Mozambique, 2024 © UNHCR/Hélène Caux

Students walk home from school in Mocimboa da Praia, where stability and services are gradually returning after years of conflict and displacement.

Protection Field Coordination Toolkit

Chapter 10: Data Responsibility and Safe Information Management

Global Protection Cluster

Chapter 10: Data Responsibility and Safe Information Management

Overview

This Chapter contains:

- Core concepts and principles of Information Management (IM) and data safeguarding.
- Data responsibility in humanitarian action.
- Role of Protection Clusters in data management and sharing.
- Tools and resources for safe and effective data handling.

Skip ahead to:

10.1 Core Concepts and Principles 1

Information Management and Data Safeguarding 1

Data Responsibility in Humanitarian Action 2

10.2 Spheres of Protection Data 2

10.3 Role of the Protection Clusters and Data Collection 3

Data Sharing Protocols 4

Protection Clusters and Data Responsibility 5

10.4 Key Resources and Tools 5

NOTE: This chapter covers the specific of protection data and data safeguarding. This chapter recognises the importance of data protection, and the challenges of data protection and management in increasingly digital spaces.

The GPC has extensive resources that are available for Protection Cluster IM and analysis, which can be found at the GPC Information Management and Analysis Toolbox

10.1 Core Concepts and Principles

Information Management and Data Safeguarding

Information Management (IM) is a critical function of cluster coordination that enhances coordination and enables relevant stakeholders to work with shared information, promoting informed decision-making.

The proper collection and management of data facilitates humanitarian responses for protection and supports other sectoral humanitarian response as well as work towards durable solutions and recovery and disaster preparedness efforts. IM ensures that cluster decisions are based on timely and evidence-driven insights.

Safe, responsible and purposeful sharing of data, information, analysis and knowledge, enables stronger, evidence-informed, comprehensive protection outcomes and humanitarian response.

Protection Clusters engage with data in many ways, including:

- Direct collection and sharing of data

- Facilitating data exchange between partners
- Exchanging data and analysis with other sectors/clusters
- Participating in intersectoral and interagency data collection exercises
- Developing data analysis, dashboards, reports and infographics

See: Protection Information in Practice for guidance and examples of how Protection Clusters and partners have used the PIM Conceptual Framework to create structure and embed principles into daily protection information management activities for quality protection outcomes.

Data Responsibility in Humanitarian Action

Data collection and sharing is a critical component of Protection Cluster coordination, which comes with responsibilities to safeguard data and use information well.

Data Responsibility in Humanitarian Action

Data responsibility in humanitarian action is the safe, ethical and effective management of personal and non-personal data for operational response. It is a critical issue for the humanitarian system to address and the stakes are high.

While each organization is responsible for its own data, humanitarians need to work together to uphold a high standard for data responsibility in different operating environments. The IASC Operational Guidance on Data Responsibility in Humanitarian Action offers a framework for collective action in this area.

Data Responsibility Working Group (DRWG)

Data is a clear prerequisite for improved humanitarian response. Yet safe and responsible sharing is challenging. In the present time, we have more ways to collect, store, share, transmit, analyze and publish data than ever before.

The absence of a common understanding of how to use data and how to safely share data can result in several adverse outcomes, including less or no sharing, irresponsible sharing, or confusion among partners about what can or should be shared. Each of these can result in a loss of the knowledge and evidence needed for decision-making and response, both internally and with operational stakeholders and partners.

Protection information management is a way of collectively facilitating, and advancing the safe, responsible, and purposeful sharing of data, information and analysis for stronger humanitarian response and protection outcomes.

10.2 Spheres of Protection Data

Protection partners and Protection Clusters collect many different types of data and contribute to data collection exercises conducted by other actors. Not all data is inherently sensitive, but there is an onus on clusters to assess the protection impacts on in processing data and for identifying remedial actions as necessary to avoid or minimize risks and negative impacts.

Types of data that are collected by protection partners	
Facts	Such as numbers, measurements or observations. Data can be qualitative and quantitative and may include personal data.

Personal data	Personally identifiable information (PII) is data relating to an identified individual or to a person that can be identified from that data, from other information, or by means reasonably likely to be used related to that data. This may include an identifier such as a name or audio-visual materials, an identification number, location data or an online identifier. Personal data includes bio data and biometric data such as a photograph, fingerprint, facial or iris image.
Sensitive protection data and information	Protection data or information whose unauthorized access or disclosure, is likely to cause harm, such as discrimination or repression, to any person including the source of the information or other identifiable persons or groups, or which may have a negative impact on an organisation's capacity to carry out its activities or on how it is perceived.
Protection data and information	Data and information collected, used, stored or shared by humanitarian and human rights organisations pertaining to protection risks, rights violations and the situation of specific individuals/groups. This may include personal data, community identifiable information, or data and information on a specific event or to a general situation or a context.

APPLICATION OF STANDARDS AND PERSONAL DATA PROTECTION PRINCIPLES

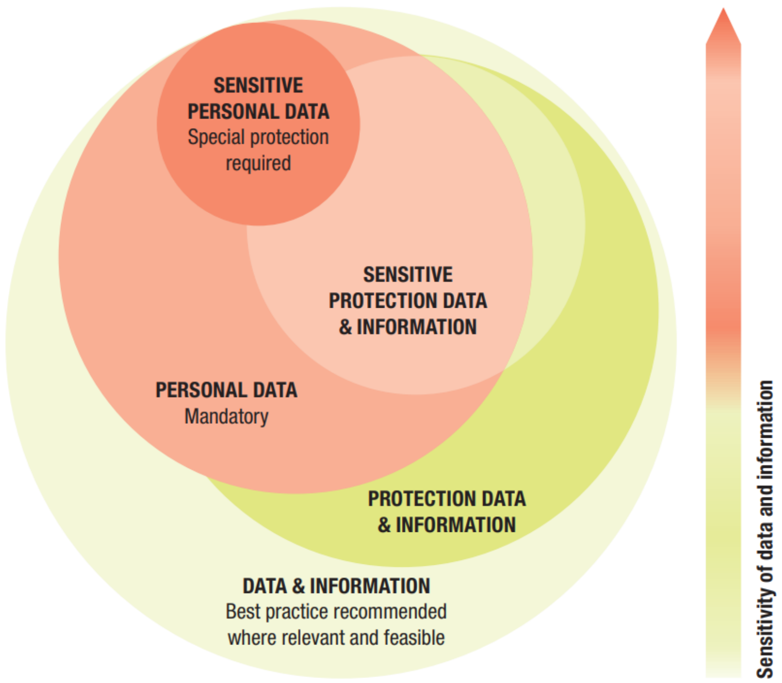
SENSITIVE PERSONAL DATA
Special protection required
SENSITIVE PROTECTION DATA & INFORMATION
PERSONAL DATA
Mandatory
PROTECTION DATA & INFORMATION
DATA & INFORMATION
Best practice recommended where relevant and feasible
Sensitivity of data and information

Image Source: Professional Standards for Protection Work – ICRC Handbook *(pg. 106)*

10.3 Role of the Protection Clusters and Data Collection

Protection Clusters may be involved in collecting data that is facts, sensitive protection data and information, and protection data and information, but Protection Clusters do not collect personal data.

Protection Cluster partners need to directly exchange information with other protection partners, and humanitarian actors. Referrals require a direct exchange of information about specific individuals and families. Protection Clusters have an important role in creating an enabling environment for this information sharing – through protocols and SOPs. This information should be shared directly between operational actors, and not via the Protection Cluster.

Personal data is collected by appropriate partners based on personal data protection principles. Personal data is shared between service providers when conducting a referral for the provision of services as needed. The personal data shared must be limited to only the information necessary for the service provider to provide that service effectively.

Aggregated data can be shared with relevant protection coordination mechanisms to allow for situation and response monitoring based on do no harm and protection information management principles.

Enablers of Safe Data Collection and Sharing

Enablers of Safe Data Collection and Sharing		
Practical & Procedural	**Institutional & Structural**	**Mindset & Trust**
• ICT and data protection & security • Data/IM environment: access, safety • Staff capacity & resources • SoPs, protocols • Data Sharing/Request Agreements • Guidance, checklists • DPIA/Risk Assessment tool	• Humanitarian 'eco-system'/architecture incl. Coordination structures • Organizational & inter-agency policies	• Incentives & sanctions • Trust Framework & Ground Rules • Show by example/role model(s) • Openness/attitude change

Data Sharing Protocols

Protection Clusters can enable safe data collection and sharing through the development of data sharing protocols. These protocols are governed by the principles of AAP, to emphasise that people affected by crises are the owners of and decision-makers regarding their data. No decisions shall be taken for them without their explicit consent.

A data sharing protocol does not replace individual agency policies or remove the need for bilateral data-sharing agreements. It is an umbrella guidance document to ensure trust and confidence between protection partners.

It can cover all relevant phases of the data management process and multiple types of protection data, including but not limited to:

- The location of protection services (service mapping)
- Referral data
- Humanitarian access data
- Needs assessment data
- Movement data and locations of affected people
- 3/4/5W data
- Community perception
- Distribution data
- Data produced from collective analysis of Focus Group Discussions (FGDs), key informant interviews (KIIs)
- Feedback and complaint mechanism (including referral) data.

Given the importance of service mapping and referral to the protection response, specific SOPs and protocols are often developed to outline standards and best practice that governs:

- Exchange of personal information between partners
- Exchange of anonymous information from the partner to the cluster (e.g. number of referrals/types of services needed)
- Reporting of overall data by the cluster, for response monitoring

Protection Clusters and Data Responsibility

The primary reference on data responsibility for Clusters is the IASC Operational Guidance on Data Responsibility in Humanitarian Action (2023) which provides 12 principles for guiding data management practices for clusters, and six Cluster-level actions for data responsibility.

1. Conduct a cluster/sector level data responsibility diagnostic.
2. Create and maintain a cluster/sector data management registry.
3. Develop and maintain a cluster/sector-specific Information Sharing Protocol.
4. Offer technical and advisory support to cluster/sector members on data responsibility.
5. Design for data responsibility in cluster/sector-led data management activities.
6. Track and communicate about data incidents within the cluster/sector.

Data responsibility plays a crucial role in IM responsibilities within the Protection Cluster. IMOs are responsible for ensuring the safe, ethical, and effective management of personal and non-personal data, aligning with established frameworks for personal data protection. To fulfil this role effectively, the principles outlined in the IASC Operational Guidance on Data Responsibility in Humanitarian Action must be adhered to throughout all the Cluster’s IM work. This includes conducting data responsibility diagnostics, creating data management registries, and developing information sharing protocols specific to the Protection Cluster.

The Cluster coordination team must be discerning in determining when and what data to share, and with who. While data like household and key informant interviews are essential for various purposes such as site profiling and surveys, certain details like precise GPS locations may pose risks.

Therefore, IMOs must establish clear protocols in collaboration with Cluster partners and other clusters to ensure the responsible and secure handling of data. This includes identifying which infographics and data can be shared safely and ethically, considering data sensitivity and potential risks, and promoting the principles of data responsibility throughout the Protection Cluster's IM activities.

10.4 Key Resources and Tools

Title	Type	Language	Year
IASC Operational Guidance on Data Responsibility in Humanitarian Action	Guidance	ENG, FRE, ESP	2023
Handbook on Data Protection in Humanitarian Action (ICRC)	Operational Guidance	ENG	2024
Protocol on sharing of data in the context of the Protection Monitoring System (PMS) of the Iraq Protection Cluster (NPC)	Example	ENG *Upon Request*	2019

Humanitarian Data Sharing Protocol – Afghanistan	Example	ENG *Upon Request*	2020
PIM Training: Updated PPT for Data Sharing	Training	ENG *Upon Request*	2017
Protection Cluster Information-Sharing and Data Confidentiality Protocol – Turkey Cross-Border Operations	Example	ENG *Upon Request*	2017
Policy on the Protection of Personal Data of Persons of Concern to UNHCR (UNHCR)	Operational Policy	ENG, ESP, RUS, ARA, FRE, TUR	2015
Inter-agency Child Protection Case Management Data Protection and Information Sharing Protocol (The Alliance)	Operational Guidance	ENG	2024
GPC Information Management and Analysis Toolbox	Toolbox – Website	ENG	2023
Professional Standards for Protection Work – ICRC	Handbook	ENG, ESP, FRE, ARA, RUS	2020

Protection Field Coordination Toolkit – Overview of Chapters

Visit the main toolkit landing page or navigate directly to the chapters below to access more resources and information on the Protection Cluster's role in the following areas:

Protection Field Coordination Toolkit – Overview of Chapters	
Chapter 1: Humanitarian Coordination Overview	• Coordination models for internal displacement, refugee response and mixed situations • Cluster Activation Criteria and Processes
Chapter 2: Humanitarian Programme Cycle	• Elements / Principles of the HPC and the Role of the Cluster • Flash Appeals and Pooled Funds • Integration cross-cutting issues and the Centrality of Protection into the HPC
Chapter 3: Internal Displacement	• Internal displacement and the needs of IDPs. • Legal frameworks and displacement
Chapter 4: Protection in Armed Conflict	• International Law/Principles • Humanitarian protection and Protection of Civilians (PoC). • Humanitarian Civil-Military Coordination
Chapter 5: Centrality of Protection	• The Protection Cluster's responsibilities in CoP • The difference between mainstreaming, integration and the centrality of protection. • IASC processes and HCT benchmarks
Chapter 6: Climate, Disaster, and Sudden Onset Emergencies	• Terminology and definitions in climate and disasters. • Responding to sudden onset emergencies • Actions that can be taken after a sudden onset shock (day 1-5) • Climate and disaster preparedness and response.
Chapter 7: Durable Solutions	• Global frameworks guiding Durable Solutions • Supporting durable solutions at strategic and operational levels. • The GPC Durable Solutions Guidance for Protection Clusters
Chapter 8: Cluster Transition, Deactivation and Reform	• Criteria for cluster deactivation and transition • Transition processes • Humanitarian reform initiatives • Area-based coordination
Chapter 9: Advocacy and Communication	• Developing advocacy strategies and action plans • Preparing briefings to ICCG/HCT and engaging donors • Leveraging human rights mechanisms • Communication products and media engagement
Chapter 10: Data Responsibility and Safe Information Management	• Principles of data safeguarding, management and sharing • Data responsibility in humanitarian action • Safe and effective data handling
Chapter 11: Cross-Cutting Issues	• Age, Gender, Diversity and Disability Inclusion • MHPSS • AAP • PSEA • Protection Mainstreaming
Chapter 12: Understanding Protection Programmatic Approaches and Interventions	• Locally Led Responses • Community Based Protection • Case Management • Service Mapping and Referrals • Legal Aid, Law and Policy • Cash and Protection • Humanitarian Negotiations • Anti-Trafficking • Mobile and Rapid Protection Responses