Inter-agency Guidance Note:

Data Protection and Information Sharing for Child Protection Case Management in Humanitarian Settings including Specific Considerations for Settings with Refugees

THE ALLIANCE
FOR CHILD PROTECTION
IN HUMANITARIAN ACTION

Data Protection and Information Sharing for Child Protection Case Management in Humanitarian Settings including Specific Considerations for Settings with Refugees

THE ALLIANCE
FOR CHILD PROTECTION
IN HUMANITARIAN ACTION

Acknowledgements:

This guidance note was researched and written by **Jessica Stuart-Clark** (UNHCR Division of International Protection, Child Protection Unit) and **Marta Passerini** (UNICEF Programme Group, Child Protection Team). Critical inputs and feedback were provided by key individuals including **Amanda Melville** (UNHCR Division of International Protection, Child Protection Unit) and **Brigid Kennedy-Pfister** (UNICEF Programme Group, Child Protection Team). Expert advice and technical review were provided by UNHCR's Legal Affairs Service and Global Data Service; UNICEF's Division of Data Analytics Planning and Monitoring, UNICEF's Legal Office and UNICEF's division of Information Communications Technology for Development.

Special appreciation goes to colleagues from the Child Protection Area of Responsibility and the members of the Case Management Task Force of the Alliance for Child Protection in Humanitarian Action. With particular thanks to International Rescue Committee, Plan International, Save the Children and Terre des Hommes Lausanne.

The development of this document was made possible by funding support from the **US Bureau of Population, Refugees, and Migration**.

Suggested citation: **The Alliance for Child Protection in Humanitarian Action, Inter-agency Guidance Note: Data Protection and Information Sharing for Child Protection Case Management in Humanitarian Settings (2023).**

Licence: This document is licensed under a Creative Commons Attribution-ShareAlike 4.0. It is attributed to the Alliance for Child Protection in Humanitarian Action (The Alliance).

For more information on the Alliance's work and joining the network, please visit www.alliancecpha.org or contact us directly: info@alliancecpha.org.

Photo Credit: @Pexels

Designed by: Formato Verde

Cover photo: Children are seen playing outside Goneko Childrens corner in Lilongwe Central Malawi @ Thoko Chikondi

---

Note: Text in italic and purple font and labelled "instructions", "note" and "example scenario" aim to support those who are developing and finalising the DPISP in-country in the process. This text provides clarification and guidance for specific sections and should be deleted from the document once the DPISP is finalised, prior to signature.

Contents

1. Overview

1.1. Background

With the aim of clarifying and streamlining how partners collect, store and share information generated through child protection case management, in 2020 the United Nations High Commissioner for Refugees (UNHCR) and the United Nations Children's Fund (UNICEF) proposed to lead the development of inter-agency guidance on the utilisation of information management systems). The process was to be conducted in consultation with partners who both deliver child protection case management and utilise information management systems in such settings.

In order to ensure that the Guidance Note would meet the needs of regional and field-based actors, including UNHCR, UNICEF, non-governmental organisations (international and national) and local authorities, it was agreed to conduct a number of country-based and field-focused consultations. In the fourth quarter of 2021, consultations were held with UNICEF, UNHCR and other key non-governmental child protection caase management actors in Lebanon, Jordan, Iraq, Ethiopia (Gambella), Kenya (Dadaab), Bangladesh, Sudan, and Somalia. These sessions were led by the Child Protection and Information Management System (CPIMS) Steering Committee Coordinator, the UNHCR Child Protection Officer for Child Protection and Gender Based Violence Information Management[1] and the CPIMS+ Steering Committee members, many of whom are also members of the Global Case Management Task Force (CMTF) of the Alliance for Child Protection in Humanitarian Action.

In summary, as reflected in the Outcomes Document from those consultations, participants clearly expressed the need for guidance on information management for case management (IM4CM) with a particular focus on data protection and information-sharing. This included clarity and guidance on the use of the Inter-agency Data Protection Impact Assessment (DPIA) and the Data Protection and Information Sharing Protocol (DPISP) for Inter-agency child protection case management in humanitarian settings.

Please see the Country Consultations Outcomes Document, which details the process and key findings informing the development of this Guidance Note.

1.2. Purpose of the Guidance Note

This Guidance Note provides actors delivering child protection case management with guidance on the key standards and principles, processes and tools available to apply good practices for data protection and information-sharing when implementing child protection case management in humanitarian settings. It includes specific considerations in relation to the UNHCR Best Interests Procedure (BIP) in settings with refugees.

The guidance aims to assist child protection actors to meet global standards for data protection and information-sharing and, in doing so, facilitate coordination processes in this area of work. Therefore, the aim is to make data protection and information-sharing more systematic and efficient, to reduce bottlenecks related to data protection and information-sharing and to ensure that children's data is appropriately collected, processed, stored, shared and analysed.

This will also facilitate the implementation of information management for case management for the delivery of timely and effective services to children in need of protection.

The Guidance Note does not mandate or require the use of any specific information management system (IMS) in any situation. However, it may refer to both CPIMS+ and proGres, where relevant, as two of the most common IMS utilised globally in humanitarian settings including settings with refugee populations. It also recognizes that partners may be using other digital or paper-based information management systems or tools.

[1] The CPIMS+ Steering Committee Coordinator and the UNCHR Child Protection Officer (CP and GBV IM4CM) are also currently coordinating several information management for case management activities under the global Case Management Task Force of the Alliance for Child Protection in Humanitarian Action, including revision of the current Data Protection Impact Assessment and Data Protection and Information-sharing Protocol templates and supporting tools.

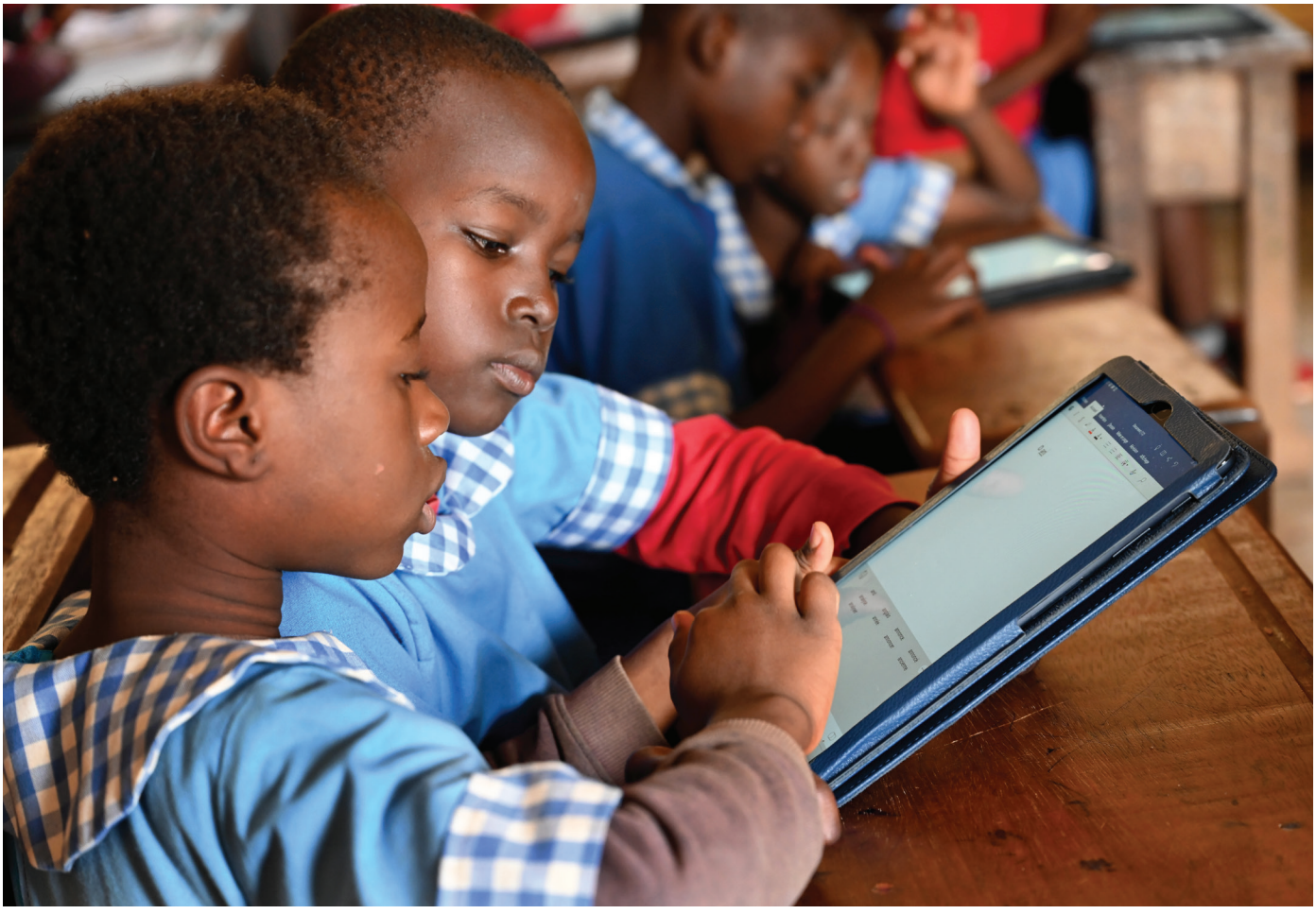
1.3. Intended audience

The Guidance Note is intended for all actors involved in child protection case management including the implementation of BIP[2] and related information management for case management (IM4CM) processes These actors include but are not limited to:

- Inter-agency Child Protection Area of Responsibility (AoR) / Child Protection Working Group (CPWG) Coordinators, as well as leads of sub-groups such as the CMTF, where it is in place.
- Data protection and other focal points in agencies that participate in inter-agency child protection case management and related information-sharing.
- Agency and/or inter-agency information or data management focal points who support the processing of data on child protection case management for reporting purposes.
- Agency focal points for child protection case management programming who participate in coordination forums.

NOTE

This Guidance Note complements and should be read together with existing Information management guidance in the Inter-agency Child Protection Case Management Guidelines and the UNHCR BIP guidelines.



Children learn with tablets and computers in the Public Melen School of Yaoundé, the capital of Cameroon. @ Frank Dejongh

[2] The Best Interests Procedure is a specific form of child protection case management for refugee and asylum-seeking children; please see the United Nations High Commissioner for Refugees (UNHCR), 2021 Best Interests Procedure Guidelines: Assessing and Determining the Best Interests of the Child, May 2021, available here.

2. Key guiding standards and principles

2.1 Key data protection and information-sharing standards in child protection guidance

Best practices for data protection and information-sharing are informed by and aligned with several key global resources including:

Standards 5 and 18 of the Minimum Standards for Child Protection in Humanitarian Action (CPMS) highlight the importance of information management in relation to case management:

STANDARD 5: INFORMATION MANAGEMENT (P. 89)

"Up-to-date information necessary for child protection action is collected, processed/analysed and shared according to international child protection principles and with full respect for confidentiality, data protection and information-sharing protocols."

STANDARD 18: CASE MANAGEMENT (P. 197)

"Children and families who face child protection concerns in humanitarian settings are identified and have their needs addressed through an individualised case management process, including direct one-on-one support and connect-ions to relevant service providers."

The Inter-agency Guidelines for Case Management and Child Protection highlight, on page 44, that after it is decided that case management is an appropriate approach to addressing child protection risks and vulnerabilities then it is imperative to set up a "safe and confidential system for collecting, storing and sharing information" as one of four essential elements of designing and implementing case management services.

The UNHCR Best Interests Procedure Guidelines highlight, in section 3.5 – Information Management for the Best Interests Procedure (p. 110), that "safe and ethical collection, storage, sharing and analysis of information on children during the best interest procedure can enhance the response for individual children as well as child protection programming more broadly".[3]

2.2. Child protection, child protection case management and data protection principles

Safe, secure and ethical collection, storage, sharing and analysis of information on children during the implementation of child protection case management, can enhance the response for individual children as well as child protection programming more broadly. The processing of children's information by any actor involved in child protection case management should always follow the key child protection and case management principles and international best practice for personal data protection. These include:

CHILD PROTECTION AND CASE MANAGEMENT PRINCIPLES:

Protection of the personal data of children and their families is also guided by core case management and child protection principles, also highlighted in the Inter-agency Guidelines for Case Management (p. 16). These core principles are like those that underpin all good practice in engaging with children. They reflect the SPHERE Handbook protection principles and the key principles and approaches outlined in the Child Protection Minimum Standards. For the purposes of this note it is important to outline the principles of do no harm, best interest of the child, confidentiality and seeking informed consent/assent, which not only need to be considered at all times but are also reflected in the data protection principles below.

[3] BIP, as a specific form of child protection case management for refugee children, involves processing personal data, including highly sensitive personal information, of refugee and asylum-seeking children and their caregivers. Section 3.5 makes direct reference to the UNHCR Policy on the Protection of Personal Data of Persons of Concern (Data Protection Policy/DPP), which binds UNHCR and UNHCR-funded partners involved in implementing BIP to the eight DPP principles: legitimate and fair processing; purpose specification; necessity and proportionality; accuracy; respect for the child's right as a data subject; confidentiality; security; accountability and supervision. Please see Page 112 of the UNHCR BIP Guidelines, to be read in conjunction with the UNHCR DPP.

PERSONAL DATA PROTECTION PRINCIPLES[4]:

The following core principles must be considered when collecting, processing and sharing Personal data (note the application of these is explained in detail within the DPISP template):

LEGITIMATE AND FAIR PROCESSING

Personal data may only be processed on a legitimate basis and in a fair and transparent manner, for a specific purpose. Each participant will process personal data on an appropriate legitimate basis in accordance with its regulatory framework, including but not limited to consent, performance of a public interest task, or the best or vital interests of the particular child.

Consent for the processing of a child's personal data, when applicable, should generally be sought from the child's parent or guardian, with the child being sufficiently informed about the processing according to their age and maturity.

Regardless of the applicable legitimate basis, data subjects must be informed, in an easily understandable manner: what type of personal data needs to be collected and for what purpose; with whom the data may be shared and with whom it will not be shared; whether there will be any detriment if they object to the processing; who will have access to their data and whom they should contact if they want to exercise their data subject rights and/or if they have concerns with respect to their data. The legitimate basis and the information provided should be recorded in an appropriate manner.

PURPOSE SPECIFICATION

Personal data will only be processed by participants for specific and legitimate purposes. Within the scope of this protocol, this means purposes associated with ensuring that children and their families are able to receive child protection case management services and enabling the provision of holistic, multi-sector services and durable solutions, as needed, based on the best interests of the child. Personal data should not be processed in any way that is incompatible with those purposes originally specified.

DATA MINIMISATION - NECESSITY AND PROPORTIONALITY

The processing of personal data will be adequate, relevant and proportionate to the original specified purpose(s).

RESPECT FOR THE DATA SUBJECT'S RIGHTS

Children and families have the right to know, access, correct and delete their personal data and to object to its processing during all stages of such processing.

CONFIDENTIALITY AND SECURITY

In order to ensure the confidentiality, availability and integrity of personal data (and sensitive non-personal data), each participant (and service provider) shall consult with an information security specialist or designated information security focal point in their organisation and put in place physical, technical and organisational information security measures (for any personal data, whether at rest, in use or in transit) appropriate to the risks incurred by the processing and in line with international best practice.

ACCURACY

Personal data should be kept accurate and up to date.

RETENTION LIMITATION

Personal data shall be deleted from any and all systems once it is no longer necessary for the purposes for which it is being processed or corollary purposes. There may be specific data-retention requirements for refugees, asylum-seekers, children associated with armed groups or armed forces, children affected by armed conflict, as well as for monitoring and reporting mechanisms for grave violations.

A girl teaches her younger sister and brother how to use a tablet in their home in the Za'atari Refugee Camp in Jordan. @ Mary Gelman / VII Photo

[4] As reflected in the United Nations Personal Data Protection and Privacy Principles, the international treaty known as Convention 108, the European General Data Protection Regulation and many other regional principles and standards, as listed here (page 18, Box 3, see also Footnote 72).

3. Principles in practice: data protection and information sharing

Information-sharing is essential for effective service provision and coordination of case management, especially where several agencies or individuals are involved in different aspects of case management service provision including BIP. Child protection case management service providers and related stakeholders in child protection case management and BIP must ensure that the above key principles are adhered to and that inter-agency standards are both met and put into practice. All actors, including relevant United Nations agencies, non-governmental organisations (both national and international) and government counterparts working on child protection case management should clearly define the specific purposes for which they require children's personal or anonymized data to be collected, used, shared or otherwise processed in line relevant principles, standards, policy and frameworks.

Two key inter-agency tools, which are part of what is known as information management for case management (IM4CM)[5], have been developed to operationalize existing guidance on child protection information management under the technical leadership of the global CMTF of the Alliance for Child Protection in Humanitarian Action. These reflect the above stated standards and principles and relevant child protection guidance. They are:

Child protection case management global standard inter-agency template for a Data Protection Impact Assessment (DPIA):

The purpose of a DPIA is to identify, evaluate and make recommendations about how to address the risks to children arising from case management service providers managing sensitive data at agency and inter-agency levels, in line with relevant data protection frameworks. Generally, it is best practice to conduct a rapid or comprehensive data protection risk assessment prior to commencing information collection, sharing, storage and analysis.[6] Please see section 3.3. for more detail.

Child protection case management global standard inter-agency template for the Data Protection and Information Sharing Protocol (DPISP):

The purpose of a DPISP is to establish appropriate practices for safe, secure and ethical information-sharing in the context of inter-agency child protection case management and related activities. It outlines general provisions and guiding principles that inform the approach that should be taken to data protection and information-sharing within international and national legal frameworks, inter-agency guidance and policies. Please see section 3.3. for more detail.

NOTE

Both templates have guidance embedded within them to support actors in developing, adapting and finalising the tools. The templates can be found here.

The DPIA and DPISP are informed by the development of context-specific case management procedures and related forms; this will inform the selection of specific data points to be collected and shared in a given setting and situation.

These templates should be used to support and formalise inter-agency data protection and information-sharing standards and practices to be applied by organisations and entities delivering child protection case management in line with local/national legislation. These tools are applicable to all settings, irrespective of the caseload, and should be signed by all organisations adhering to agreed specific case management procedures, whether at national or local level.

[5] Information management for case management is inclusive of DPIA and DPISP as well as the standard operational procedures, forms and information management systems that collectively support data management.

[6] UNHCR does not require a DPIA in all situations involving refugees. In line with the UNHCR Data Protection Policy (DPP) it is only required where data transfers might negatively impact upon the protection of personal data and when data transfers are large, repeated or structural. However, UNHCR recognizes that conducting a DPIA is generally best practice.

NOTE

A note on applying national frameworks:

The DPISP content outlines the rules for data protection and information-sharing where they are needed for child protection case management in humanitarian situations. Its development requires national regulations to be analysed and adjustments to be made accordingly; however, as a baseline, the principles outlined in this Guidance and in the DPISP content reflect global standards and practices of child protection and data protection.

NOTE

It is important to note that the development of a DPIA and a DPISP is not specific to the roll-out of any specific information management system.

DPIAs and DPISPs are information management for case management tools that should be used regardless of the system or tool used to collect, store, share and analyse child protection case management data – including paper-based or "offline" systems or tools.

This means there should be one common inter-agency DPIA and DPISP for child protection case management even *if multiple IMS are in use.*

3.1. Leadership in the roll-out of DPIA and DPISP tools

The roll-out of DPIA and development of DPISP is usually led by the child protection coordination body in the country. This could be the UNHCR- or government-led CPWG, the CP AoR coordinator or the leads of an established case management task force in a country/location. A specific agency with expertise can also play this role in agreement with the coordination mechanism. If national authorities are involved in the case management work or coordination, it is important to involve them from the outset and ensure they are aware of/part of the development of related data protection and information sharing procedures.

The coordination mechanisms should also roll-out/disseminate key related IM4CM guidance/tools to staff participating in case management activities. Agencies should be accountable for ensuring that their staff are aware of and participating in these processes and that they are equipped with the appropriate tools to adhere to the standards set out.

3.2. Roll-out timeframes specific to data protection and information-sharing

It is recommended that the following timeframes be adhered to when rolling out child protection case management in any humanitarian setting (including settings involving refugees):

Data protection impact assessment (DPIA):

The DPIA should be conducted as soon as the need and scope of humanitarian case management is confirmed[7] within a maximum of three months in order to inform contextualization of a DPISP and to support individual agencies and entities in assessing and improving internal data protection measures specific to child protection case management.

While it is generally best practice to conduct a DPIA prior to finalising the DPISP process, in order to commence inter-agency information-sharing for the purpose of child protection case management service provision and coordination, it is recognized that in the case of a rapid onset crisis, this sequencing may not be possible. If it is not possible to conduct a DPIA in the onset of an emergency, it is recommended that a DPIA be conducted as soon as possible and that any required revision to DPISP be prioritised.

In situations in which a DPIA cannot be conducted before the DPISP it is recommended that each agency undertake the Information Security Checklist Annex in the DPISP to ensure adherence to minimum data protection standards.

Data protection and information-sharing protocol (DPISP):

Contextualization of DPISP to be initiated as soon as possible, for signature within a maximum timeframe of three months, with the aim of finalising it in the shortest time possible.

The current template which has been endorsed by the Alliance of Child Protection in Humanitarian Action sets out the required safeguards needed to ensure data protection and information-sharing and aims to reduce timeframes in the contextualization.

[7] This means when agencies begin to deliver case management services, this does not require that SOPs and forms have gone through final endorsement, but once child protection case management services are being delivered it is key that data protection and information sharing standards are considered and put into practice.

NOTE

In contexts where humanitarian child protection case management activities are underway and a DPIA and/or DPISP has not been conducted/developed then it is advisable this be done as soon as possible; or in situations where there is a change in the programming, this may also require a revision on the DPISP (e.g. in cases where work was focused on a specific case load, and this is now expanded to other children then additional elements of the DPISP may need to be considered).

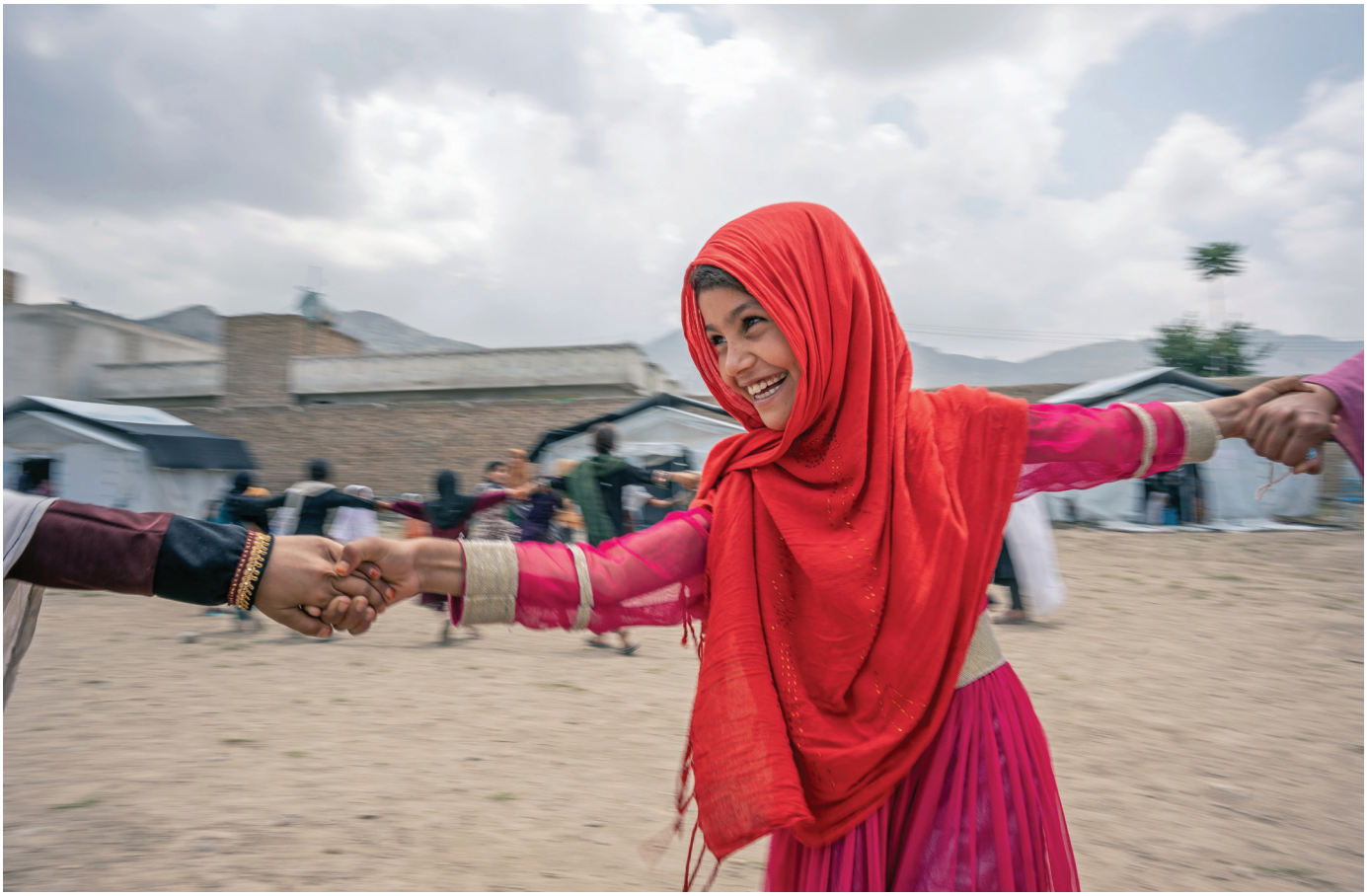
What happens before the DPISP is signed?

During the interim period, while IA DPISP is being finalised, child protection case management data-sharing shall be limited only to individual cases and for the purpose of obtaining services in the best interests of the child. Such information-sharing shall respect the data protection and case management principles outlined in this guidance and should be undertaken in line with organisations' data protection policies. The principles of data minimization (only sharing what is necessary for the provision of that specific service), confidentiality and information security must be respected. In addition, the decision to share data must be made with the best interests of the child as a primary consideration or following the consent/assent of the child (and/or legal guardian, as applicable).

Additionally, even in the absence of a DPISP data subjects must be informed about the people or organisations with whom their data will be shared, for what purposes, how the data will be processed and for how long, as well as procedures relating to their data subject rights (requests for access, correction, or deletion). Recipients of personal data must not share the personal data onwards with any third party without the express prior consent of the data subject and only sharing information without consent in exceptional circumstances with strict adherence to procedures for breaking confidentiality in the best interests of the child. Recipients must inform the data subject or any entity that shared that data if a data breach occurs, for example if a case worker loses a case file, or if someone who should not access the information management system.

NOTE

Sharing personal data without a DPISP under the circumstances described above is considered exceptional, typically occurring in the immediate onset of a humanitarian crisis and should not continue for longer than three months without a signed DPISP in place.



Girls play during breaktime at a UNICEF-supported community-based education centre in Hijrat Mina in Bagrami District, Kabul Province, Afghanistan. @ Mark Naftalin

4. Specific considerations for refugee and asylum seeking children

4.1. The BIP guidelines and the UNHCR role in child protection case management

For asylum-seeking and refugee children, UNHCR and its partners implement best interests procedures (BIP) that are aligned with inter-agency child protection case management steps, with additional procedural safeguards for the best interests determination (BID) process, which is a component of BIP. The latter is embedded within, and linked to, refugee protection case management. Refugee protection case management encompasses the full range of case management services for asylum-seekers and refugees (as well as stateless persons and returnees), including but not limited to: registration, identity management, refugee status determination, durable solutions (e.g. resettlement, voluntary repatriation, local integration and complementary pathways for admission to third countries), assistance, legal and physical protection, gender-based violence (GBV case management and BIP.

BIP is a specific type of child protection case management for refugee and asylum-seeking children, in addition to the regular provisions of child protection case management outlined above and within inter-agency case management guidelines. BIP includes a child protection case management process for assessing or determining, managing and implementing decisions that are in the best interests of individual refugee and asylum-seeking children: BID. This is implemented when specific important decisions are being made about a refugee or asylum-seeking child's life and future that may be so significant that additional safeguards are required for decision-making.

Given its international legal mandate for refugee protection, UNHCR has specific accountabilities and obligations for implementing BIP and refugee protection. It is therefore often necessary to share information with UNHCR and receive information from UNHCR in order to effectively deliver services to children and their families. BIP is embedded within, and linked to, refugee protection case management; therefore, information may be required for a child benefiting from child protection case management/BIP in order for them to have access to and benefit from broader refugee protection services, including refugee protection case management (e.g., identity management, documentation, durable solutions and other assistance). Information-sharing with UNHCR, as with any child protection case management actor, should have a legitimate basis and a specific purpose in line with the best interests of the child and the application of data protection principles.

NOTE

See the 2021 UNHCR Best Interests Procedure Guidelines for Assessing and Determining the Best Interests of the Child, Section 3.5. Information Management for Best Interests Procedure

4.2. Reciprocal information-sharing with UNHCR

To meet its obligations to children in terms of decision-making and service provision that is in children's best interests, UNHCR will require specific personal data on children from implementing partners (those funded by UNHCR) for purposes such as providing protection services, assistance and BIP. It is necessary for UNHCR to maintain the accuracy of its data sets to deliver timely and appropriate services. Similarly, partners implementing BIP will generally require specific information from UNHCR to respond to the needs of children at risk, related to child protection case management as well as broader refugee protection case management, identity management and access to basic and specialised assistance.

NOTE

Please see section 5 of the DPISP template for provisions specific to sharing data on refugee and asylum-seeking children with UNHCR.

The IA DPISP template is the global standard and preferred template governing information-sharing in inter-agency child protection case management and BIP between two or more entities. The DPISP template is also recommended for use as a template for any bilateral agreement between two parties to share case management information, if one is required and if the parties do not have another bilateral agreement such as a data-sharing agreement or a partnership agreement with a data-sharing agreement annex, such as the UNHCR data sharing agreement annex (formerly Annex C[8]) in the case of UNHCR Partners. The DPISP does not preclude or supersede other bilateral data-sharing agreements, but rather complements them and formalises information-sharing between two or more parties implementing inter-agency child protection case management and BIP.

Wherever UNHCR-funded partners (implementing partners) and humanitarian partners providing services to refugees and asylum seekers, but who are not funded by UNHCR (operational partners) are engaged in the delivery of BIP and child protection case management for asylum-seeking and refugee children, data and information-sharing should occur in line with the data protection principles outlined above. The regular and systematic sharing of information, with a legitimate basis and specific purpose, ensures expedient case referral or transfer to UNHCR for service provision where relevant and applicable. Non-personal data-sharing, again within the application of data protection and case management principles, should be ensured for monitoring, reporting, advocacy and targeting interventions. It is important also to note that for UNHCR-funded partners (implementing partners) the data sharing agreement attached to the partnership agreement defines the data to be shared. In some cases, where there is a need for specific data-sharing arrangements between UNHCR and non-funded partners (operational partners), a bilateral data-sharing agreement can be developed. This is often used when, for example, a non-funded partner (operational partner) is using proGres, the UNHCR institutional tool for refugee protection case management or where there are particular arrangements needed for data-sharing between the organisations.

While UNHCR often fulfils multiple roles in humanitarian settings under its mandate for international protection, including coordination and funding its partners for example, it is also a service provider. In the context of child protection case management and BIP, UNHCR provides key services for children at heightened risk, within BIP and broader refugee protection case management, including registration and identity management as well as durable solutions and assistance. UNHCR should, in all its roles in relation to refugees and asylum-seekers, whether as a service provider, coordinator or donor, lead and/or participate in inter-agency DPISP processes even when information management systems other than proGres are in place; this is key to ensuring appropriate data collection and information-sharing for refugee children. An inter-agency DPISP should be developed with all relevant child protection case management actors regardless of the information management system in use and the partnership arrangements in place.

4.3 Use of the ProGres Child Protection Module and other information management systems

For refugee children, UNHCR utilises its institutional identity and information management system for refugee protection case management – ProGres. This system is also used for broader protection refugee case management, including assistance and durable solutions. The proGres Child Protection module contains tools for information management for BIP and child protection case management for asylum-seeking and refugee children.

Where proGres is in use, UNHCR should keep essential information relating to BIP up to date in proGres, particularly where children are receiving BIP, in order to ensure that children and their families have access to and can benefit from broader refugee protection case management services.

ProGres is used globally by UNHCR staff as their institutional tool for refugee protection case management, including BIP. While proGres is mandatory for UNHCR staff, this is not the case for UNHCR-funded or non-funded partners, for whom UNHCR recommends the use of Primero where available (see UNHCR position below). It is advisable in settings involving refugees that CPIMS+ be rolled out in coordination with UNHCR and include the development of inter-agency DPISP to facilitate the timely and bidirectional exchange of information for the purposes of service provision between CPIMS+ users and UNHCR.

NOTE

Please see the UNHCR Position Brief on Use of the pro-Gres CP and GBV Modules and of Primero CPIMS+ and GBVIMS+ by UNHCR Staff and Partners

[8] In 2023,UNHCR is undergoing a transition from former Partnership Agreement templates and tools, including the Annex C to a forthcoming revised process and related tools.

Annexes

Annex 1: Training, tools & resources

GUIDELINES

- Inter-agency Guidelines for Case Management & Child Protection, from page 44 in the Information Management section
- 2021 UNHCR Best Interests Procedure Guidelines: Assessing and Determining the Best Interests of the Child, Section 3.5. Information management for best interests procedure

TRAINING

- Inter-agency Child Protection Case Management Training Package – IM4CM references in Level 1 Modules 2,3,6 and 11 and Level 2 module 5[9] . A Level 3 IM4CM module is forthcoming.
- UNHCR Data Protection Learning Module
- UNHCR Best Interests Procedure Online Self-paced Micro-learning Modules

IM4CM TOOLS

- Supporting tools for the development of the DPISP and DPIA for different audiences (e.g., Inter-agency forums, local actors, government counterparts) (forthcoming)
- Data Protection Impact Assessment Toolkit (forthcoming)
- Data Protection and Information-Sharing Protocol Template

OTHER RELEVANT TOOLS

- UNHCR Best Interests Procedure Toolbox
- UNHCR Best Interests Procedure SOPs Toolkit

[9] These in specific include: Level 1 – Module 2 – Session 5 How to collect and store child's information? (slide 41 – 52); Level 1 – Module 3 – Session 2 How should caseworkers prepare to meet with children? (slide 16); Level 1 – Module 6 – Session 3 How do I ask for informed assent/consent? (slide 19 – 33); Level 1 – Module 11 – Session 3 How do I close a child's case? (slide 20 – 22); and Level 2 – Module 5 – Session 3 on protection analysis and Session 5 on managing information flows and prioritizing tasks could be helpful.

Annex 2: FAQ: Frequently Asked Questions and Answers

Are DPISPs only for CPIMS+ users?

No, a DPISP should be signed by all participating agencies involved in child protection case management in the setting or situation. However, 2 agencies could also use the template bilaterally if there were a need to do so. However when multiple agencies adhere to a case management procedure through an inter-agency approach to the DPISP is advisable.

Can I share information for the purpose of service provision before the DPISP is finalised?

Generally, in the interest of the highest protection of children's data and their wellbeing, a data sharing agreement needs to be signed before the exchange of data. In exceptional circumstances, information sharing is permitted on a short-term basis (not more than 3 months) prior to the DPISP being signed for individual children where information sharing is required to provide protection and assistance for individual children at heightened risk for the purpose of service provision, based on the best interests of the child, and as long as this is in line with data protection policies and case management standards.

Who should ensure the development of the DPIA and DPISP (including signature of DPISPs) in a humanitarian response?

The inter-agency coordination body for child protection such as the Child Protection Working Group in refugee settings and the Child Protection AoR in all other humanitarian situations; a locally established case management task force, including national/local designated government counterparts and all relevant actors and agencies involved in child protection case management programming.

Who needs to be involved in the drafting of the DPIA and DPISP?

A designated focal point from each organisation should participate in the roll-out of the DPIA and DPISP. The focal point should have relevant technical skills or expertise in child protection case management and experience in data protection and information management for case management.

Who needs to sign the DPIA and DPSIP?

A designated representative from each agency participating in the development and endorsement who has the authority to bind the agency to the DPIA findings and the recommendations and protocols

If the government is involved or has oversight of case management work, do we still need a DPISP?

Yes, all actors involved in child protection case management and BIP should be signatories to a DPISP, including national or local authorities wherever and whenever applicable and relevant.

What is the relationship between a DPIA and a DPISP?

A DPIA informs each agency about data protection measures that they need to take in order to be able to comply with relevant data protection frameworks, and the DPISP, and ensure the protection of children's data. It also informs role-players on context-specific data protection considerations that may need to be reflected in a DPISP.

Do I always need to sign a DPIA?

Generally, an inter-agency DPIA is recommended in advance of developing a DPISP, in order to identify and mitigate data protection risks in inter-agency information management and case management. However, in the case of a rapid onset crisis it may not be possible to conduct a DPIA prior to the issue of a DPISP. In these circumstances, it is recommended that the standard approved DPISP template be contextualised and signed. Within three months of initiation/expansion of case management programming, a DPIA should be conducted, which can inform any necessary DPISP revision.

How often do I need to revise DPIA and DPISP?

This should be determined jointly by the participating agencies, but normally it is recommended that revision or adaptation should only be required when there is a significant change in operational context. New partners should sign a DPISP if they start providing child protection case management services.

What happens if I do not sign a DPISP?

If an actor or agency refuses to sign a DPISP and does not have a multilateral or bilateral data protection and information-sharing agreement otherwise in place you will not ethically or legally be able to reciprocally share information with them on children receiving child protection case management services, nor will other case management partners ethically or legally be able to reciprocally share information with you. You will not have access to data that is collected, stored, shared, and analysed by the DPISP signatories.

What if there is no inter-agency case management procedure in place?

If there is no Inter-Agency process in place and only one agency is doing case management, a DPIA can help the agency to understand what internal data protection measures might be needed and to assess whether further steps need to be taken to meet said minimum standards. Equally, it is recommended to have an adapted internal DPISP, particularly for referrals, to support case workers and other staff in respecting the key principles of information-sharing.

What is the geographic scope?

The DPIA and DPISP can be developed for a country or a specific geographic location/group, e.g., where an emergency may be limited to a specific area or a specific group of people. These should be aligned with the scope of the case management procedures in a specific location.

What if the coordination is led by UNHCR and then the Cluster system is rolled out due to a situation in the country, or vice versa?

The IM4CM processes and documents are relevant in all humanitarian settings independently from who is leading coordination efforts. The key documents and tools which have been developed should be considered and adapted to new and emerging needs and population groups. Refugee children have the same rights to privacy and confidentiality and to have their personal data protected from disclosure as all other children.

What is Primero?

Primero™ is a software platform that helps case workers to manage the protection-related data necessary to facilitate case management, incident monitoring and family tracing and reunification. It can also serve as a secure repository for individual-level data when needed, such as at times of large-scale population displacement. Primero is supported and maintained by UNICEF, but it is an inter-agency tool managed, governed and used by a broad group of organisations. Aligned with the United Nations Secretary General's Roadmap for Digital Cooperation, Primero is a certified digital public good designed to be adopted by organisations, government(s) or a network of partners to support the delivery of child protection services both in emergencies and in the long term (post-emergency). Primero contains dedicated information management systems for child protection and gender-based violence case management, respectively CPIMS+ and GBVIMS+.

Who uses CPIMS+?

Anyone can use CPIMS+: national authorities, United Nations agencies, non-governmental organisations (both national and international) and even private businesses; however, for the purposes of case management in humanitarian responses it is most likely UN, NGOs, and Government as per local procedures set out for case management.

What if I do case management and do not use CPIMS+ or proGres?

You can use any IM system or tool that ensures safe, ethical, and secure collection, storage, sharing and analysis – that ensures data is protected – this includes paper-based or other systems.

Do I need to use CPIMS+ or proGres to do case management

No, case management is a process of supporting children and families. This process can be supported by any appropriate IM system that also allows for data to be appropriately protected. The CPIMS+ and proGres are recommended as they have been tested and are secure IM systems. The CPIMS+ is also the recognized tool of the global CMTF.

What is proGres?

"ProGres in Partnership" or proGres is the UNHCR corporate, centralised , cloud-based case management software application. It is a digital information management tool to support UNHCR refugee identity management and refugee protection case management: refugee registration and identity management; documenting assistance like non-food items or cash-based assistance, for example, and not least – protection case management and durable solutions.

What are the proGres CP and GBV Modules?

Within proGres, the Child Protection and Gender-based Violence Modules – known as the CP and GBV Modules respectively – are powerful tools for case management and information management for case management. With rigorous security models, strict user access roles and rights, the modules continue to be enhanced for UNHCR operations to go digital, better manage the caseload and improve the quality of case management through better monitoring, supervision and support.

What is the UNHCR position on the use of proGres by partners?

UNHCR does not mandate the use of proGres by partners. However, it is available for use, free of charge, with sustained centralised technical support and maintenance. Where partners are using another digital information management system, regular and systematic data and information-sharing protocols should be in place to ensure safe, expedient case referral or transfer to UNHCR for service provision, where relevant and applicable, as well as non-personal data-sharing for monitoring, reporting, advocacy and targeting interventions. proGres must be used by UNHCR staff as the institutional tool.

Do implementing partners have to use proGres?

No, proGres is available for use by implementing partners, free of charge, with sustained centralised technical support and maintenance. UNHCR does not mandate the use of proGres and will never force an implementing partner to use the proGres CP and GBV modules; in fact, UNHCR promotes the use of CPIMS+ and GBVIMS+ for partners and can, in exceptional situations where Primero tools will not become available, make proGres available to partners.

Can the Government use proGres?

Yes. In line with UNHCR data protection policy and relevant data protection frameworks, Government counterparts can use proGres for specific purposes. Government counterparts most commonly use the refugee registration, identity management and refugee status determination modules. In rare circumstances, State social workers providing services to refugee and asylum-seeking children can be granted access. Access to any module, entities and individual fields can be restricted for any user, including government counterparts and is based strictly on the role of the user in case management to determine their level of access to data and information.

Can we limit what partners/government can see on proGres?

Yes. Access to any module, entities and individual fields can be restricted for any user, including partners and government counterparts. Please contact PRIMES User Support on primes_support@unhcr.org for guidance and assistance on setting up user permissions for partners.

Annex 3: Glossary of Terms

Anonymous data means information that cannot be associated with an identifiable individual by any means reasonably likely to be used, based on the data alone or in combination with other data. Data is said to have been anonymized when it has undergone the process of removing or modifying all personal identifiers and codes in such a way that individual data subjects cannot be identified by any means reasonably likely to be used, based on the data alone or in combination with other data. A person may sometimes be identifiable even if they have not been named in the information, in which case the information is no longer "anonymous" but constitutes personal data.

Assent means the expressed willingness of a person to participate in services, where that person has been assessed by a child protection agency as not having the capacity to give consent to participation, but as being able to learn about the services, ask questions and to agree or object to the collection and sharing of their personal data for the purposes of provision of the services.

Best interest of the child means a child's physical and emotional safety (their well-being) as well as their right to positive development. In line with Article 3 of the United Nations Convention on the Rights of the Child (UNCRC), the best interests of the child should provide the basis for all decisions, actions, and interactions between the service providers with children and their families.

Case referral (as part of the case management processes) is the process of formally requesting services for a child or their family from another agency (e.g., cash assistance, health care, etc.) through an established procedure such as an inter-agency referral pathway and/or standard referral form(s). The child protection case worker maintains overall responsibility and accountability for the child's case for which they are making referrals, and therefore responsibility for ensuring that referrals are made to quality service providers in a safe, ethical, and secure manner.

Case transfer is the process whereby cases are not closed but transferred from one Participant to another. Often this happens when a child moves to another known location, but still needs case management to ensure continuity of care and protection. Case transfers also take place where the original caseworker or participant is no longer best placed to lead, manage, and coordinate a child's case, or has concluded their employment in this role. Furthermore, case transfers can occur when an agency concludes operations or service provision in a country or location and a new or other agency takes on their caseload to sustain service provision.

Child protection case management is an approach for addressing the needs of an individual child who is at risk of harm or has been harmed. The child and their family are supported by a caseworker in a systematic and timely manner through direct support and referrals. Case management provides individualised, coordinated, holistic, multisectoral support for complex and often connected child protection concerns. Case management systems are an essential part of the child protection response.

Consent means any freely given, specific and informed indication of an agreement by the data subject to the processing of their personal data, which may be given either as a written or oral statement or by a clear affirmative action[2]. This applies to both the collection and the sharing of personal data, which constitutes processing of personal data (see processing below).

Data subject refers to a living individual whose personal data is being processed.

Data breach means a breach of data security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data or sensitive non-personal data.

Information refers to organised data and/or an interpretation/analysis of data points. The terms "data" and "information" are frequently used interchangeably but differ in substance. Data can be interpreted as individual facts, while information is a combination of facts and meaning.

Participant means each agency or authority that signs this protocol, whether on the date that this protocol comes into effect or subsequently. A list of participants and their official signatories is maintained up to date by the coordinators as set out in this DPISP.

Personal data means any information relating to an identified or identifiable individual (data subject, see above).

An identifiable individual is one who can be identified, directly or indirectly, including by reference to (a) an identifier such as a name, identification number, audio-visual materials, location data or online identifier, (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual, or (c) assessments of their status and/or specific needs, such as in the context of assistance programmes.

> **Note:** a single data source may not make an individual identifiable, however, in combination and with the application of new technologies, data sources may make the individual identifiable. Therefore, each data source should be assessed for actual or potential personal data content. Non-personal data can also be sensitive (see sensitive non-personal data below), and information-sharing should be limited accordingly.

Processing means any operation, or set of operations, whether automated or not, that is performed on Personal Data, including but not limited to the collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, transfer, dissemination or otherwise making available; correction, restriction, or destruction (partial or full).

Sensitive non-personal data means data regarding a vulnerable group that, if disclosed, could lead to risks for that group or for individuals within that group. This might include data and information collected, used, stored, or shared by humanitarian and human rights organisations relating to protection risks, rights violations or the protection situation of specific groups, or might relate to the location of a specific individual and/or group. Examples include anonymous 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 to a group. This type of data may be in aggregate or anonymous form.

Sensitive personal data means personal data that affects the data subject's most intimate private life or relates to their immutable (unchangeable) characteristics and which, if misused or subject to a data breach, could result in discrimination against them, or serious harm or a breach of their fundamental rights. Examples might for example include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union/staff association membership, genetic data and biometric data capable of uniquely identifying a natural person, data concerning health or data concerning an individual's sex life or sexual orientation.

THE ALLIANCE
FOR CHILD PROTECTION
IN HUMANITARIAN ACTION