

(iv) Requests do in principle not require reasons as a formal condition. Where information from the data subject is necessary, e.g. to verify his or her identity but also to respond to requests for correction or objection, UNHCR personnel is advised to seek such information from the data subject in a spirit of dealing with the request in a fair and efficient way.

5.7.7 On the **handling of and the response to requests**:

(i) Designation of the **responsible person** for dealing with and responding to requests by data subjects on behalf of the controller. Considering the responsibility of this function, data controllers are advised to designate a responsible

person at senior level. Recommended practice is to designate the data protection focal point, who, according to the Data Protection Policy, is in principle the most senior UNHCR protection staff member (para. 1.4 and 7.2.1). In large operations with several Sub-Offices and Field Offices, the data controller may choose to designate responsible persons in each Office with a system of sub focal points;

(ii) SOPs may identify **manifestly well-founded requests**, which, for efficiency purposes, could be handled by staff directly dealing with data subjects as part of routine case management procedures, for example requests to amend or update basic biographical data, such as contact information (address, phone number etc.) or personal situation (births, deaths, marriages etc.) in the context of continuous registration. Such staff members will also usually be able to verify the identity of the requesting individual, e.g. by conducting a visual inspection of an identity document or consult UNHCR's BIMS.

(iii) According to the Policy, UNHCR is to **record** requests received for access, correction, deletion or objection and the response provided in relation to such requests (para. 3.6.1);

(iv) Before complying with a request, the responsible person should **verify the identity** of the person making the request in order to ensure he or she is entitled (see above and para. 3.5.2 of the DPP). In particularly sensitive cases, or in the case of suspected fraud, the office may request attestation from a notary with statutory authority to confirm identity and/or the validity of official documentation.

(v) UNHCR is to respond to a request within a **reasonable time** (para. 3.6.2 of the DPP), recommended are 30 days;

(vi) The response should be crafted in a **manner and language that is understandable** to the data subject and/or his or her legal representative or legal guardian as applicable, orally or in writing (para. 3.6.2 of the DPP). As a general rule, the response should be in writing, in particular if the request is in writing. For efficiency, oral responses may be more appropriate in cases where requests can be responded immediately and positively;

(vii) The **character of procedures** on requests of data subjects should respect the dignity of the individual and confidentiality;

(viii) The response should **explain the action taken** in responding to the request and **provide reasons** where requests cannot be met, for example why access cannot or be granted only partially, why a correction cannot be made (e.g. because of lack of evidence), why deletion is not possible (e.g. because data in permanent records) or an objection cannot be respected (e.g. because of operational priorities and insufficient grounds related to the specific personal situation). Exceptions are justified where the provision of reasons would itself jeopardize or cause damage to the work of UNHCR due to the nature of an applicable restriction (e.g. fraud).

(ix) The **application of a restriction** based on para. 3.7 of the DPP should be carried out on a case-by-case basis with an individual assessment of each decision;

(x) A response to a request for access may contain documents concerning the requesting data subjects that also contains **personal data of other individuals and/or classified information**. In this case, redacting any personal data of other persons, including UNHCR or partner personnel by blackening relevant passages may be a solution to maintain a high degree of transparency. The data controller may decide to be consulted in such cases to ensure that all relevant data has been excluded prior to disclosure. A copy of the disclosed material showing the redactions is to be added to the individual case file.

(xi) In the case of requests raising complex questions in respect to UNHCR's mandate, relationship with third parties or potential security implications, the data controller may seek the advice of the DPO (para. 7.2.3 of the DPP).

5.7.8 In the case of **requests from children or persons with mental health conditions or intellectual disabilities**, SOPs may provide for the following: Before responding to a request by a child, the responsible person, in consultation with child protection personnel, should be satisfied that:

(i) The child is able to express consent or assent (see above Section 6.7) and understands the meaning of making a request and how to interpret any information he or she receives in response, and

(ii) The request has not been made under duress.

If these conditions are met, the request can be treated in the same way as requests from adults.

5.7.9 If they are not met, the responsible person is advised to initiate a best interest procedure before disclosing any information in response to the request, considering:

(i) Best interest determinations or assessments relating to parental responsibility which already apply to the child´s case;

(ii) The nature and sensitivity of the personal data and the consequences of allowing those with parental responsibility to access it;

(iii) Any allegations of abuse or ill treatment;

(iv) The views the child has on whether their parents/legal guardian should have access to information about them (in the absence of which it would normally not be released);

(v) The potential detriment to the child if those with parental responsibility were prevented from accessing the information.

A best interest determination should also be made in respect to requests made by a third party who has the right to manage the affairs of a persons of concern who, due to mental

health conditions or intellectual disabilities, is believed to lack capacity to adequately understand the process.

5.8. Role of the Inspector General's Office

5.8.1 As part of the right to information the data subject should also be informed about their right to lodge a complaint with the IGO (para. 3.1 (viii) of the DPP). The Data Protection Policy does not affect the mandated functions of the Office of the Inspector General (IGO), which includes the investigation of possible misconduct of UNHCR personnel, or any other entity that has contractual links to UNHCR, including staff of partners or commercial service providers (para. 7.4 of the DPP). In the context of data protection, this could, for example, be a UNHCR staff member disclosing or providing access to personal data of persons of concern to an unauthorized third party.

5.8.2 The IGO has also a mandate to conduct *ad hoc* inquiries into violent attacks on UNHCR operations where these entail large-scale damage to UNHCR assets[47]. This could include personal data of persons of concern, for example in the case of a serious data breach. The IGO may therefore, in exceptional circumstances, form part of the Data Breach Task Team (see para. 10.3.6 below).

5.9. Role of the Ethics Office

5.9.1 The Ethics Office seeks to foster a culture of ethics, transparency and accountability in UNHCR, and to identify potential ethical dilemmas and conflict of interest in the workplace, so that appropriate steps can be taken to prevent problems before they arise. The main responsibilities of the Ethics Office are to: (a) provide confidential advice and guidance to staff and senior management on ethical issues; (b) promote a culture of integrity and accountability, raise awareness and develop standards and education on ethics issues; (c) implement the policy on protection of staff against retaliation ("whistle-blower policy"); and (d) strengthen the response to, and prevention of, sexual exploitation and abuse.

5.9.2 In the context of data protection, the Ethics Office may provide guidance on the protection of "whistle-blowers", for example if personnel are concerned about the handling of personal data in their operation, notably on the reporting on personal data breaches, or advise staff on how to address ethical problems in relation to their personal conduct, for example in the context of disclosure of personal data of POCs. While procedurally the Ethics Office does not receive complaints directly from persons of concern, it may provide support to UNHCR personnel reviewing such complaints or having concerns about their office's data protection practices.

[47] UNHCR, *The role, functions and modus operandi of the Inspector General's Office*, February 2012, para. 2 (Mandate).

6. Data security

6.1. Context

6.1.1 In a context of increasing collection of personal data, the use of multiple ICT assets including portable equipment, storage in a range of electronic data bases, transfers through various means and tools to a growing number of partners and other third parties and, in particular, the threats by a variety of adversaries, including criminal organizations, so-called hacktivists, state agencies and non-state actors with an interest in accessing confidential information about POCs to UNHCR, the importance and challenge of data security cannot be underestimated.

6.1.2 The Data Protection Policy acknowledges these challenges and, bearing in mind the particularly vulnerable position of POCs to UNHCR and the generally sensitive nature of their personal data, demands careful handling (para. 1.2.1), a high level of data security (para. 4.2.1) and the implementation of appropriate organizational and technical measures (para. 4.2.2), including the "privacy by design" approach (para. 4.2.3). In addition, the Policy takes into account the availability and quality of necessary equipment, the cost and the operational feasibility (para. 4.2.1 and 4.2.3).

6.1.3 The Data Protection Policy does not define the data security standards UNHCR should have in place. In general terms, which security measures are appropriate, at global and country operational level, will depend on the nature of personal data to be processed, the potential harm to POCs that could result from a personal data breach, the likelihood of a breach materializing, and the availability and quality of the required equipment, cost and feasibility. The Division of Information Systems and Technology (DIST) is responsible for elaborating ICT related standards and guidance.[48]

6.1.4 The Data Protection Policy underlines the responsibility of the data controller who should ensure the implementation of organizational and security measures (para. 7.2.2 (ii) of the DPP). Irrespective of organizational measures typically falling under the purview of the data controller, data security is a responsibility of all UNHCR personnel[49]. In this Chapter, guidance is developed and provided on the notions of organizational and technical measures, the privacy by design approach, certain data security procedures and practices, secure communication and data transfers and personal data management in high risk environments and deteriorating security situations.

[48] UNHCR, *Operational Guidelines on ICT Security, approved by the Director and CIO, DIST*, October 2014.

[49] Ibid., at Section 3.

6.2. Organizational measures

6.2.1 The organizational measures referred to in para. 4.2.4 of the DPP are not exhaustive. Data controllers, assisted by their data protection focal points and other relevant staff, are encouraged to:

(i) At country level, ensure that relevant data security measures are covered in Standard Operating Procedures (para. 4.2.4 (i) of the DPP), e.g. procedures for physical and electronic file management;
(ii) Ensure that trainings in data protection are organized or attended, including for Implementing partners (para. 4.2.4 (ii) and para 5.4 of the DPP);
(iii) Raise the awareness for the responsible use of UNHCR's ICT assets and resources including email, internet, portable devices and ICT equipment;
(iv) Ensure the conduct of Data Protection Impact Assessments (para. 4.2.4 (iii) of the DPP);
(v) Implement methods of safe transfer for personal data of POCs;
(vi) Routinely review and upgrade data security measures, e.g. through random monitoring and inspections and testing, assessing and evaluating the effectiveness of existing measures;
(vii) Share relevant SOPs with and keep the DPO informed of organizations measures.

6.3. Technical measures

6.3.1 Under technical measures, the Data Protection Policy mentions the maintenance of physical security of premises, portable equipment, individual case files and records (para. 4.2.5 (i) and ICT security through a number of control measures (para. 4.2.5 (ii) of the DPP). This section elaborates on physical and electronic file management and distinguishes storage, access and user control that apply to both forms of file management. For the definition of individual case file, refer to the definitions in Section 4 of this Guidance. Data controllers may delegate the implementation of technical measures to their data protection focal points together with, for instance, registration and IT staff.

Physical file management

6.3.2 **Storage control**. Responsible personnel is advised to observe the following:

(i) Case files are kept in a lockable storage room or location designated for this purpose within UNHCR's premises, safe from water, fire and temperature damage;
(ii) Access to the storage room to be controlled, monitored or restricted, for example, through access cards, physical control barriers, local or remote monitoring systems, with only authorized personnel granted access to enter;

(iii) The storage location needs to be kept locked when unattended. Copies of the key(s)/access cards are normally kept only by the Filing/Registration staff and the Representative and/or senior protection staff;

(iv) Outside the storage room, case files should be kept in a locked cabinet or drawer when personnel dealing with it is not at his/her desk or out of office, even for short breaks;

(v) Files should not be kept in interviewing rooms unless personnel are present;

(vi) Access to UNHCR premises should be regulated, visitors logged in and out, and accompanied by UNHCR personnel inside the premises and offices (the Field Safety Advisor or the Field Security Service can be consulted for further guidance).

6.3.3 **Access control** to physical files (within and outside the designated storage location):

(i) Case workers should have access to physical files of cases that have been assigned to them, in line with their duties and responsibilities, for instance registration, RSD, BIA/BID, resettlement or specific tasks;

(ii) Reviewing officers should have access to files they are responsible for reviewing and for quality checks, in line with their duties and responsibilities;

(iii) Non-protection personnel may only request access to case files through the Senior Protection Officer (or equivalent) within each office;

(iv) Interpreters should normally not have access to individual case files. Where they exceptionally have been assigned tasks related to case processing, as approved by the data controller, access to individual files needs to be strictly limited to necessary documents related to authorized responsibilities, and should be closely supervised.

6.3.4 **User control**. Tracking and recording the movement of physical files:

(i) A file check-out/check-in procedure should be in place, with an up-to-date record of who has, and have in the past had, access to individual case files;

(ii) The Filing Clerk should register the file number, date, and initials/name of the personnel requesting the file onto the file movement log upon release, and note its date of return and initials/name of the personnel who returned it;

(iii) Requests, releases, transfers and returns of files should normally be recorded on a File Action Sheet. File movement logs should be sought stored electronically wherever possible (in proGres or an alternative database). Larger operations may also consider implementing an electronic tracking system by attaching barcodes to their files, and issuing identification with barcodes to personnel;

(iv) UNHCR personnel may not remove individual case files from UNHCR premises. Exceptions may be authorized by the data controller or Senior Protection

Officer based on a written request. There should be a limit to the number of files an individual caseworker can have in his/her possession at any given time (normally a maximum of 20).

6.3.5 General advice on **individual case files management**:

(i) Create, assemble and verify Individual case files at the time of registration;
(ii) Clearly mark files on the outside with the file number (or unique identification);
(iii) In principle, one file for one POC in one office for use by all functional units;
(iv) Insert action sheet, including of all actions and dates related to the case (scheduled interviews, referrals, house visit, added or removed documents etc.) and keep up-to-date;
(v) Keep documents in chronological order (newest documents placed on top);
(vi) Non-digitized photographs recommended subject to tamper-proofing measures (such as dry or wet seal stamps), with the name and registration number of the POC on the back;
(vii) Mark all documents which are copies with “copy” or “copy of copy”;
(viii) Keep only copies of original documents provided by a POC and hand back original. The copy should be noted “copy” and “original seen”;
(ix) Internal notes to be dated and signed, with the name and title of the case-worker;
(x) Consider keeping strictly confidential information, e.g. medical records, in a sealed and tamper-proof envelope, clearly marked as such, within the physical file.

Electronic file management

6.3.6 Personal data stored in electronic format is particularly vulnerable to accidental, unlawful or illegitimate destruction, loss, alteration, as well as unauthorized disclosure, due to the ease with which it can be copied, transferred, and even posted on the Internet. Access to such data should therefore be carefully restricted, managed and monitored. Data controllers, with close support from IT Officers, are responsible for ensuring that databases and supporting IT infrastructure are established and used according to standard, including the following measures:

6.3.7 **Storage control**

(i) Operations are advised to only use corporate UNHCR tools, document management applications, and network drives with controlled accessibility (in case of doubt seek DIST support and advice). The use of non-UNHCR approved tools (“shadow IT”) can undermine data security;
(ii) Server locations need to be physically secure, with adequate electrical, water and fire safety. IT Officers are responsible for adequate back-up procedures;

(iii) Offices with reliable access to the internet are advised to store electronic files in e-SAFE; offices without such access should establish a restricted shared drive. Personal data of POCs should not be stored on personal network drives.

6.3.8 **Access control to electronic files**

(i) Access to electronic files should be tiered, so that personnel only have access to what they need to for the purposes of performing their duties and responsibilities;

(ii) Operations are recommended to establish procedures for the submission and review of user access requests to ensure that users are only given access to the data they need. Access rights are normally defined by the Heads of Units, approved by the data controller, and updated by a database administrator in line with Administrative Instructions on Access Controls Management issued by DIST[50];

(iii) A regular review of access rights is recommended, e.g. every 6 months, to ensure that personnel who no longer require access have their permissions revoked.

Audio and video recording of counselling and interviews with persons of concern

6.3.9 Operations which are using audio recording when counselling or interviewing should ensure that these recordings are stored securely (preferably in e-SAFE) with access restricted to authorized personnel only. Recording devices should be kept in a secure location, and all electronic copies of videos/tapes clearly linked to a physical file, and securely disposed of when their retention periods have elapsed or are no longer needed. Operations which are considering introducing cameras in interview rooms and/or video recording for interviews with persons of concern are recommended to consult the DPO, FSS, and DIST in Headquarters, in order to reach the best decision based on security, data protection and case management considerations.

6.4. Privacy by design and by default

6.4.1 In addition to the need for implementing appropriate organizational and technical measures, the Data Protection Policy adopted the privacy by design and by default approach, shortly described in the Policy as data protection enhancing technologies and tools to enable data processors to better protect personal data (para. 4.2.3 of the DPP). Developed by the Information and Privacy Commissioner of Ontario, subsequently endorsed by

[50] UNHCR, *Administrative Instruction on Access Controls Management for ICT Systems, Applications and Services*, March 2018.

the International Conference of Data Protection and Privacy Commissioners (ICDPPC) and included in the GDPR (Article 25), privacy by design should be understood as a holistic concept applicable to operations throughout an organization, end-to-end, including its information technology business practices, processes, physical design and networked infrastructure[51]. The concept in the Data Protection Policy should therefore be understood in line with established terminology and practice, including the 'Foundational Principles' of privacy by design adopted by the ICDPPC: (1) Proactive not Reactive; Preventative not Remedial, (2) Privacy as the Default, (3) Privacy Embedded into Design, (4) Full Functionality: Positive-Sum, not Zero-Sum, (5) End-to-End Lifecycle Protection, (6) Visibility and Transparency, (7) Respect for User Privacy[52].

6.5. Data security procedures and practices

6.5.1 Data security is about technology, ICT assets and resources, but even more about their use. Research repeatedly shows that human error is the leading cause of data and security breaches. Weak data security practices by personnel (the human factor) can undermine UNHCR's efforts to protect personal data, for example by increasing the risks of cyberattacks or ´social engineering´. All personnel with access to UNHCR's ICT assets and resources (including basic tools such as computers and emails) are therefore advised to familiarize themselves with existing data security procedures and practices, and to avoid behaviors which may pose risks to the personal data of POCs and UNHCR´s operations more broadly. A short summary of these procedures and practices includes:

Secure use of ICT assets and resources (including email and internet)

6.5.2 All UNHCR personnel are bound by internal policies on the use of electronic mail, the internet as well as the personal use of computers and other technology resources[53]. The Secretary General's Bulletin on the Use of Information and Communication Technology Resources and Data has also been introduced to UNHCR through these policies[54]. The latter, inter alia, prohibits certain online activities by UN personnel, and makes all users responsible and liable for their personal use of ICT resources (including all activities and content created, transmitted or displayed via internet services). All UNHCR personnel are

[51] See ICDPPC, *Resolution on Privacy by Design*, 32nd International Conference in Jerusalem, Israel 27-29 October 2010, available at: https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf.

[52] See above. For further information on the Foundational Principles, see: Information and Privacy Commissioner of Ontario, *Privacy by Design*, revised September 2013, available at: https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf.

[53] UNHCR, *Electronic Mail Policy* (2006, revised in 2012); *Personal Use of UNHCR Computers and Other Technology Resources*, June 2005 and *Internet Appropriate Use Policy*, December 2009.

[54] United Nations, *Secretary General's Bulletin on Use of Information and Communication Technology Resources and Data*, 20 November 2004, ST/SGB/2004/15, available at: https://oios.un.org/resources/2015/01/ST-SGB-2004-15.pdf.

called upon to complete the mandatory Information Security Awareness Foundation and Advanced Courses available for UNHCR staff and partners at UNHCR's learn and connect platform.

6.5.3 In terms of recommended practices, all UNHCR personnel are encouraged to:

(i) **Maintain a healthy distrust and defensive posture** in respect to unknown persons and communications, for example by not clicking on links or opening attachments in emails that come from unknown addresses or seem suspicious, disclosing sensitive information about themselves or colleagues on insecure websites, or giving passwords to others;

(ii) **Pursue safe internet browsing practices**. UNHCR uses web filtering to provide basic protection to its users. UNHCR personnel should not install video players or browser extensions on their PCs without the advice of an IT Officer, as these may contain malware;

(iii) **Stay up to date**. Computers that do not have up-to-date anti-virus, patches or firewalls are far more likely to be infected by malicious software and applications ('malware'). IT Officers should ensure that all office computers are using up-to-date software and operating systems and licensed anti-virus software, to download and install automatically;

(iv) **Report suspicious activity** to the GSD to allow swift and effective measures. Potential breaches, such as compromised accounts or systems, lost or stolen computers, the unauthorized release of protected information, system downtime, and the detection of malicious software, should also be reported to the data controller.

Secure use of portable ICT equipment (including laptops, smartphones and USB drives)

6.5.4 Laptops, tablets, smartphones, and other portable devices have the advantage of being used outside UNHCR premises but may be lost or stolen, which may lead to loss of personal data and potential unauthorized access. Portable devices may also be more vulnerable to malware, and users are less likely to apply the latest security patches and have less secure operating systems. To limit the risks to persons of concern, all UNHCR personnel are recommended to:

(i) Minimize the amount of personal data of persons of concern stored on their portable devices, including on smartphones and laptops;

(ii) Ensure that all portable devices are password/PIN protected, respect guidance on the use of passwords[55], set to 'auto lock' when not in use and keep in possession or in safe locations at all times;

(iii) Portable or removable devices (such as USB drives and memory cards) should in principle not be used to store or transfer personal data. If their use is unavoidable, the devices should be encrypted (seek advice from the IT Officer), kept physically secure, and the data erased immediately upon completion of the task;

(iv) UNHCR personnel returning a device to UNHCR should ensure that they erase all their emails, messages and any other files which may contain personal data of POCs;

(v) Lost or stolen devices which have been used for personal data should be reported to the data controller and IT Officer, and any passwords changed immediately.

Secure use of ICT assets during mission travel and remote working arrangements

6.5.5 Remote working arrangements and mission travel carries additional risks, as networks and resources may not be as secure. All UNHCR personnel should be aware of the following:

(i) **Public Wi-Fi networks and open access points** (i.e. which do not require a password) pose the greatest risk, because users may be exposed to 'sniffing' (the capture of data sent across insecure networks) and 'man in the middle attacks' (using fake or malicious Wi-Fi 'hotspots'), and at greater risk from viruses, spyware, malware, and 'phishing' attempts. Personnel are therefore advised to avoid such networks. If used exceptionally, file sharing should be disabled, the wireless network settings changed to 'public' and personnel remain vigilant for suspicious activity. UNHCR personnel considering using Virtual Private Network (VPN) applications should contact the GSD or an IT Officer for advice before installing such applications;

(ii) **Personnel working from home** are encouraged to ensure that their wireless networks are secure. Access to networks should be controlled, WPA2 security protocol applied, and default router administrator passwords replaced. Seek advice from the IT Officer[56];

[55] UNHCR, *Use of Passwords in UNHCR's Computer-Based Systems*, Memorandum of April 2009.

[56] For more information, see for example: https://www.microsoft.com/en-us/safety/online-privacy/home-wireless.aspx, or https://staysafeonline.org/stay-safe-online/keep-a-clean-machine/securing-your-home-network.

(iii) **Border guards in an increasing number of countries** demand that individuals open their laptops, turn on mobile phones and enter or handover passwords to access data on such devices. In such a situation, UNHCR personnel are advised to comply with a request to turn on their electronic devices to allow a non-intrusive visual inspection (for the purposes of verifying that the devices function), but not to allow the opening, reading or downloading of documents. Requests for handing over of pin codes or passwords, or for examining the device without it being in the presence of the staff member should be declined. If necessary, staff members should request to see the guards' supervisor in order to make clear that the device(s) contain UNHCR documents which are confidential and inviolable as part of UNHCR's archives.

6.6. Secure communications and data transfers

6.6.1 There is a high risk of data breaches when personal data is communicated or transferred, for instance from UNHCR to a third party. E-mails and SMS messages may be intercepted during transmission and/or retained by surveillance programmes, thus putting persons of concern at risk of harm, in particular if accessed by countries of origin. On this issue, the Data Protection Policy states that "in order to ensure and respect confidentiality, personal data must be (…) transferred only through the use of protected means of communication (para. 4.1.2 and 6.1.2 (v)).

6.6.2 In order to reduce the risk of personal data breaches during communication and transfer of personal data, UNHCR personnel are recommended to:

(i) In principle, use only **UNHCR-developed and approved tools** to transfer personal data;
(ii) Exercise **caution** regarding the use of third party file-sharing tools;
(iii) It is impossible to guarantee the confidentiality of any electronic message transmitted outside the UNHCR system via the internet. **No information of a confidential nature should be sent by e-mail via the internet**[57]. More secure alternatives include the use of e-SAFE, UNHCR secure file transfer protocol (FTP) service, and encrypted portable media devices;
(iv) Personal data should **not be transferred using personal email accounts** (e.g. Gmail, Yahoo or Hotmail), or through social media accounts (e.g. Facebook, Twitter)[58];

[57] UNHCR, *Electronic Mail Policy*, June 2006, para. 5.5.3.

[58] UNHCR, *Administrative Instruction on the Use of Social Media*, September 2014, para. 5.1.6.

(v) If e-mail is used, ensure that **additional measures are taken to protect the content,** such as encrypting the email or its attachment. When sharing password protected files, the password should be sent via an alternative means of communication (such as phone call or text message);

(vi) **SMS should be avoided as a means to communicate personal data**, internally within UNHCR, externally and with persons of concern. Text messaging services that are encrypted end-to-end are more secure than SMS messages and should be used instead;

(vii) **Seek advice** from the IT Officer, GSD or the DIST ICT Security Section on which tools to use for different purposes and in different operational scenarios.

Communication with communities through "bulk SMS" and messaging applications

6.6.3 Bulk SMS and messaging applications present opportunities for enhanced communication with displaced communities, in particular in areas which are difficult for UNHCR to access[59]. UNHCR personnel should, however, be aware of the potential lack of security related to these tools, which may reveal the identity and location of individuals or communities to third parties, as well as collect personal data and metadata, and facilitate access for law enforcement agencies and other state authorities. These risks are further exacerbated in the case of web-based platforms, inadequate encryption, or service providers which are based in different countries than the senders and/or recipients[60].

6.6.4 To minimize protection risks, UNHCR recommends the use of such tools only for purposes such as emergency or security broadcasts, administration of assistance distribution, and monitoring. They should, as far as possible, be avoided for protection sensitive information. Furthermore, Chief Information Security Officer (CISO) and, where relevant, the DPO should be consulted on the choice of application and service provider. A DPIA would normally also be required for such initiatives.

The use of electronic survey tools

6.6.5 The use of survey tools and mobile devices to collect data from persons of concern allows for more efficient assessments than paper-based systems. In light of the potential data protection challenges, personnel are strongly advised to consult with FICCS and the IT Officer (or the CISO) to select survey tools and modalities which ensure that personal

[59] UNHCR, *Connecting Refugees: How Internet and Mobile Connectivity can Improve Refugee Well-Being and Transform Humanitarian Action*, 2016, available at: http://www.unhcr.org/connectivity-for-refugees.html.

[60] See also ICRC, *Handbook on Data Protection in Humanitarian Action*, Chapter 11 and ICRC, *Humanitarian Futures for Messaging Apps: Understanding the opportunities and risks for humanitarian action*, January 2017, available at: https://www.icrc.org/en/publication/humanitarian-futures-messaging-apps.

data is only collected, processed and retained in accordance with the requirements of the Policy.

6.7. High risk environments and deteriorating security situations

6.7.1 The Data Protection Policy acknowledges that personal data processing by UNHCR may take place in deteriorating security situations or high-risk environments (para. 4.2.6). The data controller should therefore make provisions for the handling of personal data in the eventuality of a potential evacuation or relocation. This could be done at various levels, including the contingency, security or response plan as well as internal SOPs. It is recommended to make clear ***assignments of responsibility for the decision and implementation*** of removal or destruction of all assets and records containing personal data of POCs in physical and electronic files. It is also recommended to include the topic in security trainings and the standard induction checklist for the new-arriving staff.

6.7.2 In the event of a **relocation or evacuation**, the data controller, with the support of the IT Officer and Field Safety Advisor, is responsible for overseeing, that all computer(s), servers, back-up systems and paper files are moved to a **secure location**, if feasible. Where this cannot be achieved, the data controller, may also decide, as a **matter of last resort, to destroy** assets and records to prevent that personal data falls in the hands of people who may cause harm to UNHCR POCs.

6.7.3 In order to prevent the occurrence of the above and generally to reduce the risk of data breaches resulting from an evacuation, or a potential security incident, data controllers are advised to consider the digitization of hardcopy documents containing personal data in consultation with RAS[61]. Other data security measures, including the use of encryption, can also reduce the risk of unauthorized exposure resulting from an evacuation, relocation, or security incident. Seek support from the IT Officer, or CISO in Headquarters, when needed.

[61] See UNHCR, *Operational Guidelines for digitization (for conversion of analogue records into digital format)*, 2015, June 2015.

7. Personal Data Breaches and their Notification

7.1. Concept of personal data breaches

7.1.1 The Data Protection Policy defines a personal data breach as "a breach of data security leading to the accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transferred, stored or otherwise processed" (para. 1.4)[62]. Personal data breaches may therefore be the result of internal wrongdoing or external intrusion. Often, they will entail also a breach of confidentiality, i.e. unauthorized persons gaining access to personal data of POCs. The severity and impact of a personal data breach can vary. Also, if communicated to the public or other stakeholders, personal data breaches have the potential to undermine the reputation and confidence in the integrity of UNHCR´s operations. Hence the **importance of dealing with personal data breaches in an orderly way, including the notification** of such breaches, as foreseen in the Data Protection Policy and complemented by this Guidance.

7.1.2 As seen from the definition, the concept of personal data breach covers a range of situations. **Unauthorized access to personal data** may be the result of negligence, such as compromised login credentials, caused by attacks on ICT assets designed to deliberately undermine or obstruct UNHCR's activities or extort financial reward, or a consequence of surveillance, or interception of communications or transfers. There are also 'insider threats' linked to fraud and corruption, and theft and confiscation of portable ICT devices. Furthermore, **loss of, or damage to, personal data** may be the result of laptops, servers or portable devices being lost or stolen, infected with 'malware' or damaged due to natural or man-made hazards. Negligence may also lead to a data breach, for example inadequate backups or when documents including personal data are printed and left unattended.

7.2. Categorization of personal data breaches

7.2.1 For the purpose of follow up measures and reporting, personal data breaches may be categorized as minor, significant or serious based on the following criteria: (i) the number of persons of concern to UNHCR and other persons affected; (ii) the risk of serious harm to the affected individual(s); (iii) the indication of any systemic or large-scale problem in UNHCR's physical or ICT security systems; and (iv) the potential for media or other stakeholder attention as a result of the breach.

[62] This definition corresponds with Article 4 para. 12 of the GDPR.

7.2.2 **Minor data breaches** pose minimal risk to POCs and the integrity of UNHCR's operations, e.g. negligence by personnel, lost mobile devices which may be handled adequately by the operation, having regard to staff performance and disciplinary procedures, where relevant.

7.2.3 **Significant data breaches** pose a significant risk to the security, safety or fundamental rights of individual persons of concern or affected communities, or to the integrity of UNHCR's operations, for instance data security failures leading to personal data being accessed by persons outside of the organization, minor breaches of ICT security management systems or stolen computers or mobile devices containing personal data.

7.2.4 **Serious data breaches** affect significant numbers of persons of concern or pose a substantial risk to the security, safety or fundamental rights of persons of concern, their families and associates, and/or affected communities, or to the overall integrity of UNHCR's operations, for example the ransacking or evacuation of UNHCR's offices, major breaches of ICT security management systems or the posting of personal data of POCs on the internet.

7.3. Responding to personal data breaches

7.3.1 With regard to the response to personal data breaches, the Data Protection Policy mentions recording and notification by any UNHCR personnel to the data controller, from the data controller to the DPO and communication to the data subject (para. 4.4.1). The Policy also refers to mitigating measures and implies an assessment of the known and foreseeable adverse consequences of a personal data breach (para. 4.4.2 and 4.4.3). When responding to personal data breaches, one may therefore distinguish key steps: Assessment, Mitigation, Recording and Notification.

7.3.2 **Assessment**. Upon becoming aware of an actual or potential personal data breach, several factors need to be assessed:

(i) Data records and type of personal data affected;
(ii) Date, time, duration and location;
(iii) Cause of the data breach;
(iv) List of affected data subjects;
(v) Risk of serious harm to data subjects;
(vi) Risk of other adverse consequences (operational, security, financial, reputational).

7.3.3 **Mitigation**. The priority is to take measures to end the breach and prevent further breaches. Depending on the assessment, a number of measures may become necessary:

(i) If personal harm or injury is likely to occur, communicate the personal data breach to the data subject (para. 4.4.2 of the DPP). The risks to the data subject can at best be assessed together with affected individuals, for example if details of an asylum-seeker's identity, location or asylum application have been brought to the attention of the authorities of the country of origin. Counselling should convey the data breach in a factual manner, highlighting any uncertainty related to the events in a clear and transparent way, and attempt to respond to any questions or concerns from the individual(s), with due consideration to their individual circumstances, situation and background;

(ii) Prepare or carry out follow up measures for the protection of data subjects. This could include changing of phone numbers or SIM cards, but also immediate physical protection measures, such as relocation or support from local police, with the consent of the individual(s) concerned and in cooperation with the Field Safety Advisor;

(iii) ICT related measures up to the activation of the ICT Incident Response Plan;

(iv) Establish security monitoring systems.

7.3.4 **Recording and Notification**. Personal data breaches need to be recorded and notified (para. 4.4.1 of the DPP) for accountability reasons, a proper understanding of the causes and consequences and in order to prevent future breaches. Recording and notification should include the elements mentioned in para. 4.4.3 of the DPP in conjunction with the points mentioned above under 'Assessment'. The following actions should be observed:

(i) Every UNHCR personnel has to notify an actual or suspended personal data breach to the data controller. The data controller may also designate the data protection focal point to receive such notifications. It should be understood that such initial notifications may not contain all elements mentioned in para. 4.4.3 of the DPP. Recording may be completed as the assessment continues;

(ii) According to the Data Protection Policy, the data controller should notify the DPO if a personal data breach is likely to result in personal injury or harm to a data subject (para. 4.4.2). In terms of the above-mentioned categories, this means that the DPO should be notified of all significant and serious breaches. The notification to the DPO should take place within 72 hours after a significant breach becomes known and 24 hours after a serious breach is known[63]. In order to facilitate the monitoring function of the DPO, notification of minor breaches is also encouraged, and in any case of doubt as to whether breaches are significant or serious.

[63] See in this respect also Article 33 (1) of the GDPR.

7.3.5 In addition to the above-mentioned key steps, this Guidance recommends data controllers to set up of a **Data Breach Response Team** comprised of personnel with the required seniority, technical expertise and diversity to respond effectively to personal data breaches. A Data Breach Response Team would include the data controller, the data protection focal point, Protection and Registration staff, the Field Security Advisor and IT Officer (or Assistant), and to the extent available in a field operation and relevant for the particular data breach, information or data management, programme and external relations staff. It could be activated in significant and serious breaches.

7.3.6 In the case of serious data breaches, a country level Data Breach Response Team could also be supported by relevant colleagues at HQ level, including the

(i) DPO;
(ii) The ICT Chief Information Security Officer (takes the lead in containing cybersecurity breaches affecting UNHCR's corporate ICT systems and tools and in rectifying systemic problems in UNHCR's ICT security management systems);
(iii) The Field Security Section (FSS), (takes the lead in breaches of physical security structures or access to premises, and can provide support in situations where the breach causes security risks to POC(s) or personnel, as well as support investigations);
(iv) Identity Management and Registration Section (IMRS), (in the case a breach is related to UNHCR's corporate registration tools, such as proGres, BIMS etc.);
(v) Division of International Protection (DIP) and regional protection staff (in the case of data breaches potentially causing protection risks to individual POCs or POC communities);
(vi) The Legal Affairs Service (LAS), (if the breach is caused by a commercial service provider or implementing partner and measures need to be taken to suspend or terminate the relevant contract or partnership, or there is a request for compensation of damages);
(vii) Regional Bureau (for oversight and assessment of operational or reputation risks);
(viii) External relations (if a communications strategy will be required); and
(ix) Inspector General's Office (IGO) (mandatory if there is any suspicion of misconduct of UNHCR personnel, potentially also for *ad hoc* inquiries into serious attacks on UNHCR´s assets).

7.3.7 Dealing robustly with personal data breaches is among the best ways an operation can build a "culture of data protection" and **prevent breaches in the future**. In cases where the assessment of the personal data breach has indicated a weakness in UNHCR's procedures, tools or systems, their review and enhancement may be required, for example update security and response plans and/or SOPs. Similarly, a breach which has indicated an inadequate level of awareness among personnel related to data protection, including data

security practices and procedures, may require the operation to make further efforts in training/ capacity building.

7.4. Personal data breaches with implementing partners and third parties

7.4.1 Any of the potential data breaches listed above could also occur with partners or third parties, to whom UNHCR has transferred personal data. It is therefore essential that all relevant contracts of service, MOUs, PPAs, Data Transfer Agreements, and other written undertakings regarding the processing of POC data include standard provisions on the notification of data breaches to UNHCR, and cooperation in respect to potential mitigation measures[64].

7.4.2 The key steps in responding to personal data breaches listed above may also be relevant to data breaches which occur with UNHCR´s implementing partners or third parties. Where necessary, UNHCR should assist Implementing partners in building or enhancing their capacity to prevent or mitigate the risk of data breaches affecting personal data of POCs (see also para. 5.4 of the DPP). IPMS and LAS should be consulted on mitigating measures in the case of a data breach with a partner or commercial service provider.

8. Data Protection Impact Assessments

8.1. A tool and a process

8.1.1 In para. 4.5, the Data Protection Policy introduces the concept of Data Protection Impact Assessments (DPIAs). According to the definition in para. 1.4 of the Policy, a DPIA is "**a tool and a process** for assessing the protection impacts on data subjects in processing their personal data and for identifying remedial actions as necessary in order to avoid or minimize such impacts". DPIAs, also known as Privacy Impact Assessments (PIAs), are today a common feature in numerous data protection and privacy laws[65] and

[64] UNHCR, *Standard Format Bipartite Project Partnership Agreement (UNHCR with non-governmental and other not-for-profit partners)*, para. 13.22.

[65] See, for all EU Member States, Article 35 of the GDPR; see also Section 208 (b) of the US E-Government Act of 2002, available at: https://www.gpo.gov/fdsys/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf.

national data protection authorities and other bodies have developed ample guidance material on DPIAs/PIAs[66]. In light of existing practice, **a DPIA may serve several purposes**:

(i) Determine and assess potential impacts or risks related to personal data processing;
(ii) Identify and evaluate alternative processes to mitigate such risks;
(iii) Enhance informed decision making for data controllers (managers);
(iv) Implement the privacy by design and by default approach;
(v) Demonstrating compliance with data protection principles and that data protection is taken seriously;
(vi) Contribute to trust and confidence in the organization.

8.1.2 These purposes of a DPIA are equally valid for UNHCR. DPIAs as a tool for accountability and a process for building and demonstrating compliance are particularly import in an international organization that, due to its institutional set up and the limited recourse and sanctions mechanisms, needs to focus on preventative action to ensure compliance. Moreover, the particularly vulnerable position of POCs to UNHCR and the generally sensitive nature of their personal data (see para. 1.2.1 of the DPP) speak in favor of the **importance of DPIAs in UNHCR's data processing context**[67]. There is finally a strong link between DPIAs and the privacy by design and by default approach (para. 4.2.3 of the DPP) in that a DPIA may provide an early warning system, a way to detect data protection problems and build safeguards before not after important investments are made, e.g. in expensive technology systems.

8.2. When to conduct a Data Protection Impact Assessment

8.2.1 With regard to the **timing**, the Policy suggests that a DPIA is carried our "when elaborating new systems (…) or before entering into (…) agreements" (para. 4.5.1). Only when undertaken **during the planning and design stages of new data processing initiatives**, i.e. before a system is purchased and rolled out or an agreement signed, can the DPIA fulfil its purpose not only of assessing but also of preventing risks. However, a DPIA

[66] See also Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, WP 248 of 4 April 2017, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, page 4; Commission nationale de l'informatique et des libertés (CNIL), *PIA software, tool and guides,* 2018, available at: https://www.cnil.fr/en/tag/Privacy+Impact+Assessment+(PIA); Australian Information Commissioner, *Guide to undertaking privacy impact assessments*, available at: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments; Government of Canada, *Directive on Privacy Impact Assessment*, available at: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308; and International Organization for Standardization (ISO), *Guidelines for privacy impact assessment*, ISO/IEC 29134:2017, at: https://www.iso.org/standard/62289.html (for purchase).

[67] See with regard to vulnerable data subjects also Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, page 9.

may still be undertaken to assess and mitigate the data protection risks arising from projects that are already operational.

8.2.2 With regard to the **material scope**, it follows from the logic of the importance of DPIAs in UNHCR's data processing environment that is **broadly interpreted and applied**. At the same time, not every act of data processing or partnership will require a DPIA. Para. 4.5.1 of the DPP refers to "new systems, projects or policies or (…) data transfer agreements with Implementing Partners or third parties" as well as to the "collection and processing or transfer of personal data (that) is likely to be large, repeated or structural". In addition, a DPIA is only required **when the processing may negatively impact on the protection of data subjects**. Based on the Policy, this Guidance provides the following advice for the determination whether a DPIA is necessary (threshold analysis):

8.2.3 **New technologies** or systems, tools, modules, or data processing platforms, including inter-operable or shared databases, which are perceived or expected to carry inherent privacy risks should, as a matter of principle, undergo a DPIA. This includes for example the collection of biometric data, cloud storage, big data analytics, artificial intelligence, drones, automated decision-making systems, two-way communications using social media, smartphones or bulk SMS.

8.2.4 A DPIA is strongly recommended in case of **transfers of personal data sets to a partner or third party**, whether NGO, agency or commercial service provider, with presumed data protection weaknesses and/or where the assessment of the level of data protection (required based on para. 6.1.4 of the DPP) is difficult, e.g. due to the absence of internal data protection statutes and policies or the lack of track record and experience in cooperation, taking also into consideration the applicable laws, local culture and the specific operational and security context.

8.2.5 A DPIA may also be recommended in the case of processing of **particularly sensitive personal data** in particular where UNHCR receives or transfers such data from or to partners or third parties. This may include health records, SGBV or protection incidents, sexual orientation, and/or acute protection needs, data on a particularly vulnerable group, e.g. an ethnic or religious minority.

8.2.6 In the case of a combination of the above, for instance the processing of particularly sensitive personal data involving transfers to a third party with a presumed weak data protection record and/or in a risky environment using new technology, a DPIA would necessarily be required.

8.3. How to conduct a Data Protection Impact Assessment

8.3.1 While stressing the nature of a DPIA as a **process**, the Policy elaborates less on this aspect. Based on industry standards, the guidance for the DPIA process consists of several steps[68]:

(i) Threshold analysis, i.e. whether a DPIA is necessary;
(ii) Preparation of the DPIA, including setting up a team, plan, allocate resources, identify and consult stakeholders;
(iii) Performing the DPIA, including identification of personal data flows, determination of data protection safeguard requirements, risk identification, analysis and evaluation and setting out options or alternatives;
(iv) Follow up, including preparation of the report and a public summary, implement risk treatment plans and review or update the DPIA.

8.3.2 A key result of a DPIA is the production of a **report**. The DPP includes a fairly detailed outline when it states that "a DPIA would contain a general description of the envisaged system, project, policy or data sharing arrangement involving processing of personal data, an analysis of the risks to the rights of data subjects by virtue of the circumstances and the nature of the personal data processed, the safeguards, security and other measures in place or proposed to ensure the compliance with this Policy" (para. 4.5.2).

8.3.3 A DPIA may be conducted internally by UNHCR or externally. The DPIA report should consist of 6 parts:

(i) Information on the person responsible for the DPIA
(ii) Description of the initiative
(iii) Mapping of stakeholders
(iv) Mapping data flows and operational environment
(v) Identifying and assessing the risks
(vi) Recommendations and review

8.3.4 An external DPIA is recommended for challenging data processing initiatives involving particularly sensitive data, complex technologies and/or multiple stakeholders. It may also be recommended following an internal DPIA which has identified significant data protection risks. An external DPIA would normally be designed with the support of the Regional Office and/or Headquarters. It may be also appropriate to conduct an external assessment, using qualified data protection experts, having regard to the operational context and available resources. The terms of reference should be devised in close consultation with the DPO.

[68] See ISO/IEC 29134:2017, Section 6 (Guidance on the process for conducting a PIA).

8.3.5 A DPIA may concern a single data processing operation at country level or a set of similar processing operations (see para. 4.5.3 of the DPP). A single data processing operation, for example the question of signing and data transfer agreement with a specific third party in a specific country operation would normally done internally. There are however several situations in UNHCR's context where it may be reasonable, economical and in accordance with the privacy by design approach to conduct DPIAs at global level that cover a set of similar processing operations. This would apply to UNHCR's use of a number of technology products combined in the Population Registration and Identity Management Eco System (PRIMES). The core modules (e.g. BIMS) and tools (e.g. GDT or RAIS) are UNHCR developed and approved to be used globally, including with or for partner organizations. It could also apply where UNHCR considers using a technology system developed by a third party. In both cases, an external DPIA may be more appropriate.

8.4. Implementation

8.4.1 Responsible for the decision to conduct a DPIA is the data controller (para. 4.5.3 of the DPP). He or she also has to sign-off the DPIA report and, based on the findings, decide whether to proceed with the data processing initiative, and, if so, how. He or she may task the data protection focal point for the threshold analysis, whether a DPIA is required and/or may consult the DPO for further advice. If and once the decision for a DPIA is made, the DPFP would also normally be designated for the organization of the process and the delivery of the DPIA report. The DPFP may be supported by a multi-functional team, comprised of protection, registration, programme, and community services, IT and Security personnel. After its completion, the DPIA report needs to be validated by the data controller. As stated in the DPP, and in order to verify the quality and adequacy of DPIAs, data controllers are required to keep the DPO fully informed and share a copy of the report. It is also recommended that the findings are shared with stakeholders and service providers, where relevant, in order to assist with the implementation of its recommendations and for general transparency and accountability reasons (see above the purposes of a DPIA).

9. Data sharing and transfers

9.1. Context and Notion of data sharing and transfers

9.1.1 The Data Protection Policy recognizes that **in pursuit of its international protection and solutions mandate, UNHCR is often required** to process personal data of persons of concern, including **to share personal data with implementing partners and/or third parties** (para. 1.2.1). While Implementing partners are defined in concrete terms, the notion of third party includes a natural or legal person other than the data subject, UNHCR or an implementing partner (see definitions in para. 1.4 of the DPP). This reflects the large

variety of actors UNHCR collaborates with, including governments, intergovernmental, non-governmental organizations, UN agencies, community-based organizations, universities, the judiciary and the private sector[69]. Partnerships and cooperation with other actors are embedded in the UNHCR Statute, have been the topic of several initiatives and figure prominently in UNHCR's Strategic Directions 2017-2021[70]. UNHCR currently maintains more than 900 partnerships and entrusts around 40% of its annual expenditure to its partners.

9.1.2 The Data Protection Policy deals with the transfer of personal data to third parties in Chapter 6. Transferring personal data is a form of data processing (see the definition of processing of personal data in para. 1.4) but the Policy does not define transfers. Moreover, the Policy also occasionally uses the term sharing (para. 1.2.1, 4.5.1, 6.2.1 and 7.3.1). A contextual view of the use of both terms allows the conclusion that the Policy makes no difference[71]. Considering the use of the term transfers in other instruments, notably the GDPR[72], transfers of personal data would normally imply the elements of **communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of the sender that the recipient(s) will have access** to it[73].

9.2. General requirements for data transfers

9.2.1 While the Data Protection Policy recognizes the need to share personal data with implementing partners and third parties (para. 1.2.1), it also acknowledges the potential data protection risks involved in transfers to third parties (para. 6.1.2). On the one hand, the protection mandate of UNHCR requires it to minimize the risks of personal data breaches due to transfers, on the other hand, UNHCR needs to be pragmatic and take into account, for instance, different levels of data protection capacity among third parties as well as different national jurisdictions to which they may be subject. The approach with regard to personal data therefore needs to be principled with a level of flexibility. This is the rationale for the Data Protection Policy to require that **third parties afford a level of data protection the same or comparable to the UNHCR Policy** (para. 6.1.1).

[69] See only http://www.unhcr.org/partnerships.html.

[70] UNHCR, *Strategic Directions 2017-2021*, 16 January 2017, available at: http://www.unhcr.org/5894558d4.pdf, page 13/14.

[71] For instance, para. 6.2.1 of the DPP uses both terms. The ICRC Handbook also uses both terms without distinction, see Chapter 2, para. 2.12 at page 49.

[72] See Chapter V of the GDPR on the Transfer of personal data to third countries or international organisations and the Madrid Resolution of the ICDPPC using the term international transfers.

[73] See European Data Protection Supervisor (EDPS*), The transfer of personal data to third countries and international organisations by EU institutions and bodies*, Position paper of 14 July 2014, available at: https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf, at page 7; The ICRC Handbook adopts a very similar definition of the term (international) data sharing, see Chapter 2, para. 2.12 at page 49 and in Chapter 4 (International Data Sharing).

9.2.2 With regard to the meaning of "the same or comparable standards", the Data Protection Policy does not contain a fixed definition. However, considering the object and purpose of the Policy, every third party should in principle respect the **basic principles of personal data processing as set out in para. 2.1 of the DPP**, i.e. legitimate and fair processing, purpose specification, necessity and proportionality, accuracy, respect for the rights of data subjects, confidentiality, security and accountability and supervision. In para. 6.1.2 point (v) and (vi), the DPP emphasizes **confidentiality** ("written agreement") **and data security** ("high level of data security").

9.2.3 The **level of data protection afforded by a third party needs to be assessed before agreeing to transfer personal data**. This is what para. 6.1.4 in conjunction with para. 7.2.2 of the DPP requires the data controller to do. The same provision also provides guidance for such assessments by referring to "applicable laws and regulations, internal statutes and policies of the third party, specific contractual obligations or undertakings to respect specific data protection frameworks, their effective implementation as well as technical and organizational means of data security in place." **The best way to carry out this assessment is through a DPIA** (see para. 6.1.4 with reference to para. 4.5 of the DPP). Reference is made to para. 11.2 of this Guidance.

9.2.4 In addition to the level of data protection afforded by the third party, the **act of transferring personal data itself needs to meet the conditions set out by the Data Protection Policy**. According to para. 6.1.2 (i) to (iv) of the DPP, data transfers need to be based on a legitimate basis, for one or more specific and legitimate purpose(s), be limited to personal data that is adequate, relevant, necessary and not excessive in relation to such purpose(s) and the data subject needs to be informed. When recording specific instances of data sharing with third parties (see para. 7.3.1 (ii) of the DPP), UNHCR personnel is advised to refer to these conditions. In addition, para. 6.1.2 (v) and 4.1.2 of the DPP require personal data only to be transferred through the use of protected means of communication.

9.2.5 Finally, based on para. 6.1.3, "UNHCR needs to ensure that transferring personal data does not negatively impact (i) the **safety and security of UNHCR personnel and/or personnel of Implementing Partners**; and/or (ii) the effective functioning of an UNHCR operation or compromise UNHCR's mandate, for example due to the **loss of the climate of trust and confidence between UNHCR and persons of concern** or the loss of the perception of UNHCR as an independent, humanitarian and non-political Organization." These considerations are of a general nature and not strictly linked to data protection principles. This also applies to the **privileges and immunities of UNHCR**. According to para. 6.5, transfers of personal data are without prejudice to UNHCR's privileges and immunities and should not be construed as doing so.

9.3. Practical advice on transfers to third parties

9.3.1 When raising the need to comply at least with a comparable data protection level to UNHCR's Policy, UNHCR may face a lack of understanding, appreciation and/or capacity among third parties. The advice in such situations is to approach the issue positively by explaining the rationale of data protection and offer measures to enhance data protection capacities, for instance by:

(i) Providing all partners and third parties with information about the rationale for the requirements in the Policy, why the protection of personal data is in the common interest of both UNHCR and its partners, and what this means in practice;
(ii) Including data protection as part of the selection procedure for partners, and as part of the mid-term review, so that any concerns can be addressed in a timely manner;
(iii) Seeking written confirmation that the appropriate safeguards are in place already in the early stages of negotiating a Data Transfer Agreement;
(iv) Include data protection capacity-building and/or training on the agenda of thematic working groups of humanitarian organisations engaged in extensive data sharing (e.g. protection or cash working groups).

9.3.2 With regard to the issue of assessing third parties, in particular verifying information security standards of commercial service providers, UNHCR personnel are advised to:

(i) Use reputable and known service providers only;
(ii) Request information on the use of and, ideally, certification in industry standards on security processes and procedures, cloud standards, bulk SMS, encryption/cryptology and financial services standards[74];
(iii) Ensure that data protection and information security is clearly stated in the Requests for Proposals and in the assessments of potential service providers;
(iv) Seek the support of the IT Officer and, if needed, the CISO in Headquarters, in the selection of service providers;
(v) Always ask commercial service providers about the location of their data centres and any cross-border transfers that will take place as part of their processing of the POC data (including to the country of origin of refugees);
(vi) Enquire about the national legislation in the countries in which the company stores and processes data, and to what extent they receive and comply with requests for data from national law enforcement or other authorities.

[74] Namely ISO/IEC 27000 family - Information security management systems, available at: https://www.iso.org/isoiec-27001-information-security.html.

9.3.3 A certain level of risks due to the lack of capacity or national legislation may be compensated through contractual arrangements with the third party, implementation of strict data minimization procedures and limitation of access rights based on the recommendations of a DPIA and in consultation with the DPO and LAS. However, if the level of data protection standards offered by a third party cannot be satisfactorily verified or mitigated through capacity building and/or other efforts, UNHCR should not agree to transfer personal data.

9.4. Data Transfer Agreements

9.4.1 Where transfers of personal data are likely to be large, repeated or structural, i.e. where the same type(s) of data is shared with the same third party for the same purpose over a certain period of time, the data controller should seek to sign a data transfer agreement (para. 6.2.1 of the DPP). Thus, unless transfers are sporadic and unpredictable, **data transfer agreements are the rule**. In referring to "unless there are satisfactory reasons not to do so", the Policy acknowledges that signing an agreement may either not be possible, or, in very exceptional situations, not be appropriate. Examples include the early stages of an emergency and the reluctance among a third party with which data sharing is however necessary for broader protection purposes.

9.4.2 In para. 6.2.2, the DPP mentions a number of points that a data transfer agreement should include. This list is however by no means exhaustive. LAS and the DPO have developed **sample data transfer agreements** that include provisions on the following topics: object and purpose, personal data to be transferred, transfer of additional data elements, means of data transfers, specific purposes of transfer, transferring to third parties, data security, breach notification, dispute settlement, privileges and immunities. LAS and the DPO in Headquarters can be contacted for copies of such agreements and further guidance. The DPO and LAS are also to review and clear all data transfer agreements prior to finalization (para. 6.2.3 of the DPP). Data controllers are recommended to maintain an up-to-date inventory of all data transfer agreements in their operation and lodge final copies with the DPO.

9.5. Access to UNHCR's databases and shared databases

9.5.1 Where third parties or Implementing Partners require ongoing access to personal data of POCs, it may be efficient to provide them with **access to a UNHCR database** or to establish a shared or inter-operable database, instead of regularly transferring large amounts of data. While UNHCR is in principle open to such arrangements, it should be done within the conditions and requirements for data transfers as outlined above and as set out in the Policy. For instance, such access should always be regulated by a formal agreement, whether a stand-alone Data Transfer Agreement or a PPA addendum, setting out, at a minimum, the terms and purpose of use, the personnel authorised to access the

data, the data sets to be accessed and any mechanisms for supervision and accountability. Access should be limited to the datasets that are necessary and proportionate for the partner to fulfil the specified purpose only.

9.5.2 In the case of shared or inter-operable databases, a DPIA is recommended to identify and mitigate risks to POCs and verify that the database is protected in accordance with the Policy. It is recommended that any further guidance which is needed be sought from the DPO, IMRS and DIST in Headquarters.

9.6. Personal data received from third parties

9.6.1 UNHCR may receive personal data from partners or third parties, in accordance with its mandate. In such situations, UNHCR should seek to receive such data through secure data transfers, whenever possible, only retain such data if it has a legitimate basis for doing so and clearly record the source of such data, if retained. Personal data which does not meet these standards should be safely disposed of.

10. Personal data processing by Implementing Partners

10.1. Implementing Partners as data processors

10.1.1 Considering the importance of UNHCR's cooperation with implementing partners (standard definition in para. 1.4 of the DPP), including the processing of personal data of POCs by implementing partners, the Data protection Policy deals with this situation in a separate chapter. In para. 5.1, the Policy clarifies that "where the collection and processing of personal data is one of the responsibilities of Implementing Partners, the personal data is being collected and processed **on behalf of UNHCR**." In other words, and in line with the definition in para. 1.4, implementing partners are data processors.

10.1.2 This means that a number of **responsibilities incumbent on the data controller**, for instance determining the applicable legitimate basis for and the specific and legitimate purposes of data processing, remain the task of UNHCR. It also means that implementing partners are expected to respect the **same or comparable standards and basic principles of personal data protection** as contained in UNHCR's Policy (para. 5.1 of the DPP). For these reasons and based on para. 5.3 of the DPP, the Standard Project Partnership Agreement (PPA) contains a number of clauses specifically related to the protection of

personal data[75]. These agreements should also state the legitimate basis and the specific purpose(s) for data processing and arrangements for partnership termination. Where implementing partners are provided with access to a UNHCR database, an addendum to the PPA is recommended to regulate the partner´s access rights and user conditions.

10.2. Verifying and Assisting Partners

10.2.1 The close relationship between UNHCR and its implementing partners also entails the responsibility upon UNHCR to verify that the processing of personal data by the implementing partner satisfies UNHCR's data protection standards and principles (para. 5.2 of the DPP) and to ensure that implementing partners have the necessary capacity in order to comply with and may need to provide relevant assistance (see para. 5.4 of the DPP). Concerns about, or deficiencies in, the data protection capacity of implementing partners may be addressed through technical assistance and/or training provided by, or supported by, UNHCR. Such measures could include:

(i) Advising on measures to improve the physical security of its offices;
(ii) Advising on potential measures to enhance its IT/data security, physical file management and data transfer practices;
(iii) Organizing training on data protection and its importance for persons of concern;
(iv) Support in establishing, or adjusting, procedures to seek consent from POCs;
(v) Assisting the partner in developing procedures to ensure basic rights of POCs;
(vi) Encourage partner staff to access and complete the eLearning on Information Security Awareness Programme on Learn & Connect (HQInfoSec@unhcr.org);
(vii) Support the development of SOPs to address specific data protection concerns, such as the use of portable electronic devices or survey tools.

[75] UNHCR, *Standard Format Bipartite Project Partnership Agreement (UNHCR with non-governmental and other not-for-profit partners)*, para. 13.17 to 13.25.

11. Accountability and supervision

11.1. Accountability principle and structure

11.1.1 Numerous data protection instruments recognize **accountability as a principle**[76]. In its 1990 Guidelines, the General Assembly requested countries to designate the authority to be responsible for supervising observance of the principles[77]. The rationale for an accountability principle rests on the assumption that unless data protection becomes part of the shared values and practices of an organization, and responsibilities for it are clearly assigned, compliance with data protection principles will be at continued risk[78]. In other words, accountability is seen as a **driver for effective implementation of data protection principles**. In para. 2.9, the UNHCR Data Protection Policy follows this trend.

11.1.2 According to para. 7.1 of the DPP, UNHCR's accountability and supervision structure consists of three key actors, **data controllers in each country office/operation, data protection focal points and a Data Protection Officer (DPO)** at Headquarters. In the following, this Guidance elaborates the concept and notion of the data controller in UNHCR's context, the role of the data protection focal points and of the DPO.

11.2. Data controller and Data protection focal points

11.2.1 The concept of the data controller is intrinsically linked with the accountability principle. In line with key data protection instruments, UNHCR introduced the notion of data controller and allocated to him or her the **main responsibility for compliance with the Policy** (para. 7.2.1 of the DPP). Based on the **authority of a Country Representative**, inter alia, to define the country strategies and priorities, approve the country protection strategy and enforce local compliance with UNHCR's global protection standards, including registration, RSD and resettlement standard operating procedures, in accordance with operational needs and context,[79] the Policy defines the data controller as "the UNHCR staff member, usually the Representative in a UNHCR country office, who has the authority to

[76] OECD, *Guidelines governing the protection of privacy and transborder flows of personal data*, September 1980, revised in July 2013, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; ICDPPC, *The Madrid Resolution*, Principle 11; Article 5 (2) of the GDPR.

[77] United Nations General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, adopted by Resolution 45/95 of 14 December 1990, available at: http://www.refworld.org/pdfid/3ddcafaac.pdf, para. 8.

[78] See Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173 of 13 July 2010, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf, page 2.

[79] UNHCR Manual Chapter 2, *Organizational Structure and Accountabilities, Responsibilities & Authorities*, UNHCR Field presence, Overall ARAs – country offices.

oversee the management of, and determine the purposes for, the processing of personal data (para. 1.4 of the DPP).

11.2.2 The data controller concept therefore follows the **factual control over the processing of personal data based on established organizational structure and accountabilities, responsibilities and authorities** in UNHCR. By inserting the term 'usually', the Policy takes into account the factual and not formal nature of the data controller, which can also be at Regional or Headquarters level as well as delegated, for specific responsibilities, e.g. to a Deputy or Assistant Representative. The Data controller notion in UNHCR's Policy serves internal accountability purposes, it has no bearing on the quality as data controller of UNHCR as an organizational entity from the perspective of third parties. Moreover, although not explicitly mentioned, the Data Protection Policy does not exclude situations of **joint data controllers**, where two or more data controllers jointly determine the purposes and means of personal data processing[80]. For joint data controllers, it is important to clearly determine their respective responsibilities for the compliance with data protection principles. In the case of cooperation with third parties and/or the use of joint data bases, this could be done in agreements or protocols.

11.2.3 Data controllers are assisted by **data protection focal points**. The role of the DPFP is to assist the data controller in carrying out his or her responsibilities regarding the Policy (see para. 1.4); the DPFP should in principle be the most senior protection staff member in a country office/operation (para. 7.2.1 of the DPP). With this pragmatic approach, the Data Protection Policy seeks to place the **DPFP function in an area and at a level** (most senior protection staff) **where many other functions relevant to data protection**, for instance the supervision of registration, RSD and/or Resettlement units, **are already allocated**. Data controllers should designate a DPFP (para. 7.1 (iii) and 7.2.1); they may also ask Heads of Sub Offices or Field Offices to designate DPFP at Sub or Field Office level, assume themselves this function and/or ask DPFPs to set up a data protection team with a composition similar or the same as the data breach response team (see above at para. 10.3.5).

11.2.4 Upon request of the data controller, and based on Chapter 7 of the DPP, the DPFP may assume the following **tasks**:

(i) Determine the legitimate basis for processing, in particular when consent by the data subject is required and ensure that proper consent procedures are in place (7.2.2 (i));
(ii) Ensure that procedures for the rights of data subjects are in place, deal with and respond to requests by data subjects (7.2.2 (iii) and above para. 8.6.7);

[80] See for example Article 26 of the GDPR.

(iii) Coordinate the implementation of organizational and security measures (7.2.2 (ii));

(iv) Carry out or coordinate DPIAs and assessments of data security of third parties (7.2.2 (iii));

(v) Act as first point of contact for the DPO with regard to requests for advice, reporting and seeking clearance of data transfer agreements.

(vi) Maintain an up-to-date inventory of information on relevant personal data processing activities (para. 7.3.1 (ii)) including all databases, information systems, partnerships and contractual arrangements. This inventory should include (as relevant to each operation):

a. Procedures for creating and testing backups, and the personnel responsible for this;
b. The physical location of all field servers and backups;
c. An overview of access rights procedures for both physical and electronic files;
d. Data transfer agreements with partners and other third parties (in force and expired);
e. DPIAs conducted by the operation;
f. An overview of personnel responsibilities in respect to each ICT system (i.e. personnel responsible for maintenance, administration, support and data security);
g. Logs of requests from data subjects for access, correction and deletion and objection;
h. Logs of personal data breaches and responses by the operation.

11.3. The Data Protection Officer (DPO)

11.3.1 Para. 7.1 of the DPP mentions the Data Protection Officer (DPO) within the Division of International Protection as one of the key actors of UNHCR's accountability and supervision structure. The tasks of the DPO are listed in para. 7.3.1 of the DPP and can be characterized as advising, supporting, training, monitoring and reporting. The Policy follows the growing practice at national and regional level of requiring DPOs in public authorities, in particular in each institution and body of the European Communities[81].

11.3.2 In addition to the traditional tasks of a DPO, the UNHCR Data Protection Policy also entrusts the DPO with the responsibility, jointly with the Legal Affairs Service (LAS) to

[81] See Section 8 (Articles 24 to 26) of the Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. See also Articles 37 to 39 of the GDPR and Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, WP 243 adopted on 13 December 2016 (as last revised on 5 April 2017), available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

review and clear all data transfer agreements (para. 6.2.3) and to provide advice, in consultation with the Protection and National Security Section in the Division of International Protection (DIP), LAS and the concerned Bureau(x), prior to the transfer of personal data to a national law enforcement agency or court (para. 6.3.3). In addition, the DPO may join, upon invitation of responsible UNHCR staff, bodies or committees set up by other Policies in areas of particular relevance for the processing of personal data of POCs.

12. References

The Universal Declaration of Human Rights, Article 12, available at: http://www.ohchr.org/EN/UDHR/Pages/Introduction.aspx

The International Covenant on Civil and Political Rights, Article 17, available at: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

United Nations, *Guidelines for the regulation of computerized personal data files,* A/RES/45/95 14 December 1990, available at: http://www.un.org/documents/ga/res/45/a45r095.htm

Office of the High Commissioner for Human Rights (OHCHR), *Report of the High Commissioner for Human Rights on the right to privacy in the digital age A/HRC/27/37*, available at: http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

Human Rights Council, *Summary of the Human Rights Council panel discussion on the right to privacy in the digital age*, A/HRC/28/39, available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39

International Conference on Data Protection and Privacy Commissioners (ICDPPC), *International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution)*, available at: https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf

Organization for Economic Co-operation and Development (OECD), *Privacy Guidelines*, available at: https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, CETS No. 108, as it will be amended by its Protocol, 25 June 2018, CETS No. 223 (Modernized Convention 108), available at: https://rm.coe.int/16808ade9d

European Union Agency for Fundamental Rights (FRA) and Council of Europe, *Handbook on European data protection law*, 2018 edition, available at: http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law

International Organization for Migration (IOM)*, Data Protection Manual (2010),* available at: https://publications.iom.int/books/iom-data-protection-manual

World Food Programme (WFP), *Guide to Personal Data Protection and Privacy*, available at: https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

International Committee of the Red Cross (ICRC), *ICRC Rules on Personal Data Protection*, available at: https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection

International Committee of the Red Cross (ICRC) and the Brussels Privacy Hub (VUB), *Handbook on Data Protection in International Humanitarian Action,* available at: https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

United Nations Conference on Trade and Development (UNCTAD), *Data protection regulations and international data flows: Implications for trade and development*, April 2016, available at: http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468

GUIDANCE ON THE PROTECTION OF PERSONAL DATA OF PERSONS OF CONCERN TO UNHCR

2018

Published By
UNHCR
Division of International Protection
P.O. Box 2500
1211 Geneva 2