UNHCR
The UN Refugee Agency

TECHNICAL NOTE

ON SHARING PERSONAL PROTECTION DATA

Guidance for UNHCR Operations and Partners

VERSION FOR FIELD TESTING

June 2020

Acknowledgements

This guidance was developed collaboratively by UNHCR and partners:

- Care International
- DRC
- HIAS
- InterAction
- IMC
- IRC
- Plan International
- Save the Children
- Terre des Hommes

Photo Credit:

© UNHCR/Mohamed Alalem
Libya. UNHCR distributes cash cards to internally displaced families

CONTACT US

Contents

© UNHCR/Roland Schönbauer

Introduction

Persons of Concern (PoC) have a right to make informed choices about their personal data, and an expectation that UNHCR and its partners will manage their data responsibly and effectively to maximize the protection that they are afforded. Responsible data sharing and use is important for effective protection and solutions in line with the expectations of Persons of Concern. However, we must keep in mind that mishandling of data can have serious harmful consequences that exacerbate protection needs. This document aims to lay out clear and agreed upon definitions as well as give practical guidance to protection and data staff in UNHCR and partner organizations on how to ensure responsible sharing and use of data for scenarios involving personal protection data described by this Technical Note. This document was written collaboratively between UNHCR and partner organizations to ensure clarity on key principles and terminology as well as how those terms and principles are applied in practice.

This guidance was developed to guide operations in developing information sharing arrangements with partners as part of relevant Project Partnership Agreements (PPAs), operational coordination, or individual initiatives. In particular, it aims to support colleagues to ensure that information sharing arrangements with respect to personal protection data with partners meets both data protection rules as well as agreed international standards and principles relating to protection work and protection

information management that are consistent with data protection rules in the context of the situations addressed by this Technical Note. It is based on common field scenarios for information sharing between UNHCR and partners within the context of the provision of protection activities.

This Technical Note is designed to aid colleagues in agreeing data sharing procedures and practices for protection activities that require the collection, processing and sharing of sensitive personal protection data in order to provide protection services commonly provided by UNHCR partners. Common activities include protection (including child protection and GBV) case management, protection information and counselling, vulnerability or specific needs assessment, human rights reporting, protection monitoring, and psychosocial support. The provisions of this Technical Note should not be extended to other protection activities that do not require the collection of sensitive protection data, such as food, NFI or general cash distributions. The Technical Note also does not cover population registration, enrolment or profiling activities.

Terminology

This section recalls key terminology for protection work and data protection that can be applied in relation to sharing personal protection data. It draws on and complements key documents such as UNHCR's Data Protection Policy[1] and the PIM Common Terminology,[2] and related guidance and tools.

Personal Data is "any information relating to an identified or identifiable natural person ('data subject')."[3] Also known as personally identifiable information (PII), personal data includes for example biographical data, 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; and any expression of opinion about an individual, such as an assessment of their legal status and/or specific needs.[4]

Protection data is "data (and information) collected, used, stored or shared by humanitarian and human rights organizations that pertain to protection risks, rights violations and the [protection] situation of specific individuals/groups. Protection data and information may include personal data, or data and information on a specific event, a general situation or a particular context." [5] Examples include: details of protection incidents, specific needs codes or other structured data about protection issues or vulnerabilities, details of assessed protection risks and needs, and information about protection services that have been provided.

Protection data is considered to be **sensitive protection data** or information when "unauthorized access to or disclosure of which is likely to cause harm, such as discrimination, to persons such as the source of the information or other identifiable persons or groups, or adversely affect an organization's capacity to carry out its activities or public perceptions of its character or activities. Certain data and information may be considered sensitive in one context but not in another."[6]

[1] UNHCR, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* (2015) (hereafter, UNHCR Data Protection Policy), pp.9-13, available at: *https://www.refworld.org/pdfid/55643c1d4.pdf*
[2] OCHA/PIM, *Protection Information Management Common Terminology* (hereafter PIM Common Terminology), available at: *http://pim.guide/wp-content/uploads/2018/04/Protection-Information-Management-Terminology_Revised-Edition-April-2018.pdf*
[3] UNHCR Data Protection Policy, p.11
[4] ICRC, *Professional Standards for Protection Work Carried Out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence* (2018) (hereafter, ICRC Professional Standards), p.9.
[5] *Ibid.*
[6] ICRC Professional Standards, p.9

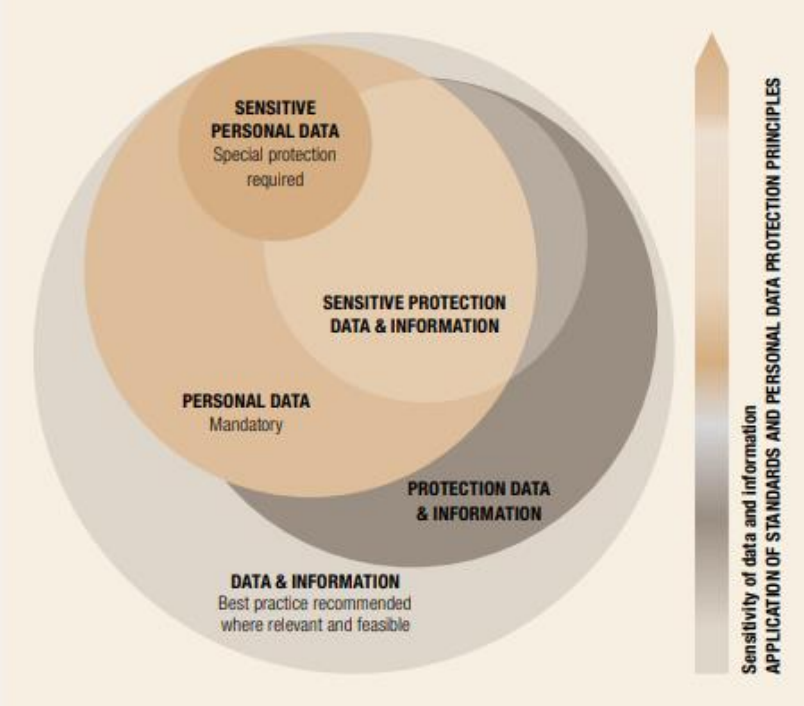


Figure 1: Diagram: Relationships between types of data and information[7]

Personal protection data is defined as data related to protection incidents, vulnerabilities or activities that can be tied to an identified or identifiable individual. For example, the birth date of an individual who is at risk of being forced into recruitment or the vulnerability status of children. Biographical data is not considered to be personal protection data on its own, but when combined with the above described protection data or coming from a protection-specific source, it is included in the concept of personal protection data. For example, the birth date of an individual who is at risk of being forced into recruitment or the vulnerability status of children. Personal protection data is usually collected during case management activities for children at risk, survivors of GBV, and other persons with specific needs or undergoing other protection processes. Activities such as protection monitoring don't usually collect personal data, although they may do where referrals are needed and consented to.

To make a referral is to "...proactively facilitate access to [...] services. Facilitating referral [...] may also involve ensuring that the person can physically reach and obtain access to the necessary services. At a minimum, it requires providing contact information on services of proven reliability"[8]. There must be a legitimate purpose for a referral, consent/assent must normally be obtained from the referral subject (see below), and the personal data provided should be limited to what is needed for the service to be provided. The modalities of referrals will differ from context to context, and should be defined as per operation-specific standard operating procedures (SOPs).

[7] ICRC Professional Standards, p.112
[8] *Ibid.*, p.98-99

"A **data controller** is the person or organization who alone or jointly with others determines the purposes and means of the Processing of Personal Data, whereas a Data Processor is the person or organization who processes Personal Data on behalf of the Data Controller. Finally, a Third Party is any natural or legal person, public authority, agency or any body other than the Data Subject, the Data Controller or the Data Processor."[9] In UNHCR operations, the data controller for internal responsibility purposes is the UNHCR staff member, usually the Representative in a UNHCR country office, who has the authority to oversee the management of, and to determine the purposes for, the processing of personal data.[10] UNHCR partners may be data processors when collecting data expressly on behalf of UNHCR, for example where a partner conducts registration activities. Partners are typically co-controllers for personal protection data, such as in the case of protection case management activities. The "Data Controller" determines how beneficiary data can be used and shared, so where a partner is a data controller or co-controller, decisions must be made together.

A **data processor** means the person or organization who processes Personal Data on behalf of the Data Controller.[11] In cases where a partner is a data processor, it is more likely that the partner is collecting data expressly on behalf of UNHCR. This could be the case, for example, where a partner is contracted specifically to conduct a vulnerability assessment survey in order to provide data for UNHCR to calculate scores for eligibility for cash assistance, for example.

Legitimate basis is a concept that provides the legal and regulatory justification for processing of personal data. Legitimate bases include consent of the data subject, because it is in the vital interest of the data subject, to enable an organization to carry out its mission, or for the safety and security of persons of concern. However, legitimate basis is distinct from the "legitimate purpose."
Refer to the Legitimate Bases section below for more information on the legitimate bases for sharing personal protection data between UNHCR and partners.
.
Legitimate purpose concerns the how "personal data should be collected "for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."

Refer to "Legitimate Purposes" section below for more information on the legitimate purposes for sharing personal protection data between UNHCR and partners.

(Informed) Consent is any freely and voluntarily 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.[12] Consent

[9] ICRC, *Handbook on Data Protection in Humanitarian Action*
[10] UNHCR Data Protection Policy, p. 9
[11] ICRC, *Handbook on Data Protection in Humanitarian Action, p.8*
[12] UNHCR Data Protection Policy, p. 9

needs to be tailored to the unique characteristics of the data subject. This includes considering age, sex, gender, language, disability status and other diversity criteria.[13] For example, for persons with a disability, consent forms should be made in an accessible format and reasonable accommodation should be provided when required.[14] Given the importance of providing information in the context of obtaining consent, UNHCR and partners often use the term 'informed consent'. [15]

In most cases, protection actors must only collect personal protection data "with the informed consent of the person concerned, who is made aware of the purpose of the collection. Unless specific consent to do so has been obtained, personal information must not be disclosed or transferred for purposes other than those for which they were originally collected, and for which the consent was given."[16] It should not be used for other purposes without additional consent and a further assessment of the risks associated with the new purpose(s). The sharing of personal protection data without consent should only occur in exceptional circumstances (see section below on exceptional circumstances).

The process for informed consent is central in protection work as well. It is more than simply providing a form to be signed. Careful attention must be paid to how information is given, considering issues of power and control in the setting. "Especially as those providing information in protection services may feel beholden to service providers or dependent on them as a route to services. Thus, individuals may feel compelled to answer all questions, submit to examinations and/or agree to interview requests regardless of their own discomfort, risk or preference. Humanitarian actors need to make sure they are not overly influencing participants with their authority, attitude, or demeanour, for example, their heartfelt conviction that the information collection is worthwhile, that it will not hurt the participants, and that "professionals" know best. Those collecting information should also be mindful of not making any unrealistic promises, in terms of benefits of participation, as this may unduly influence someone to agree to an interview.[17]

Consent can be fluid. It is given in relation to analysis of the situation at a given moment when changes occur, it is important to re-verify consent with the data subject.

"(**Informed) assent** is the expressed willingness or agreement of the child to participate in services. For younger children who are, by definition, too young to give informed

[13] See the UNHCR Policy on Age, Gender and Diversity (2018), https://www.unhcr.org/5aa13c0c7.pdf.
[14] *Guidance on the provision of reasonable accommodation is available in the IASC Guidelines on Inclusion of persons with disabilities in humanitarian action, in Annex 1 (page 189). Available at: https://interagencystandingcommittee.org/iasc-task-team-inclusion-persons-disabilities-humanitarian-action/documents/iasc-guidelines. The right to provide consent should be never denied on the basis of disability alone. The provision of dedicated measures to ensure supported decision making should always be promoted in cases where an individual with a disability find barriers to provide informed consent, and could take the form of one trusted person, sign language interpretation, or the use of accessible formats. Even in cases when an individual with a disability requires total support to communicate and understand information, the support person or process should enable the individual to exercise their capacity to make a decision according to their wishes.*
[15] See more on informed consent in OCHA/PIM, Framework for Data Sharing in Practice (2018) (hereafter PIM Framework for Data Sharing in Practice), available at: *http://pim.guide/wp-content/uploads/2018/05/Framework-for-Data-Sharing-in-Practice.pdf.*, p.11
[16] F. Bouchet-Saulnier, *The Practical Guide to Humanitarian Law* (2014), p.542
[17] WHO, *Ethical and safety recommendations for researching, documenting and monitoring sexual violence in emergencies* (2007)

consent, but old enough to understand and agree to some decisions, for example participation in services, the child's "informed assent" is sought."[18]

Consent from parents/guardians is normally required for sharing of personal protection data of their children. Consent from parents/guardians is not necessary where it is not in the best interests of the child to share information with the child's parents/guardian or where parents/guardians are not reachable. The information provided and the way in which consent/assent is expressed must be appropriate to the age and capacity of the child and to the particular circumstances in which it is given. For separated children, relatives responsible for their care are normally able to provide consent on their behalf. For unaccompanied children, where care arrangements have been formalised, caregivers are also able to provide consent. Children of sufficient age and maturity may be able to provide consent for decisions that are of lesser weight or consequence – for example, to attend a child friendly space. In all circumstances, assent should be sought from children prior to taking action, and consent sought from parents/caregivers where possible and in the child's best interests. This includes all referrals or service provision.[19]

© UNHCR/Marie-Joëlle Jean-Charles

[18] IRC, *Caring for Child Survivors of Sexual Abuse: Guidelines for health and psychosocial service providers in humanitarian settings* (2012), p.16
[19] UNHCR, *Guidelines on Assessing and Determining the Best Interests of the Child* (2018) (hereafter, UNHCR BIP Guidelines), p.60

Principles

This section provides details and examples of some key principles for personal protection data sharing in practice. It draws on and complements principles outlined in UNHCR's Data Protection Policy and Data Transformation Strategy,[20] as well as the PIM Principles[21], and related guidance and tools.

Confidentiality

Personal data should in principle remain confidential, i.e. not accessible to those who are not authorised to have access. Access should be authorised such that sensitive information is only shared with those who require the information in order to provide protection and assistance to the data subject. In the case of sensitive personal protection data, the highest level of confidentiality is required. Persons authorised to have access to personal protection data should be vetted and designated by their respective organisations in accordance with SOPs based on the need-to-know principle (see below).

In practice, this means that access to personal protection data such as case files should be limited even within organisations, so that only staff who are directly working on cases or overseeing those working on cases should have access.

For example, when conducting programme monitoring activities such as reviewing feedback surveys from recipients of protection services, M&E staff do not usually need to review personally identifying information in order to analyse qualitative and quantitative aspects of feedback. Before providing information for M&E purposes, staff should check that any identifying information (e.g. names, addresses, individual accounts or stories that provide identifying details) are removed.

Need-to-Know

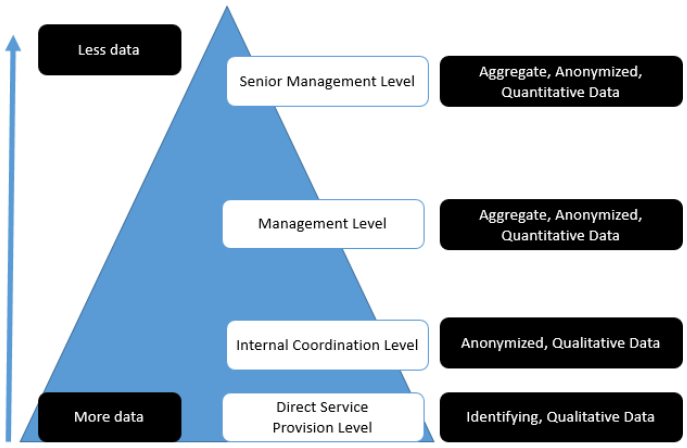
This is a widely accepted principle in protection work that focusses on the application of the principle of confidentiality in terms of sharing personal protection data. This principle essentially describes the sharing of information that is considered sensitive for and limited to a specific, useful purpose. Staff 'need to know' because the information is essential to their purposes. For example, information should/must only be shared with those individuals who need the information to provide the client with specific activities/interventions. Sharing must follow internationally-recognized standards for safe and ethical data management.

In practice, any sensitive or personal data collected on persons of concern should only be shared on a need-to-know basis with as few individuals as is necessary to meet the

[20] UNHCR, *Data Transformation Strategy : 2020-2025* (2019), pp.6-7, available at: *https://www.unhcr.org/5dc2e4734.pdf*. The 'Our Principles' section includes being people centred, data protection and security, and purpose and proportion.
[21] OCHA/PIM, *PIM Principles* (2017) (hereafter PIM Principles). The PIM Principles include people-centred and inclusive; do no harm; defined purpose; informed consent and confidentiality; data responsibility; protection and security; competency and capacity; impartiality; coordination and collaboration.

purpose. All staff involved have a responsibility not to accidentally divulge information to other colleagues or partners, or to share data unnecessarily.

For example, a Senior Protection Officer overseeing protection case management activities does not usually need to know personal details related to an individual. Normally, aggregate data on protection cases would fulfil their level of need to know, including understanding the types of protection cases received and the responses provided. When a caseworker under their oversight needs advanced technical assistance on a case, for example a high-profile case where intervention with government authorities is needed, this could fall under “need to know”.



Purpose specification

Within the context of protection data, personal data should only be collected if it’s necessary for a specific protection-related activity, service or outcome – i.e. a defined purpose.[22] In addition, data collected for one specific purpose cannot automatically be used for another purpose. Imprecise, indefinite, or overly-expansive reasons should not be accommodated under need-to-know, it should be specific to the individual.

In practice, when processing personal protection data, this means that staff need to carefully think through the purposes for which they are collecting, storing, sharing and analysing information, and be sure that these are clearly articulated to all concerned, and most especially to the data subject. The purposes for which it is acceptable to use the information must be documented for all information collected to minimize the risk of improper processing.

For example, when conducting a Best Interests Assessment (BIA), the purpose is to provide necessary and timely assistance and protection for children at risk. As such, relevant information about a child's situation can be collected, but personal data on other members of the household, for instance, should be limited to what is necessary to understand the child's situation. However, should an organisation wish to use personal

[22] See also PIM Framework for Data Sharing in Practice, p.1.

data collected during the BIA to contact individuals for a purpose outside of providing assistance and protection as agreed during the BIA, for example, a research initiative, this would not be acceptable.

Necessity and Proportionality

"The processing of personal data should be necessary and proportionate to the purpose(s) for which it is being processed. Therefore, data that is processed should be adequate and relevant to the identified purpose, and not exceed that purpose."[23] "This requires, in particular, ensuring that only the Personal Data that are necessary to achieve the purposes (fixed in advance) are collected and further processed and that the period for which the data are stored,"[24] before being anonymized or deleted, is limited to the minimum necessary.

In practice, for personal protection data, this means that any information processed should be minimized and be proportional to the purpose for processing. It can be helpful to ask the question, "Do I need this information to do achieve the desired outcome for this person?". If the information is not needed and cannot be used, it should not be collected.

For example, when transferring a GBV case file, caseworkers should conduct a data minimization exercise to ensure that the information in the file is necessary for the transfer and proportional to its purpose and expected utility. In the case of a transfer, a new caseworker will take over the case, so most of the finalized and essential information relating to the GBV case such as assessments, action plans and follow-ups, and copies of documents, *inter alia*, should be included. However, information relating to non-GBV aspects of UNHCR's work with the person, for example related to Refugee Status Determination (RSD) other areas of protection, should not be included. In addition, things like a caseworker's notes, rough drafts, administrative information, and correspondence may not need to be included.

Legitimate and fair processing

Processing of personal data may only be carried out on a legitimate basis and in a fair and transparent manner. UNHCR may only process personal data based on one or more of the following legitimate bases: (i) With the consent of the data subject (ii) In the vital or best interests of the data subject (iii) To enable UNHCR to carry out its mandate (iv) Beyond UNHCR's mandate, to ensure the safety and security of persons of concern or other individuals.[25]

In practice, this means that UNHCR should only process personal personal protection data when the following conditions are met: 1) There is a legitimate basis for processing (see above definition); 2) there is a legitimate and specific purpose for processing (see below); and 3) processing is in accordance with the rights of the data subject, including

[23] *UNHCR Data Protection Policy*, p.16
[24] ICRC, *Handbook on Data Protection in Humanitarian Action*
[25] *UNHCR Data Protection Policy*, p.16

their right to transparent information about data processing. If the information is not needed and cannot be used, it should not be collected.

For example, when working with a partner on a community-based protection project, UNHCR could ask for individual numbers, contact details and basic disability related information of persons with disabilities to be shared with UNHCR for the purposes of providing assistive devices and other support services, on the basis of consent (provided by the data subject). In this case, the legitimate basis is the consent of the data subject and the legitimate purpose is to provide assistive devices and other support as needed. Additional measures to ensure fairness would be, *inter alia*, to provide information in ways that are accessible to the data subjects and to make sure that data subjects (e.g. facilitating access to sign language interpretation during data collection) are informed about how they will be contacted by UNHCR.

Survivor-centred approach

"A survivor-centred approach aims to create a supportive environment in which each survivor's rights are respected and in which the person is treated with dignity and respect. A survivor-centred approach recognizes that every survivor:

- Has equal rights to care and support;
- Is different and unique;
- Will react differently to their experience of GBV;
- Has different strengths, capacities, resources and needs;
- Has the right, appropriate to her/his age and circumstances, to decide who should know about what has happened to her/him and what should happen next; and
- Should be believed and be treated with respect, kindness and empathy."[26]

In practice, in relation to sharing personal protection data, this means that survivors should be informed about how their data will be recorded, stored and used and given the opportunity to decide whether they want to share their data or not. Confidentiality is central to the survivor-centred approach (see section on confidentiality above). The survivor-centred approach is specifically relevant to survivors of GBV. However, it may also be useful for working with survivors of other types of violence and human rights violations. In the case of children, the survivor-centred approach must be applied in conjunction with the principle of the best interests of the child (see below).

For example, when making a referral for a survivor of GBV, caseworkers should never pressure a survivor to accept a particular service or to share information, even if in the caseworker's opinion it might be in the interests of the survivor.

Best Interests of the Child

[26] *InterAgency GBV Case Management Guidelines: Providing care and case management services to gender-based violence survivors in humanitarian settings* (2017)

"In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."[27] "The term best interests of the child broadly describes the well-being of a child. Such well-being is determined by a variety of individual circumstances, such as the age, gender, level of maturity and experiences of the child, as well as other factors such as the presence or absence of parents, quality of the relationships between the child and family/caretaker, physical and psychosocial situation of the child, and her/his protection situation (security, protection risks, etc.). Its interpretation and application must conform with the Convention on the Rights of the Child and other international legal norms, as well as with the guidance provided by the Committee on the Rights of the Child."[28]. This gives the child "the right to have her or his best interests assessed and taken into account as a primary consideration in all actions or decisions that concern him or her, both in the public and private sphere."[29]

In practice, this means that organisations must: 1) assess and determine the best interests of individual children (including adolescents) before sharing their personal protection data, and 2) conduct an analysis of policies and procedures relating to sharing of personal protection data to ensure that children's best interests are considered and safeguarded. The analysis should include specific groups of children (such as child survivors of GBV) as well as children in general.[30]

For example, when developing SOPs for family tracing and reunification, operations should identify risks in relation to sharing children's personal protection data, and put in place appropriate mitigation measures, such as regular training for staff, spot-checks and audits on file management systems, and digital security measures such as regularly changing passwords. For individual children, before making a referral for family tracing, the risks of sharing information about the child in the country of origin, as well as the child's wishes and current situation, must be considered before sharing information.

Human rights-based approach

A human rights-based approach is a conceptual framework that integrates the norms, standards and principles of the international human rights system into the policies, programmes and processes of development and humanitarian actors.[31] It therefore focuses on both procedures and outcomes.

In practice, this means ensuring that the full range of rights of persons of concern are considered and promoted in work relating to the sharing of personal protection data. It follows that the purpose of sharing information should be protective and in line with human rights principles and standards, and that the process should ensure respect for

[27] *Convention on the Rights of the Child*, Art. 3(1)
[28] *UNHCR BIP Guidelines,* p.26
[29] *Ibid.*
[30] *Ibid. p. 30*
[31] See also 'people-centred and inclusive' principle in PIM Framework for Data Sharing in Practice.

the rights and dignity of individuals. It should also be noted that, where identified risks may inhibit sharing for purposes that are protective, organisations should work together to overcome those risks in order to allow for safe, responsible and purposeful information sharing. The sharing should promote the safety, dignity, rights and capacities of POCs and affected communities.

For example, when sharing information for human rights monitoring mechanisms, operations should undertake a joint benefit and risk assessment prior[32] to collecting and sharing information in order to ensure the safety and dignity of persons providing information, members of their household or community, as well as of others involved in the data management process.

Do No Harm

"Although it is often extremely difficult to anticipate the consequences of certain activities, or to determine when an action could result in harmful effects, it is nonetheless the ethical and legal obligation of protection actors to take measures to avoid such negative consequences. Such measures are essential during the analysis, design, implementation and monitoring of all protection activities. Protection actors must keep in mind that protection activities can inadvertently stigmatize individuals or communities who may be seen as providing sensitive information to monitoring bodies, or as supporting opposing parties. Such perceptions must be kept in mind by protection actors, who bear the responsibility of avoiding or mitigating such negative consequences of their activities."[33] The Do No Harm imperative applies to UNHCR and partners' data activities as much as it does to protection interventions.[34]

In practice, this means that the potential for harm in data management activities need to be thoroughly identified, considered and discussed with sector-specific protection specialists to understand real, perceived and potential harm and consequences. Think through the risks and benefits, identify realistic prevention and mitigation strategies document this process, for example as part of a Data Protection Impact Assessment.[35] The benefits, or expected positive protection outcomes of the data activity, should always outweigh the risks, bearing in mind the planned prevention and mitigation measures.[36]

For example, labelling a referral for cash assistance as "GBV Referral" could be perceived as helpful because it is clear and indicates a level of priority, but this ends up being stigmatizing and breaks the confidentiality of the survivor. This is an example of potential unintended harm that could come from a lack consultation from GBV specialists or a lack of inclusion of women and girls' voices. Instead, the referral could simply be labelled as high priority, without any reference to GBV.

[32] *See* PIM Framework for Data Sharing in Practice, pp.3-5.
[33] ICRC Professional Standards, p.27
[34] See also 'do no harm' principle in PIM Framework for Data Sharing in Practice, p.1
[35] See UNHCR, Guidance on the Protection of Personal Data of Persons of Concern to UNHCR, pp.51-55
[36] *See* PIM Framework for Data Sharing in Practice, pp.3-5.

Operationalisation

This section of the Technical Note provides practical guidance for applying data protection and protection standards to personal protection data.

It is divided into three sections:

- **Cross-cutting issues**: this section provides do's and don'ts that need to be considered throughout the data sharing process.
- **Legitimate bases**: this section outlines the appropriate legitimate bases that can be used for sharing of personal protection data between UNHCR and partners.
- **Legitimate purposes**: this section outlines the appropriate legitimate purposes which can be used for sharing of personal protection data between UNHCR and partners. It includes scenario-based examples to illustrate how these can be applied in different contexts.

© UNHCR/Roger Arnold

Cross-cutting issues

Protection Sensitive Processing

DO make sure that programming related to data processing follows international protection standards.

DO agree how data subject will be contacted.

DO make sure that confidentiality is respected at all times.

DON'T follow up with GBV survivors in their home.

The sharing of personal protection data must always remain situated within the purposes and principles of the broader framework of protection programming. This means that key protection principles and standards such as do no harm, the survivor-centred approach, and the best interests of the child must always be respected (see Principles section for more information). Whenever making arrangements for the sharing of personal protection data, UNHCR must identify the expected benefits and risks, identify realistic prevention and mitigation strategies for the risks, and ensure that there are no foreseen consequences of the processing which would be contrary to these principles and standards.

For example, in humanitarian settings, it is common for service providers to use home visits as part of their service delivery approach because it is an easy way to access individuals and families in need of services. While there are several benefits to using home visits as part of a case management service, for cases of GBV, home visits are not advised or supported because of the challenges they present to maintaining the survivor's confidentiality and safety. Visiting survivors' homes as part of a follow-up service can put their lives at risk, as it could expose that they have reported an incident, particularly in situation of intimate partner violence and child sexual abuse.

DO make safe and ethical data sharing part of a PPA.

DON'T put pressure on partners to share data without consent from PoCs and a clear purpose.

PPA negotiations should always be held in the spirit of equality and complementarity between partners. Data sharing arrangements that are safe and that respect the data subject's rights and that facilitate protection and assistance should be included. Sharing personal protection data outside of the principles and purposes outlined in this document should not be included in nor a condition of partnership agreements.

Consent

DO work together to ensure adherence to informed consent good practices.

DON'T share information without the data subject's consent, except in exceptional circumstances (see below).

Ensuring the processes around consent are followed is critically important to our work. Part of a survivor-centered or rights-based approach is ensuring we respect the confidentiality, choices, and decisions of the PoC. This means that data subjects are fully informed of risks and benefits, especially as it concerns information sharing. Informed consent is a two-way exchange of information, not the one-off signing of a form.

It could be said that obtaining consent is more of an art than a science. However, there are measures that UNHCR and partners can implement to ensure that data subjects fully understand how their information will be used and shared. For example, conducting joint trainings on informed consent with UNHCR and partner caseworkers, or jointly developing guidance on asking for consent in a given context, including consent scripts in different languages and formats.

DO include/ develop child-friendly procedures for informed consent and assent.

DON'T share information without the child's informed assent and the caregiver's informed consent (where appropriate).

Respecting the wishes and choices of girls and boys and their caregivers (where appropriate) is central to the principle of the 'best interests of the child' and 'do no harm'. A child's views must be given due weight in accordance with the child's age and maturity. When we need to go against these wishes, in line with the best interests of the child, this needs to be carefully considered and communicated with the child and their caregiver if appropriate to ensure they fully understand the reasons behind such decisions (please refer to the Principles section above for more information on the best interests of the child and on confidentiality).

DO limit the sharing of individual case information to referrals with the data subject's informed consent, following the guidelines for informed consent/assent for children and best interests.

There are times when it is necessary to share individual case information through a referral to facilitate access to a service without the data subject having to repeat the information about the incident already given to the first service provider. Using a survivor-centered or rights-based approach means that the data subject has as much control as possible over the information related to the incident. Detailed information about the specific case should only be shared with specific actors for a determined purpose and if the data subject consents.

DON'T mandate that service providers submit individual case files (i.e. intake or incident report form) as routine reporting.

DON'T share case files without the consent of the data subject and only on exceptional occasions according to the needs of the PoC.

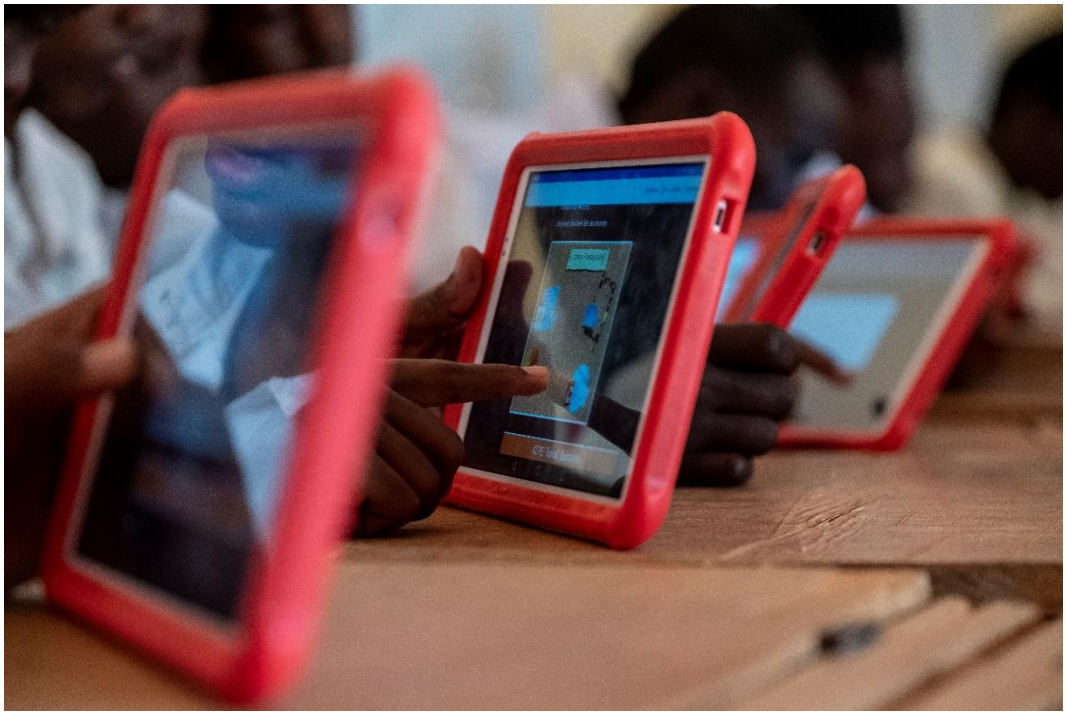
DO give PoC the full range of choices in the consent process.

In general, case files or full accounts of protection incidents rarely need to be shared. Rather, only relevant information to the service to be provided can be shared – for example, if a child has already provided an account of their arrival in a country of asylum as part of a BIA, sharing that account with RSD officers can avoid the child having to repeat their story. It may not, however, be relevant to share information about the child's current psychological state (note however, that information that is relevant for RSD will depend on the context).

In rare situations it may be necessary to share a case file or a full account of an incident, for example,

- if total care/support of a person is being transferred because an organisation is pulling out or the person is moving to a new location where another organization will provide support (with data subject's consent);
- if sharing the full account of an incident or case will avoid the need for a person to be re-interviewed about traumatic events, or will provide documentary support for a person's RSD or durable solutions case. A data subject's consent should always be sought before sharing a full account of an incident or a case file.

PoC have the right to know how their information will be used. Think about the end result. Be transparent with PoCs about how their information will be processed and shared, so they can make an informed decision.



© UNHCR/Sebastian Rich

Purpose Specification

DO be as specific as possible about the purpose for information sharing.

DON'T use overly broad or non-specific purposes such as 'international protection' or 'fulfilment of UNHCR's mandate'.

DO think through the purposes for which processing of personal data is needed in the context of the operation/project and all the activities that the project entails.

A critical step in ensuring safe and responsible sharing of personal protection data is defining the specific purpose or purposes for sharing. On the whole, purposes should be as specific as possible, providing as much detail as feasible about how, when and why information will be shared, and with whom. The purposes of both the data collection itself and the data sharing should also be clearly and transparently explained to PoC for their consent considerations.

When articulating a purpose for sharing personal protection data between partners, follow these three steps:

- State the benefit to the person of concern, noting that this must be something that, if personal data is being shared, it *directly* benefits the individual concerned, such as provision of protection or assistance services. *Indirect* benefits, like improving programming for all PoC, are not permissible, since those can be achieved without sharing personal information.
- List the specific activity(ies) or service(s) (e.g. cash assistance, protection counselling, legal assistance) that will be or could be provided as a result of sharing the information. Be sure to provide as much detail as possible, for example: contacting PoC for an interview to assess eligibility for cash assistance.
- List the modalities of information sharing / processing, for example: if there is a relevant time period for storing or processing the information (e.g. 6 months, duration of partnership, duration of refugee status, etc.), the functions of people who will have access to the data during this time, and what specific data elements are needed.

DO consider whether anonymised or aggregate data would be sufficient for the purpose

For many purposes, anonymised or aggregate data may be enough. For example, for the purposes of research or quality monitoring, often anonymised data is sufficient. For the purposes of reporting or trends analysis, usually aggregate statistics, disaggregated according to agreed data points, are sufficient. In normal day-to-day programming, personal protection data is usually only needed for the provision of protection and assistance services to individuals.

DO establish the purposes for data sharing between partners in advance, and document these in PPAs and SOPs and Data Sharing Protocols.

Consider the purposes of information sharing as part of SOP development in relation to any protection activities that involve the processing of personal protection data. At all steps of an activity that involves processing of personal protection data, there should be one or several specific purposes. These are defined and agreed between partners at an operational level, and endorsed at a management level. When working with funded partners, the purposes for sharing information should also be included in Annex F of the PPA.

DO provide information about the purposes of data sharing to PoC in a transparent and accessible manner.

DON'T pressure or mislead PoC into agreeing to share data

It is important to be as clear and simple as possible in explaining the purposes of data sharing to PoC. Ideally, the way that the purposes are explained should be tested with focus groups of different ages, sexes, disabilities, nationalities and other diversities, in order to ensure that they are easily understood. Examples can also be used or shown.

When explaining purposes to PoC, avoid using complex language and sentences, or vague qualifiers such as 'may', 'might', 'possible', 'some', etc.. For example, "We will share information with UNHCR so that they may use your personal data to develop new services", or "for research purposes", is not sufficiently specific. However, the following would be sufficient: "If you are interested in receiving the described UNHCR service, I will share XX information with UNHCR."

Processing for Other Purposes

DO clarify the purpose of information sharing, and only share relevant information (see above).

There are a limited number of legitimate purposes for sharing personal protection data, which are outlined in the section below. The purpose(s) for sharing information from that list should be clearly presented as a choice to PoC, along with benefits and risks in order to have a meaningful discussion about consent for information sharing.

DON'T use information collected for one purpose for a different purpose without consent.

When a data subject provides consent for a specific purpose, that consent can't be transferred to other purposes. If information is to be used for another purpose than that for which it was collected, additional consent must be obtained for the new purpose. For example, if someone consented to sharing their information with UNHCR for relocation, their personal information cannot then be utilized for sharing with livelihoods programs, or for research or advocacy purposes, without further consent. (See below on exceptional circumstances.)

DO discuss and clarify what action and how you will take that action based off information shared.

Having a proactive discussion with implementing and operational partners about how information will be used specifically can aid in establishing a better understanding between UNHCR and partners. This will also ensure the right language is being used to discuss consent with PoC, and that accurate information is being shared with them about the purpose.

Exceptional Circumstances

DO try to anticipate what exceptional circumstances might arise in your context, and set parameters for these with partners and PoC in advance.

Exceptional circumstances occur when data subjects cannot provide consent due to medical or other urgent situations, but processing their data is in their immediate and vital interests. Examples include, when a person is unconscious and cannot provide consent, when a person poses an immediate threat to themselves or others, or when persons cannot be reached to provide consent due to active conflict or ongoing displacement; or when access to a person is arbitrarily denied by a relevant authority. In such cases, it would be acceptable to share or otherwise process personal protection data without consent, as long as such processing was required for an immediate and necessary intervention in their vital interests. For example, providing information about a person's plans to commit suicide to a specialized care provider may be necessary to save a person's life. Even in these cases, we must do everything we can to explain to PoC the action we are taking on their behalf and listen to concerns they may raise about further harm.

DO explain to PoC what possible exceptional circumstances might be for sharing data without consent as part of your consent process.

Exceptional circumstances also occur, as per the Standard General Provisions of the PPA, in cases of the identification of individuals associated with terrorism, and investigations into fraud committed by PoCs and misconduct by anyone contractually linked to the UN, such as corruption and possible sexual exploitation and abuse.[37] In such cases, it may be required and permissible to share personal protection data without consent, in particular if seeking consent could compromise the integrity of the investigation and/or expose victims or others to harm. However, sharing in these cases should be examined on a case by case basis.

Exceptional circumstances may also arise in the context of preserving the safety of POCs, in particular in the context of an ongoing and serious security threat (e.g. recovering or transporting files in case of possible seizure by a third party).

DO conduct a risk assessment before sharing any information.

Even in exceptional circumstances, however, a benefit and risk assessments should be done to ensure that the foreseen risks of processing do not outweigh the benefits, bearing in mind prevention and mitigation measures. In the above

[37] See UNHCR, Project Partnership Agreement, Appendix 2 : Standard General Provisions, in particular paras. 4.9 (terrorism), 5.5 and 5.5 (sexual exploitation and abuse), and 5.10 (sexual exploitation and abuse, violations of human rights, fraudulent acts, corrption or any other form of misconduct).

DON'T neglect the do no harm principle even in exceptional circumstances.

example, the information relating to a planned suicide should also only be shared where the service provider in question has been assessed as safe and able to provide care. It may not, for example, be appropriate to share such information if this would expose the data subject to a risk of *refoulement*, where another option or service provider may be available.

Data Security

DO conduct joint assessments related to data protection and data security with partners.

DO ensure that prevention and mitigation measures are included within the PPA.

UNHCR's Data Protection Guidance includes a partner assessment checklist that can be used to go through basic data protection and data security issues, and identify feasible technical and organisation measures. Where issues are identified, UNHCR and the partner should agree on mitigation measures, such as using unique identifiers rather than names. If these require additional funding or resources, like locked filing cabinets or additional IT equipment, this should be included in the PPA if possible. It is also recommended that all actors involved should identify the relevant data protection and security policies and guidelines of their respective organizations, prior to data sharing.

© UNHCR/Cristiano Minichiello

Legitimate Bases

All sharing of personal protection data between UNHCR and partners requires a legitimate or a lawful basis. Consent is usually the preferred basis for sharing personal protection data such as case management information and details of protection vulnerabilities or incidents, however, there are 4 legitimate bases on which UNHCR may request for information to be shared:[38]

- **Consent:** Consent is the most frequently used and often the preferred legal basis for the processing of personal protection data processing. As noted above (see principles section), obtaining consent is a fluid and challenging process, in particular given unequal power dynamics that usually exist between service providers and data subjects. As such, UNHCR and partners must invest sufficient resources in the development of consent processes and procedures, and training of staff on these, to allow for consent to be both informed and freely given and to serve as the legitimate basis for the processing of personal protection data. Different methods can be used to obtain consent, but 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.
- **Vital interests**: Vital interests can be used as a legitimate basis for processing 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. In instances where vital interests is used, the specific purpose should be related to a tangible and immediate danger/benefit to the data subject (see for example, section below on Exceptional Circumstances). Vague or possible future protection risks or threats, for example, cannot be used to justify processing based on vital interests. Examples are: urgent and lifesaving assistance, processing of data of POCs who are unable to provide consent due to their state of health (including unconsciousness), to secure the release of a POC from detention, or similar facility, and where UNHCR does not have access to obtain consent directly from the individual.
- **Best interests** can also be used as a legitimate basis for processing the personal protection data of children. This would normally be in cases where parents/guardians are absent and unreachable, and the age and maturity of the child does not allow them to provide consent for the processing in question. It can also be used where consent is not provided in cases where the best interests of the child is specifically assessed and determined, taking into account the views of the child and parents/guardians. Examples include: processing of personal data relating to unaccompanied or separated children in their best interests.
- **To enable UNHCR to carry out its mandate.** UNHCR's mandate may be used as a legitimate basis where there are important grounds of public interest are triggered when the activity in question is part of a humanitarian mandate established under international law. This basis is usually not applicable to the processing of personal protection data, since consent is the preferred basis for any processing, and any circumstances where processing is otherwise

[38] Information in this section is based on the UNHCR Data Protection Policy. *Neither implementing partners nor operational partners are bound by UNHCR's Data Protection Policy; rather, they are expected to respect the "same or comparable standards" (DPP, paras. 5.1 and 6.1). The specific standards by which NGO partners are bound will vary depending on any domestic legislation on data protection that has been adopted in the country in which they are operating, any applicable regional legislation, and any internal data protection rules, policies and procedures that the NGO concerned may itself have adopted.*

necessary would normally be acceptable only in the vital or best interests of the data subject. Exceptional cases where this legitimate basis may be used to request personal protection data could be processing data measures taken in the context of formal investigations into possible fraud committed by PoCs, or 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. It may also apply in the case of individuals linked with terrorism. In all of these cases, the purpose specification must be linked to particular individuals, and cannot be applied on a blanket basis. Exceptional circumstances may also arise in the context of preserving the safety of POCs, in particular in the context of an ongoing and serious security threat (e.g. recovering or transporting files in case of possible seizure by a third party).

© UNHCR/Mohamed Alalem

Legitimate Purposes

The following section provides guidance on some common and general legitimate purposes for sharing personal protection data between UNHCR and partners. These purposes have been developed with the common protection activities that are covered in this Technical Note in mind – notably protection case management, individual protection assessment / vulnerability assessment, protection monitoring, and the delivery of protection services such as psychosocial support, legal or other protection counselling etc.. The legitimate purposes for sharing listed below thus relate directly to the purposes for data collection associated with those activities. In each context, these general purposes should be supplemented with specific purposes relevant to the context (see section above on Purpose Specification). In addition, whether these general purposes apply or not will depend very much on the context of the Operation, including UNHCR's role, the type of protection programming being implemented, and other factors. Note that this does not preclude sharing in exceptional circumstances (see section above on Exceptional Circumstances).

Open, active cases for referrals for specific and immediate protection services and assistance

This general purpose covers the sharing of personal protection data related to PoCs currently being seen by one organisation (UNHCR or a partner organisation) in order to provide access to an immediately available protection or assistance service provided by another organisation (UNHCR or a partner organisation).

What is this:	This purpose covers the sharing of personal protection data for a needed, immediately available service referrals that immediately benefit the individual. Information sharing for referrals is done with the data subject's consent, and/or where it is in the best interests of the child, or, in exceptional circumstances where consent is not possible or provided, where it is in the vital interests of the data subject (i.e. they are a risk to themselves), or where the data subject is a risk to the safety and security of others.
Questions to consider:	• What is the purpose of sharing personal protection data in this context? • Who will the data be shared with? Who will have access? How will the data be stored? • Is there a chance the data will be shared further? • How will the data subject be contacted?
How to do this well:	UNHCR and partners should discuss and get clarity on all available services offered (typically captured in SOPs) in order to facilitate referrals for services. This should include detailing the minimum information needed for the referral (typically service needed and basic identifying information, but may include more information where this is required for the service), the communication method for contacting the data

	subject and a method for feedback on the referral (see section on Necessity and Proportionality for more).
Benefits:	Information sharing for referrals will facilitate timely and effective service provision for persons of concern. Providing personal protection data can ensure that individuals access a service more quickly, more safely, or in a way that is better tailored to their needs. It can also avoid an individual having to repeat themselves.
Risks:	• Exposing the data subject's protection report/breaking confidentiality to perpetrators/family/friends/neighbours • Stigmatisation • Retribution • Reluctance to seek help/assistance • Unmet expectations • Lack of trust of service providers Mistrust among partners, or between UNHCR and partners • Lack of access to services and no follow up is possible because information was not provided. • Lack of service provision due to inadequate information provided (e.g. referral deprioritised or considered not eligible for lack of information). • Unnecessary and harmful re-interviewing of data subjects because information has not been shared from one service provider to another. • Duplication of services because information has not been shared form one service provider to another. • Harm/risk for service provider/case worker
Okay to Share:	It is permissible to share personal protection information in an agreed-upon referral form (including agreed necessary data elements) when the service referral is currently needed and available; and provides specific benefits to the data subject; with the data subject's consent and/or where it is in the best interests of the child. As always, referrals are made on a case by case basis, not indiscriminately.
Not Okay to Share:	It is not permissible to share this personal protection information when there is no consent from the data subject, or no clear information on the benefit or service to be received. It is also not okay to share large amounts of data (e.g. whole case files) indiscriminately, especially where there is not a guarantee that the service will be provided or all the information is not essential to the purpose.
Beneficial Practice:	Developing clear referral pathways that include information flow and data elements required. Giving criteria for resettlement/other solutions to partners so they can make relevant, more specific referrals for PoC. Documenting the answers to the questions above in SOPs or similar documents, and having it endorsed by the senior management of all the actors involved before any data is shared.

Sample Scenarios

- In Operation A, NGO A provides legal counselling. NGO A often sees clients who have legal complaints relating to GBV issues, and its caseworkers have noted that many would benefit from being referred for livelihoods services. NGO A decides to refer all its GBV clients to a livelihoods partner, NGO B, without the consent of the clients. One of the perpetrators of a GBV incident works at NGO B, and recognises his victim in the referrals. After calling NGO A about the referrals, he realises that she has filed a case against him. As a result, he seeks her

out and threatens her life, and also shares the details of others survivors referred to NGO B.
In this scenario, the staff of NGO A have violated data protection rules by sharing information without consent, resulting in a further data breach by the staff member of NGO B. Even when a staff member thinks a person would benefit from livelihoods services, they must not share their information without consent (except when the limitations of confidentiality apply – see section on Informed Consent above).

- In Operation C, NGO C provides psychosocial support for persons with mental health conditions. UNHCR has asked NGO C to refer persons who require particular medical support as well as survivors of violence for consideration for resettlement. When NGO C assesses that a particular person meets either of these criteria, NGO C explains the process of resettlement consideration, including that there is no guarantee of acceptance, and asks for consent to submit their details to UNHCR. NGO C then fills out an agreed referral form which provides essential details about the case that allow UNHCR Resettlement Staff to identify if the person should be interviewed for resettlement consideration. In cases where UNHCR needs more information from NGO C, UNHCR may also ask, with the consent of the data subject, for NGO C to share additional details that are needed for the submission such as incident descriptions, interview transcripts, medical records, etc.
  In this scenario, consent is obtained at different stages for information sharing at different levels. Less information is provided in the initial referral, since this is only needed to determine eligibility for a resettlement interview. Providing too much information (e.g. whole case file) at this stage would be disproportionate to the purpose. However, at a later stage, when the information is needed for the submission for resettlement, more information may be provided, but consent for this additional sharing will need to be sought from the data subject.
- In Operation D, NGO D runs a support group for LGBTI individuals. In UNHCR's weekly protection information sessions, staff are often approached by LGBTI individuals asking about support services. Rather than provide a referral to NGO D, which operates on the basis of anonymity due to security considerations, UNHCR staff provide information to individuals on how they can contact NGO D themselves.
  In this scenario, no sharing of personal data is required for the referral. While it may be less likely that all individuals wanting support from NGO D will access their services without the benefit of a specific referral, a data protection risk assessment has indicated that the risks of providing the referral outweigh the benefits.

Open, active cases for referrals for protection services and assistance which are provided in the future or immediately, based on information known to UNHCR.

This general purpose covers the sharing of personal protection data related to PoCs currently being seen by a partner organisation with UNHCR in order to allow UNHCR to assess their eligibility for protection or assistance services that are either available immediately or may be provided in the future.

What is this:	Many protection and assistance services in UNHCR operations are provided on the basis of information known to UNHCR, rather than being provided on the basis of referrals. This allows UNHCR to ensure efficient and targeted service provision on the basis of objective criteria, and to prioritise individuals by weighing and combining different factors. This method of providing assistance and protection services is, in some cases, also adopted as part of fraud mitigation measures, where referrals are likely to be 'bought'. In addition, given that UNHCR remains in refugee operations for the duration of a person's time as a refugee, some services which may not require a referral currently, may be needed by an individual in the future. By ensuring up to date and accurate basic protection information on persons of concern (with their consent), UNHCR can make sure that its services are always tailored to their specific needs. Essentially, if a POC meets certain criteria, they can access a service or be added to or prioritized for an intervention.	
Questions to consider:	• What is the purpose of sharing personal protection in this context? • Who will the data be shared with? Who will have access? How will the data be stored? • Is there a chance the data will be shared further? • Will there be an individual follow-up on the data? How will the data subject be contacted? • How can the purpose and processing be communicated transparently and effectively to data subjects, bearing in mind accessibility?	
How to do this well:	UNHCR and partners should agree on the list of potential protection and assistance services that can be accessed or are likely to be accessed in the future (e.g. those in relation to voluntary repatriation) in a particular operation. UNHCR should provide clear and transparent information about how data will be processed, stored, shared and used, and how data subjects may or may not be informed about this or contacted. UNHCR and partners should also take steps to identify and mitigate any identified risks in the process. UNHCR should not ask for information to be shared without the consent of the data subjects, and partners should ask for consent from PoC in good faith.	
Benefits:	Having updated protection and vulnerability information stored with UNHCR can result in a person receiving additional protection and assistance services, or services that are specifically tailored to their individual situation. While there is not a guarantee that a person will benefit from sharing their information with UNHCR, data subjects have the right to be informed of their options in terms of data sharing.	
Risks:	• Exposing the data subject's protection report/breaking confidentiality to perpetrators/family/friends/neighbours • Stigmatisation • Retribution • Reluctance to seek help/assistance • Unmet expectations • Lack of trust in service providers • Mistrust among partners	• Individuals at risk are not provided with necessary services or prioritisation for services • Individuals are re-interviewed or services are duplicated because no information or system to flag that a person had already been in touch with an existing service provider. • Harm/risk for service provider/case worker

Okay to Share:	It is only ok to share limited personal protection data about a protection incident or vulnerability for this purpose (for example, a specific needs code or case number). It is permissible to share this information in an agreed-upon referral form/modality with the data subject's consent.
Not Okay to Share:	It is not ok to share extensive information about protection incidents or vulnerabilities for this purpose (for example, GBV intake forms or full assessments or case files). If additional information is needed at the time of service provision, this can be requested from the data subject and/or service provider (with the data subject's consent). It is not permissible to share limited protection incident or vulnerability information for this purpose when there is no consent from the data subject, or if UNHCR has not provided information about the services for which data will be processed and modalities of processing.
Beneficial Practice:	Sharing a list of what programs/services could be included; including information on how people will be contacted and how protection incident data will be kept confidential.

Sample scenarios:

- In Operation A, UNHCR provides cash assistance based on a scorecard methodology that draws from various demographic and protection data points about individuals known to the organization. In this operation, exposure to protection incidents or existing vulnerabilities are inputted into a person's score, which may impact their eligibility for assistance or the amount they receive. Partners cannot, however, refer individuals directly for cash assistance. NGO A, which provides an individualised information service for PoCs, agrees to provide information to data subjects about the option to update their vulnerability / protection incident data with UNHCR, being clear that information sharing does not directly result in a service, and that the information will not be further shared or processed without their consent.
  In this scenario, the information shared must be proportional to the purpose – i.e. NGO A should share with UNHCR only the information that is needed for the cash score calculation, and no further details. NGO A should provide sufficient information to the data subject to ensure that they are aware that their information will be used in UNHCR's processes for determining eligibility for cash assistance, but do not need to be given full details of the scoring criteria. UNHCR should ensure that only staff who need to know are able to access the information shared and that this information is securely stored.
- In Operation B, UNHCR provides durable solutions and complementary pathways assistance for PoC, including identifying cases for resettlement, providing counselling and support on complementary pathways, and providing individual counselling and assistance for vulnerable persons returning home. These services are not necessarily available immediately, but rather could be triggered at any point during a person's time as a refugee, depending on their individual situation as well as external factors (e.g. availability of resettlement places, favourable conditions for return, etc.). NGO B, which provides case management for survivors of torture, agrees to provide information to data subjects about the option to update their vulnerability / case management information with UNHCR, being clear that information sharing does not directly result in a service, and that the information will not be further shared or processed without their consent.
  In this scenario, NGO B should share only the specifc information which will allow UNHCR to

tailor their assistance to survivors of torture (e.g. specific needs code, summary of case). UNHCR should ensure that only a very limited number of staff who have appropriate training and relevant roles and responsibilities have access to this information.

- In Operation C, UNHCR is responsible for the Best Interests Procedure. This means that UNHCR needs to ensure that the best interests of the child have been assessed and determined with regards to care plans, durable solutions, temporary care arrangements, family reunification, and separation from parents for children at risk. NGO C provides child protection case management in Operation C, and agrees to applicable specific needs codes, care arrangement details, and process information related to BIAs and BIDs (e.g. BIA completed, BID required) with UNHCR, with the consent/assent of the child/caregiver and/or in line with their best interests. This allows for UNHCR to know which children are already receiving support or have received support, in order not to duplicate assistance or assessments and potentially cause delays in case processing in other areas (e.g. durable solutions, RSD, etc.). Only key members of UNHCR's child protection staff are able to access the information shared by partners.

  Although UNHCR's involvement in best interests procedures is context-specific, in this scenario, UNHCR's involvement in the oversight of BIP as well as the need for BIP-related information to inform refugee protection case management requires that for more information is shared, although it must still be kept at the minimum required for the specific purpose depending on operational realities. Since more information is being shared, UNHCR has limited access to the information to the very few staff members who require it for the purpose.
- In Operation D, NGO D has been providing focused psychosocial support services for persons with moderate mental health conditions for the last 3 years. UNHCR has recently set up a new programme to provide cash assistance which includes persons with mental health issues in the calculation of the cash score. UNHCR has asked NGO D to provide a list of its clients, in the interests of making sure their calculation is correct. However, NGO D has previously never asked its clients about providing such information to UNHCR. UNHCR and NGO D therefore agree that from now on this will be included in NGO D's consent script, and, where possible, NGO D will reach out to its previous clients to seek their consent to share the information with UNHCR. If they are not able to obtain consent despite the dedicated measures to provide supported decision-making, however, the information will not be shared.

  In this scenario, UNHCR and NGO D have arrived at the appropriate conclusion. UNHCR and NGO D should agree on and document the details of the data sharing arrangement before any data is shared. In this document, UNHCR also needs to provide additional assurance as to how the information will be stored and processed before NGO D should agree to include this provision in the consent script. Mental health issues can be highly stigmatized, and many PoCmay not need or want for this information to be shared even if it may result in a cash benefit.
- In Operation E, UNHCR has a PPA with NGO E to provide case management services for survivors of GBV. UNHCR has requested that NGO E share specific needs codes of all of its clients for the purpose of durable solutions. NGO E does not agree to share the information because it is not able to ask for consent from PoC without a more specific purpose.

In this scenario, UNHCR and NGO E would need to agree on a consent process which will detail the services related to durable solutions which UNHCR may provide (e.g. counselling, repatriation support, consideration for resettlement, etc.) as well as how individuals may be contacted about the services (if applicable), and NGO E is now able to share the information with UNHCR where PoC provide consent.

Feedback on service referrals

This general purpose covers the sharing of personal protection data related to PoCs currently being seen by an organisation (UNHCR or a partner) with another organisation (UNHCR or a partner) in order to coordinate protection and assistance service delivery.

What is this:	When an organization providing protection case management (including refugee protection case management) to a PoC refers that person to another organization, they may ask for feedback on their referral for their own records and case management processes. There are two types of feedback: 1) process feedback (e.g. is the referral pending, accepted, rejected); and 2) service feedback (e.g. what services were provided to the person).
Questions to consider:	• What is the purpose of sharing personal protection in this context? • Who will the data be shared with? Who will have access? How will the data be stored? • Is there a chance the data will be shared further? • Will there be an individual follow-up on the data? How will the data subject be contacted? • Is personal data on services needed for UNHCR's case management, or could aggregate data on service provision fulfil the information needs?
How to do this well:	Assess in your operation with your partners what feedback on referrals is needed to fulfil UNHCR's coordination responsibilities and specific accountabilities. In some cases, usually where UNHCR's own case management processes are not affected by referral, process feedback only may be necessary, and information about service provision can be provided in aggregate form for analysis. However, in others, where UNHCR is providing particular services it could be important to have more detailed information on the service provision to the individual. This would only be necessary where additional information is needed in order for UNHCR to effectively perform its own case management or related service provision. For example, where UNHCR's own case management processes related to RSD, durable solutions, or other protection and assistance are dependent on information relating services provided by the partner. Usually, the information provided is limited to a few relevant data elements on service provision (e.g. service status, service date, or summary of outcome).
Benefits:	Providing additional feedback on referrals helps to make sure that services are coordinated between different actors involved in providing services for a person of concern. This helps to ensure timely, efficient and holistic services for persons of concern, and avoids gaps in service provision or lapses in coordination / communication between service providers.

Risks:	• Exposing the data subject's protection report/breaking confidentiality to perpetrators/family/friends/neighbours • Stigma • Retribution • Lack of willingness to seek help/assistance • Expectations unmet • Reputational risk for service providers • Mistrust among coordination actors	• Services are not provided for individuals in a timely and effective manner • People 'fall through the cracks' as referrals are made but no follow up is possible to ensure a person received a service • Harm risk for service provider/case worker
Okay to Share:	Organisations may provide 'process' feedback without the consent of the data subject, since the information relates to their own organizational processes rather than information provided by or about the PoC. For more substantive feedback on referrals, for example, relating to the status of the services provided, service types, or other details, consent should be obtained before providing feedback to the requesting organization. In addition, the specific elements of data to be shared as feedback on referrals should be agreed as part of referral SOPs between the organisations, and should be proportional to service provided.	
Not Okay to Share:	It is not okay to share extensive information about a case (e.g. whole case file or incident description) as part of process or service feedback on a referral.	
Beneficial Practice:	Mapping out what information is needed by different service providers at different points in time, and translating this into SOPs for feedback on referrals.	

Sample Scenarios

- In Operation A, NGO A provides legal aid services for PoC. UNHCR provides financial assistance and travel documents for PoC who are traveling to court hearings, material assistance for PoC in detention centres or prisons, advocacy with governments on individual cases, and reintegration of persons released from custody. As such, when UNHCR refers a case to NGO A, feedback is expected not only on whether or not the referral is accepted, but also on the status of the case and relevant dates (e.g. pending initial hearing, pending for court date, pending appeal, pending release, etc.). However, if UNHCR needs more substantive details about a legal case, it would have to provide a specific purpose for the requested information (e.g. drafting a letter to authorities on behalf of the data subject). In all cases, NGO A must ask the data subject for consent to provide the information to UNHCR. *In this scenario, UNHCR and the partner have agreed on the specific elements of information (status of the case and relevant dates) that will be shared in order to facilitate seamless service delivery for the PoC.*
- In Operation B, UNHCR maintains a weekly protection counselling clinic where refugees can come to seek information and support. UNHCR, with the consent of the data subject, refers many of those who come in to different NGO service providers. NGO service providers agree to provide UNHCR with process feedback so that UNHCR staff members can close their cases/tickets from the protection counselling clinic once all needed services are received by the PoC. If a service provider rejects a referral, however, UNHCR is able to contact the PoC (as agreed in the initial counselling session) to follow up. In addition, NGO B, which provides education support, agrees to provide aggregate information to UNHCR on

a quarterly basis about the types of services offered to persons referred (e.g. 40% of persons referred to NGO B are provided with education materials, 30% with cash grants for travel to school, and 60% are referred for enrolment). This allows UNHCR and NGO B to analyse the assistance being provided and make improvements to programming (e.g. UNHCR's information service may provide additional information about enrolment directly to PoC, and ask additional screening questions to ensure they meet the criteria for material or cash assistance before referring them to NGO B).

In this scenario, UNHCR and NGO B have determined that only aggregate information on services provided is needed to meet their information needs in this context. If UNHCR wanted further information about a person referred to NGO B, such as to which school they were referred and whether they specifically were provided with assistance, UNHCR would need to provide a specific purpose, and consent/assent would need to be obtained.

© UNHCR/John Wessels

Closed cases for access for future protection and assistance services

This general purpose covers the sharing of personal protection data related to PoCs no longer receiving services from a partner organisation with UNHCR in order to ensure access to the data by the data subject or UNHCR for future protection and assistance services.

What is this:	UNHCR maintains offices in 134 countries and retains its mandate for protecting refugees for as long as no durable solution has been identified. As such, UNHCR often remains in operations and works on individual case management as well as other forms of protection and assistance even after NGO partners may close their programmes. In such cases, it can be useful for closed cases to be transferred to UNHCR by partners when they leave an operation, in case a case needs to be reopened or referenced (with the consent of the data subject). For closed cases that are scheduled for destruction by an NGO according to filing schedules (e.g. after 7 years), see point below.
Questions to consider:	• What is the purpose of sharing personal protection l data in this context? • Who will have access to closed cases? How will closed cases be stored? • What is the process for reopening a case, or for otherwise processing data in closed cases? • Will there be an individual follow-up on the data? How will the data subject be contacted?
How to do this well:	Discuss with partners the process for transferring closed cases at the point of programme closure, and in particular the data protection measures needed to do this transfer safely and in accordance with the principles mentioned above, including data minimization, purpose specification and consent (see principles section). Consider the modalities of file transfer (e.g. hard copy only, digital copy in what format, etc.), and who in UNHCR will be able to access the files (limited to as few people as necessary for the purpose). Agree on the best ways to provide information in order for data subjects to make decisions for themselves. Put in place a regular review mechanism (e.g. once per year) to check on whether data subjects are providing consent or not, and consider whether changes need to be made to any of the above processes to improve fairness and transparency as well as protection benefits for persons of concern.
Benefits:	Keeping closed case files allows UNHCR to avoid re-interviewing data subjects about potentially difficult experiences that they have already recounted to another service provider. It also allows UNHCR to ensure that a person receives the most relevant and effective services by having a complete picture of previous actions and assistance. In many scenarios, data subjects may feel more secure knowing that the information they have provided to one service provider has not been lost, and can be referenced if needed even if the service provider itself is no longer present. It may also be safer for the PoC than having to keep their own copy of their records at home.
Risks:	• Exposing the data subject's protection report/breaking confidentiality to perpetrators/ family/friends/neighbors • Stigma • Retribution • Lack of willingness to seek help/assistance • Reputational risk for service providers • Mistrust among coordination actors • Harm risk for service provider/case worker • Lost case files • Re-traumatisation of survivors or witnesses • Ineffective or inefficient assistance due to incomplete information about services previously provided • Expectations unmet

Okay to Share:	It is okay to share data for this purpose provided that the principles of purpose specification and data minimization are respected (e.g. case files are redacted to include only essential information), and consent is obtained and/or it is in the best interests of the child. Depending on the context, for example in locations with high insecurity or mobility, it may or may not be necessary to ask for consent at intake as opposed to only at case closure.
Not Okay to Share:	It is not ok to share closed files with UNHCR when a data subject has refused this option or when it's not in the child's best interests. In addition, UNHCR should provide information to partners and PoC about how closed files will be handled, shared and accessed.
Beneficial Practice:	The process for obtaining consent for sharing closed files should be discussed with data subjects.

Sample Scenarios

- In Operation A, UNHCR is responsible for Refugee Status Determination. Refugees who previously were recognized prima facie now need to apply for status on an individual basis. NGO A, which provided services related to GBV, left Operation A 2 years ago. When it left, closed case files were transferred to UNHCR, with the data subject's consent. As a result, survivors of GBV in the country of origin were able to ask for information about GBV incidents relating to their claim for refugee status to be shared as part of their RSD claim without having to be re-interviewed.
  In this scenario, UNHCR would need to ensure that access to closed case files was restricted to the minimum number of staff who need the information (possibly one or two staff members only), and that the files were accessed only when there was a specific purpose and individual benefit to the data subject. Wherever possible, consent from the data subject should be re-verified before accessing the closed case files.
- In Operation B, NGO B provides support for persons with disabilities and their families. When a case is closed, NGO B archives the file for a period of 7 years, and then destroys it. However, NGO B, with the consent of the data subject, provides UNHCR with a summary of the case, including assessed needs, actions taken, and reasons for closure. This means that data subjects can reopen their cases or access information such as the contact details of their specialist or the serial number of their assistive device, they can approach UNHCR to request it.
  In this scenario, NGO B has appropriately minimized the case file before sharing the information with UNHCR according to the likely information needs of UNHCR and the data subject in the future. Ensuring that data subjects are well informed about how their data will be kept and how they can access it in the future is essential.

Closed cases for archiving

This general purpose covers the sharing of personal protection data of PoCs no longer receiving services from a partner organisation with UNHCR for storage of the data in UNHCR's archives in order to facilitate i) later access by the PoC as requested; ii) use by researchers in accordance with UNHCR's Records and Archives Policy.[39]

What is this:	As a United Nations Organisation, UNHCR keeps archives as part of the public record and in the public interest as part of the history of humanity. UNHCR's archives are kept for the purposes of historical research, as well as for personal access for data subjects and their family members. For UNHCR, individual case files are considered to be permanent records, and as such are subject to archiving – although access to personal data remains highly regulated as part of the archives policy. Each UNHCR office archives its own files for eventual transfer to the central archives in Geneva.
Questions to consider:	• What is the purpose of sharing personal protection data in this context? • Who will the data be shared with? Who will have access? How will the data be stored? • Is there a chance the data will be shared further? • Will there be an individual follow-up with the data subject? How will they be contacted? • How can PoC request access to their data once archived?
How to do this well:	Agree with partners on how to inform data subjects of the option to share their files with UNHCR for archiving, as well as their rights to request access to their files. Discuss with partners the process for transferring cases for archiving, and in particular the necessary data protection measures, including data minimization, purpose specification and consent (see principles section above). Consider the modalities of file transfer (e.g. hard copy only, digital copy in what format, etc.), and the schedule (e.g. if an NGO will destroy files after 7 years, archiving should take place before this). Specify who in UNHCR will be able to access the files (limited to as few people as necessary). Put in place a regular review mechanism (e.g. once per year) to check on whether data subjects are providing consent or not, and consider whether changes need to be made to any of the above processes to improve fairness and transparency as well as protection benefits for persons of concern.
Benefits:	In addition to the benefits to the general public in terms of historical research and analysis, the archiving of personal protection data also benefits individuals and their families. In the past, individual requests have been made to the UNHCR archives to support family tracing, to support judicial processes and claims for compensation for violations, and for personal information (e.g. understanding family history). UNHCR archivists review and redact case files before allowing access to researchers and/or family members, to ensure that sensitive personal information is removed.
Risks:	• Exposing the data subject's protection report/breaking confidentiality to perpetrators/family/friends/neighbors • Stigma • Retribution • Lack of willingness to seek help/assistance • Expectations unmet • Reputational risk for service providers • Mistrust among coordination actors • Harm risk for service provider/case worker • Lack of opportunities to seek redress / compensation in the future • Loss of records to support family reunification.

[39] See UNHCR, *Policy on the Management of UNHCR Records and Archives* (2017), and in particular its Appendix C, *Guidelines on Access to UNHCR Archives*, available at: *https://www.unhcr.org/3b03896a4.pdf*.

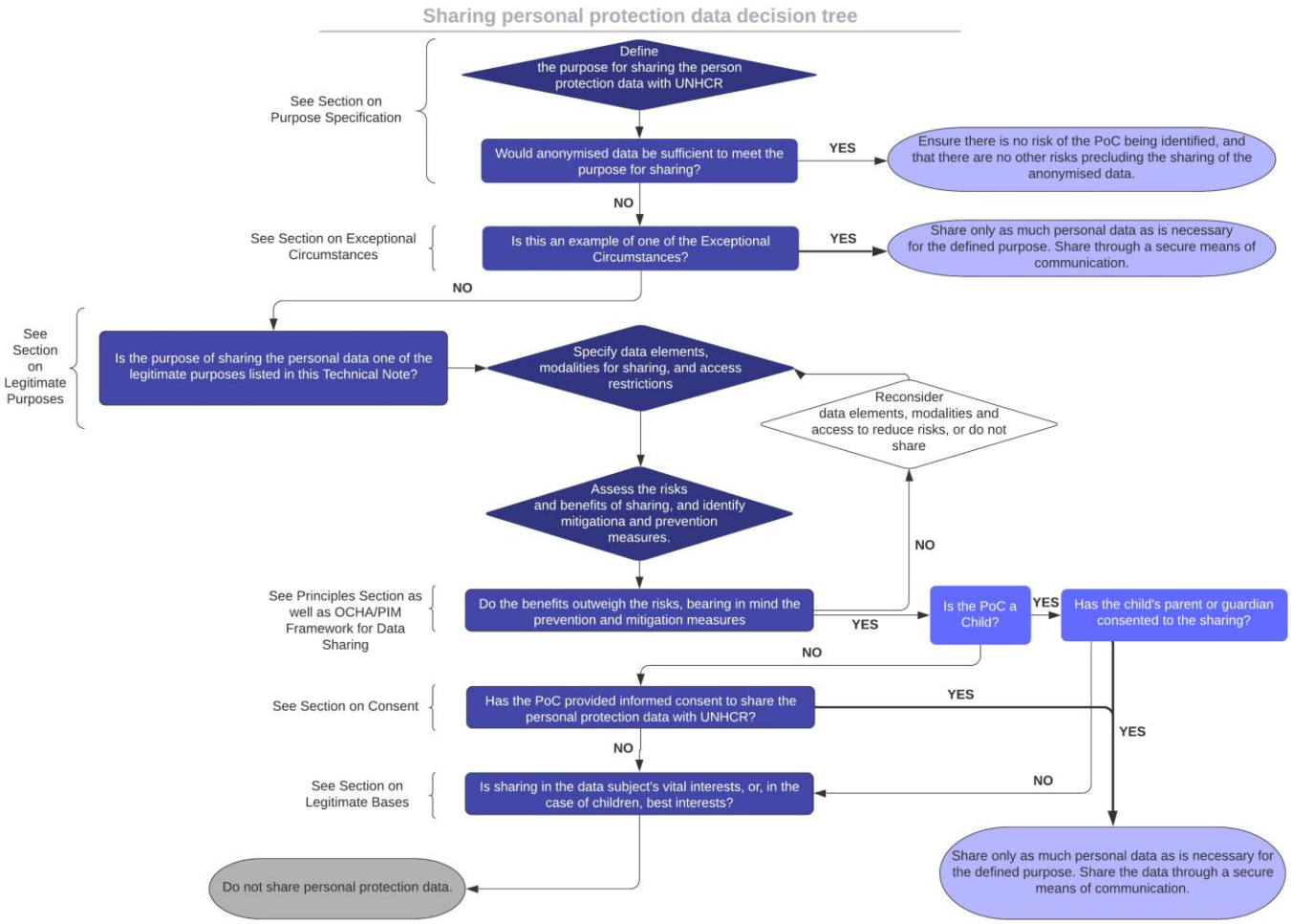
Okay to Share:	It is okay to share data for this purpose provided that the principles of purpose specification and data minimization are respected (e.g. case files are redacted to include only essential information), and consent is obtained and/or it is in the best interests of the child. Consent for transferring case files should be asked for at intake (in case of disappearance) and should be reconfirmed at case closure.
Not Okay to Share:	It is not ok to share case files to be archived with UNHCR when a data subject has explicitly refused this option or when it's not in the child's best interests. In addition, UNHCR should provide information about how case files will be handled and accessed.
Beneficial Practice:	Ensuring extremely restricted access to archived case files, based on a formal request procedure that respects the principles mentioned above.

Sample Scenarios

- In Operation A, UNHCR and partners conducted family tracing and child protection case management for unaccompanied children before making decisions about alternative care or family reunification during a crisis that occurred 20 years ago. In many cases, children were too young to fully understand the determinations that were made at that time, and may have lost copies of their documentation over time. Now, children looking for traces of their parents or relatives, can request and access copies of their files from the UNHCR archive, where they may find invaluable information on their family and personal history.
  In this scenario, ensuring that children and caregivers are well informed about how their information will be kept is essential to ensure consent/assent, and/or in assessing what is in the best interests of the child.
- In UNHCR HQ, an archive access request is received by a former refugee who would like to see the individual case files for himself and his family. Before allowing access to the file, the UNHCR archivist reviews the files and notices that there is a GBV case file for the person's wife. The archivist removes this file, as well as any other sensitive or otherwise confidential information and case files belonging to the wife, before sharing the case files that pertain to the husband.
  In this scenario, UNHCR ensures confidentiality in line with the rights of the data subject by providing only the information that pertained to the person requesting the data and not that belonging to his wife, and by ensuring that no other sensitive or otherwise confidential information was included in the file.

Annexes

Annex 1 : Data Sharing Decision Tree



Annex 2: Consent Script Sample(s)

Annex 3: Consent Form Sample(s)

Annex 4: Annex F Sample

Annex 4: Additional Resources

- IRC's "Obtaining Meaningful Informed Consent", 2018: https://www.rescue.org/resource/obtaining-meaningful-informed-consent
- GBV CM Guidelines
- CP CM Guidelines
- BIP Guidelines
- PIM

TECHNICAL NOTE ON SHARING PERSONAL PROTECTION DATA

Guidance for UNHCR and Partners

June 2020

UNHCR
P.O. Box 2500
1211 Geneva 2

www.unhcr.org