IASC Inter-Agency Standing Committee

# Operational Guidance

# DATA RESPONSIBILITY IN HUMANITARIAN ACTION

Data Responsibility Working Group

April 2023

Endorsed by IASC Operational Policy and Advocacy Group (OPAG)

IASC Inter-Agency Standing Committee

## OPERATIONAL GUIDANCE

# DATA RESPONSIBILITY IN HUMANITARIAN ACTION

# TABLE OF CONTENTS

# ACRONYMS

| | |
|---|---|
| AAP | Accountability to Affected Populations |
| AoR | Area of responsibility |
| DIA | Data Impact Assessment |
| DII | Demographically Identifiable Information |
| DPIA | Data Protection Impact Assessment |
| DRWG | Data Responsibility Working Group |
| DSA | Data Sharing Agreement |
| HCT | Humanitarian Country Team |
| HLCM | High-Level Committee on Management |
| IASC | Inter-Agency Standing Committee |
| ICCG | Inter-Cluster Coordination Group |
| ICCM | Inter-Cluster Coordination Mechanism |
| IM | Information Management |
| IMO | Information Management Officer |
| IMWG | Information Management Working Group |
| IO | International Organization |
| ISCG | Inter-Sector Coordination Group |
| ISP | Information Sharing Protocol |
| ISWG | Inter-Sector Working Group |
| NGO | Non-Governmental Organization |
| OCHA | United Nations Office for the Coordination of Humanitarian Affairs |

# FOREWORD

The Inter-Agency Standing Committee (IASC) endorsed the first version of this Operational Guidance on Data Responsibility in Humanitarian Action in February 2021. Over the past two years, the Operational Guidance has been used by humanitarian practitioners to inform actions for data responsibility and strengthen their application in at least twenty response contexts.

Given the dynamic and evolving nature of the challenges of and opportunities for data responsibility in humanitarian action, the IASC committed to reviewing and updating the Operational Guidance every two years. In June 2022, the IASC formally requested that the Data Responsibility Working Group (**DRWG**) lead this revision process.

The DRWG is a global coordination body working to advance data responsibility across the humanitarian system. It brings together a diverse group of stakeholders, including UN entities, other International Organizations, Non-Governmental Organizations, and other actors engaged in the implementation and coordination of humanitarian action. The DRWG is co-chaired by the DRC Danish Refugee Council, IOM, OCHA and UNHCR.

Between June 2022 and April 2023, the DRWG led a collaborative and consultative process to inform the preparation of this second edition of the Operational Guidance. This included:

- a literature review of relevant policies, guidance, and frameworks;
- a global survey, which received responses from 125 humanitarian practitioners from over 50 countries;
- a series of consultations with stakeholders from across the humanitarian system, including organizations, clusters, and system-wide structures;
- an open feedback period through which 100 colleagues from 25 different organizations provided input and feedback on the draft revised version; and
- three rounds of formal structured review of the draft Operational Guidance by DRWG member organizations, at different stages of its revision.

The major revisions reflected in this edition of the Operational Guidance include:

- the addition of lessons learned from the first two years of implementation of the Guidance;
- an updated assessment and overview of the challenges to and opportunities for data responsibility in humanitarian action;
- updated content to frame the Principles for Data Responsibility and minor edits to sharpen the language of each Principle and cite or otherwise reflect new frameworks of relevance;
- updated framing and descriptive text on the Actions for Data Responsibility, including modifications to specific actions to make them more operationally manageable and relevant;
- the addition of examples of data responsibility in practice as an annex to the Guidance; and
- major updates to the templates to support the effective implementation of the actions.

Progress in the area of data responsibility depends on our ability to work together, to anticipate, assess and mitigate data-related risks, and to design and implement activities that maximize the benefits and use of data, and enable the protection and rights of affected populations. We hope this second edition of the IASC Operational Guidance on Data Responsibility in Humanitarian Action can serve as the common framework for joint efforts to advance this work, which is increasingly central to how we protect and serve populations affected by crises.

**Data Responsibility Working Group Co-Chairs:**

**Kathrine Starup**
Head of Global Protection Unit
DRC Danish Refugee Council

**Rachelle Cloutier**
Senior Data Policy Officer, Global Data Service
UNHCR

**Robert Trigwell**
Data Responsibility and Ethics Officer
IOM

**Stuart Campo**
Team Lead, Data Responsibility
OCHA Centre for Humanitarian Data

# EXECUTIVE SUMMARY

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

The implementation of data responsibility in practice is often inconsistent within and across humanitarian response contexts. This is true despite established principles, norms and professional standards regarding respect for the rights of affected populations, the range of resources on data responsibility available in the wider international data community, as well as significant efforts by many humanitarian organizations to develop and update their policies and guidance in this area. While each organization is responsible for its own data management, humanitarians need common guidance to inform individual and collective action, and to uphold a high standard for data responsibility in all response contexts and in all phases of humanitarian action.

This Operational Guidance on Data Responsibility in Humanitarian Action responds to this need. The first edition of this Guidance was endorsed in February 2021 as the result of an inclusive and consultative process led under the auspices of the Inter-Agency Standing Committee (IASC). The present version of the Guidance was prepared through a collaborative process led by the Data Responsibility Working Group (**DRWG**) and endorsed by the IASC in March 2023 (see **Annex E** for additional details on the development and revision process).

## Lessons Learned on Data Responsibility in Practice

In the two years since this Operational Guidance was first endorsed in February 2021, system-wide entities, clusters/sectors and individual organizations have used it to design and implement actions for data responsibility.[1] The lessons learned through this experience (summarized below) informed the revision of the Operational Guidance, and will help promote its further use and adoption.

Lessons at the system-wide level:

- Prioritizing the establishment of an Information Sharing Protocol (ISP) at the outset of an emergency helps raise awareness of data responsibility and lays the foundation for additional actions at all levels of a response.
- Ensuring the awareness of and buy-in from the Humanitarian Country Team (HCT) on issues related to data responsibility creates space for additional investment in this area.
- Integrating actions for data responsibility into the Terms of Reference and work plans of system-wide structures such as the Information Management Working Group (IMWG), the Inter-Cluster/-Sector Coordination Group (ICCG or ISCG) and the Cash Working Group (CWG) fosters more collective action on areas of common interest.
- Providing advisory support to clusters/sectors on the implementation of actions for data responsibility fosters a more coherent approach and enables the more effective coordination of actions across the response by the ICCG/ISCG and IMWG.

1. The 15 examples are **available here**, together with a list of additional examples updated by the DRWG.
2. The ISP Template is **available here**. It is one of the many templates and tools available in **Annex B of this Operational Guidance**.

Lessons at the cluster/sector level:

- In cases where system-wide assets (i.e., an ISP and/or data and information sensitivity classification) do not provide sufficient detail or nuance to navigate cluster/sector-specific issues, developing additional guidance on data sensitivity and related techniques for handling sensitive data for cluster/sector members supports a more coherent approach to responsible data management.

- Developing common tools and approaches for responsible data management improves data sharing and use within the cluster/sector.

Lessons at the organization level:

- An organization implementing actions for data responsibility may use the templates in **Annex B** or adapt its existing organizational processes, templates and tools to be more fully aligned with this Operational Guidance.

- Data responsibility requires cross-functional collaboration. Clearly articulating the roles and responsibilities for implementing the various actions in this Operational Guidance helps staff understand how to apply it to their respective functions and activities.

- Identifying a data management activity within which actions for data responsibility can be piloted helps to demonstrate the value of this work, foster a joint understanding of concepts, and promote buy-in and ownership with staff and partners.

## Structure of the Operational Guidance

The Operational Guidance is divided into four sections:

1. The first section presents a background on data responsibility in humanitarian action, clarifies the audience and scope of the document, and provides instructions on how to use the Operational Guidance in different response scenarios.

2. The second section presents a set of Principles for Data Responsibility in Humanitarian Action.

3. The third section describes recommended actions for data responsibility to be taken at the different levels of humanitarian response (i.e., system-wide, cluster/sector, and organization levels), including specific roles and responsibilities for realizing these actions.

4. The fourth section describes an approach for the monitoring, evaluation and learning of data responsibility and the implementation of this Operational Guidance in practice.

The Annexes offer key terms and definitions (**Annex A**), suggested templates for data responsibility (**Annex B**), examples of data responsibility in practice (**Annex C**), resources and references (**Annex D**), and background information on the development of the Operational Guidance (**Annex E**).

Given the dynamic and evolving nature of the challenges and opportunities for data responsibility in humanitarian action, this Operational Guidance will be reviewed and updated through a collaborative and consultative process every two years, or more frequently if the IASC deems it necessary.

## BOX 1: DEFINING DATA RESPONSIBILITY

*A full list of terms and definitions is available in Annex A.*

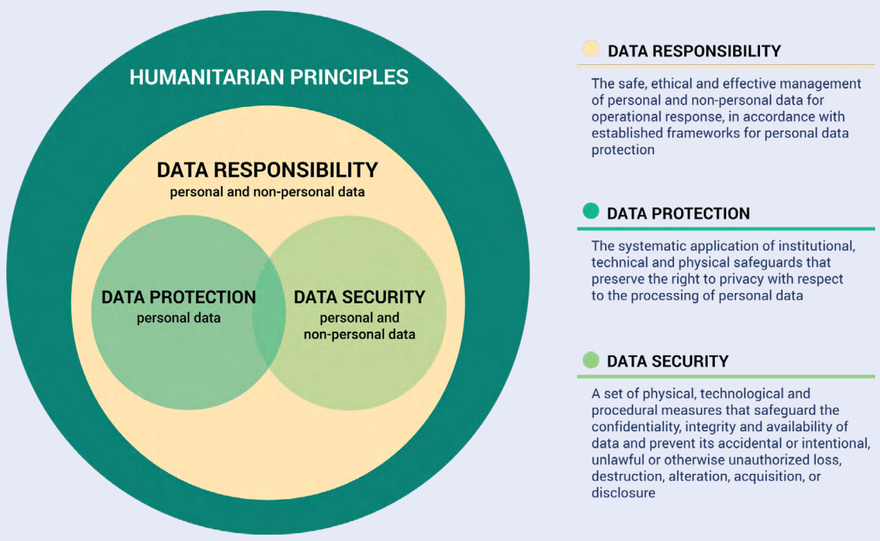
Data responsibility in humanitarian action is the **safe, ethical and effective management of personal and non-personal data for operational response**, in accordance with established frameworks for personal data protection.[3]

- **Safe** | Data management activities ensure the security of data at all times, respect and uphold human rights and other legal obligations, and do not cause harm.
- **Ethical** | Data management activities are aligned with the established frameworks and standards for humanitarian ethics[4] and data ethics.[5]
- **Effective** | Data management activities are well coordinated and achieve the purpose(s) for which they were carried out.

Data responsibility requires principled action at all levels of a humanitarian response. This includes for example actions to ensure data protection and data security, as well as strategies to minimize risks while maximizing benefits in operational data management.

While data responsibility is linked to data protection and data security, these terms are different. 'Data protection' refers to the systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the processing of personal data and uphold the rights of data subjects. 'Data security', which is applicable to both personal and non-personal data, refers to physical, technical and procedural measures that aim to safeguard the confidentiality, availability, and integrity of data.

The graphic below depicts the relationship between these key concepts and the humanitarian principles.




Description: Relationship between Humanitarian Principles, Data Security, Data Protection and Data Responsibility.

3. For the purposes of this Operational Guidance, 'in accordance with established frameworks for personal data protection' means that data management activities are guided by national and regional data protection laws or organizational data protection policies.

4. Humanitarian ethics has developed as a principle-based ethics grounded in the principles of humanity, impartiality, neutrality and independence that guide the provision of humanitarian assistance and protection. These principles and related rules are enshrined in various codes of conduct now widely recognized as the basis for ethical humanitarian practice, including: The Humanitarian Charter and Minimum Standards in Humanitarian Response, including the Core Standards and Protection Principles, the Core Humanitarian Standard on Quality and Accountability, and the Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief.



The following additional key terms should guide the reading of this Operational Guidance:

**Operational data management**: The ensemble of data management activities for operational response, including the design of activities and their subsequent execution, including the collection or receipt, storage, quality assurance, analysis, sharing, use, retention and destruction of data and information by humanitarian actors. Data management occurs as part of humanitarian action throughout the planning and response cycle across clusters/sectors and includes activities such as situational analysis, needs assessments, population data management, registration and enrollment, case management, communicating with affected populations, protection monitoring, and response monitoring and evaluation.

**Personal Data**: Any information relating to an identified or identifiable natural person ('data subject').[6] An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an image, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Non-Personal Data**: Any information that does not relate to a data subject.[7] Non-personal data can be categorized in terms of its original nature: data that has never related to a data subject (i.e., that has always been non-personal data), such as data about the context in which a response is taking place and data about humanitarian organization and their activities; or data that was initially personal data but later rendered anonymous, such as data about the people affected by the humanitarian situation and their needs, the threats and vulnerabilities they face, and their capacities. Non-personal data includes Demographically Identifiable Information (DII), i.e., data that enables the identification of groups of individuals by demographically defining factors, such as ethnicity, gender, age, occupation, religion, or location.

**Sensitive Data**: Data that, if disclosed or accessed without proper authorization, is likely to cause:

- harm (such as sanctions, discrimination) to any person, including the source of the information or other identifiable persons or groups, or;
- a negative impact on an organization's capacity to carry out its activities or on public perceptions of that organization.[8]

Both personal and non-personal data can be sensitive. Data sensitivity is defined in relation to the response context. The same types of data may have different levels of sensitivity in different contexts and sensitivity may change over time. Many organizations have specific classification systems and tools to assess data sensitivity in order to facilitate responsible data management practices.

5. The OCHA Centre for Humanitarian Data, *Guidance Note: Humanitarian Data Ethics* (2019) provides further background information on the relation between humanitarian ethics and data ethics, and is available at: https://centre.humdata.org/guidance-note-humanitarian-data-ethics/.

6. ICRC, *Handbook on Data Protection in Humanitarian Action* (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

7. Based on the definition of 'personal data' in ICRC, *Handbook on Data Protection in Humanitarian Action* (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

8. Based on the definition in the ICRC-led Advisory Group on Professional Standards, *Professional Standards for Protection Work* (2018, 3rd edition), https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights.

## BOX 2: CHALLENGES AND OPPORTUNITIES FOR DATA RESPONSIBILITY IN HUMANITARIAN ACTION

Humanitarian organizations face a range of common challenges and opportunities that form the basis for collective action as well as action by individual organizations, in the area of data responsibility.

**Challenges:**

- **Increases in the scale and number of data management activities in the sector**, often implemented without due consideration for data responsibility.
- **Limited awareness of the risks, harms and other potential negative impacts** of poor data management for affected populations, humanitarian organizations and their staff.
- **Underrepresentation** of local organizations, civil society organizations, community-based structures and data subjects in decision-making regarding data management activities.
- **Lack of risk mitigation measures and accountability mechanisms** for data management in humanitarian action.
- Lack of **common definitions** of key concepts within data responsibility and related **inconsistencies in understanding and in the use of terminology** among humanitarian organizations.
- **Gaps in existing guidance and standards**, particularly regarding the management of sensitive data, the assessment of risks related to different types of data in different contexts, and the specific and complex challenges of data responsibility in response contexts.
- **Gaps between existing guidance and implementation** thereof, both in terms of major differences between organizations' abilities to operationalize guidance, and internal differences between HQ and field offices.
- Varied applicability of **legal and regulatory frameworks**, in particular for the management of personal data, for International organizations (IOs), including UN-system organizations, international NGOs, local NGOs, and other actors.
- **Uncertainty and lack of coordination** regarding the development of new technologies and humanitarian data management standards and practices, which often evolve faster than the policies that govern their use.
- **Prioritization of organizations' internal data responsibility practices** rather than investment in the implementation of guidance across the sector.
- **Absence of shared and endorsed tools and processes** for implementing data responsibility in practice.
- **Insufficient capacity** for the implementation of data responsibility among many humanitarian organizations and their staff, including in terms of technical abilities, time constraints and technical infrastructure.



**Opportunities:**

- **Increased investment by humanitarian and development organizations, donors, and governments** in data responsibility as a strategy to advance the rights of affected populations and contribute to humanitarian outcomes and broader development goals.
- **Increased interest and demand by donors and governments** in data and evidence-informed approaches to humanitarian planning and reporting.
- **Strengthened collaboration** on data responsibility between organizations, including the sharing of resources and learnings.
- **Improved institutional and collective capacity** regarding issues related to responsible data management and the implementation of international standards and recommendations including on the protection of personal data.
- **Expanded opportunities for collaboration on data management, with the resulting efficiencies**, including through coordinated assessments, joint delivery of assistance, joint analysis (including with affected populations) and other similar activities.
- **Increased interest in and support for building a practical evidence base** of 'what works' and 'what does not work' for data responsibility in humanitarian contexts, including through greater inclusion of local knowledge.
- **Increased transparency** in how humanitarian organizations manage data in different response activities, with an associated strengthening of **accountability to affected populations**.
- **Economies of scale** through joint efforts to produce guidance on and tools for the implementation of specific measures for data responsibility.

# OVERVIEW OF THE OPERATIONAL GUIDANCE

## Background

Data responsibility is a critical issue for the humanitarian sector to address. Ensuring we Do No Harm while maximizing the benefits of data requires collective action that extends across all levels of the humanitarian system. Humanitarians must be careful when managing data to avoid placing already vulnerable individuals and communities at further risk and to safeguard trust between affected populations and humanitarian organizations.

The implementation of data responsibility in practice is often inconsistent within and across humanitarian response contexts. This is true despite established principles, norms and professional standards regarding respect for the rights of affected populations, the range of resources on data responsibility available in the wider international data community, as well as significant efforts by many humanitarian organizations to develop and update their policies and guidance in this area. Given that the humanitarian data ecosystem is inherently interconnected, no individual organization can tackle all these challenges alone.

While each organization is responsible for its own data, humanitarians need common guidance to inform individual and collective action and to uphold a high standard for data responsibility in all response contexts. This Operational Guidance complements and is informed by existing guidance[9] on data responsibility, both from development actors and the humanitarian community. It was developed under the auspices of the IASC and first endorsed in February 2021. The current version was prepared through a collaborative revision and consultation process led by the Data Responsibility Working Group (**DRWG**) and endorsed in April 2023 (see **Annex E** for additional details on the development and revision process).

## Scope

This Operational Guidance applies to both personal and non-personal data for operational response that is generated and/or used in humanitarian action, namely:

- **Data about the context** in which a response is taking place (e.g., political, social and economic conditions, geospatial data, infrastructure, etc.) and the humanitarian situation in question (e.g., security incidents, protection risks, displacement patterns and forecasts, drivers and underlying causes/factors of the situation or crisis).

- **Data about the people affected by the situation** and their needs, the threats and vulnerabilities they face, and their capacities.

- **Data about humanitarian response actors and their activities** (e.g., as reported in the Who, What, Where (3Ws) Operational Presence and similar response tracking tools).

9. This includes, for example, the IASC Operational Guidance on Responsibilities of Cluster/Sector Leads, the Professional Standards for Protection Work, the Protection Information Management (PIM) Framework, the Responsible Data for Children initiative, and the Signal Code: A Human Rights Approach to Information During Crisis, among others (see **Annex D** for additional references and resources).

Given its focus on operational data, this Operational Guidance does not cover or apply to 'corporate' (back-office) data, such as data related to internal financial management, human resources and personnel, supply chain management and logistics, and other administrative functions in humanitarian organizations.

The Operational Guidance is relevant to all forms of operational data management taking place in all humanitarian response contexts. Because humanitarian organizations have a variety of processes for data management and the data lifecycle,[10] this Operational Guidance does not present a standard or harmonized set of steps for data management. Rather, the Principles and actions in this Operational Guidance are relevant to all steps involved in operational data management for humanitarian action, regardless of the specific models developed or used by individual organizations and entities.

## Target Audience

This Operational Guidance should guide the operational data management of all humanitarian actors, including UN entities, other international organizations (IOs), international and national NGOs, civil society organizations, governments and other authorities, private sector service providers, and other stakeholders engaged in humanitarian action.

The Operational Guidance targets humanitarian coordination structures as forums for promoting, supporting and monitoring the implementation of data responsibility at different levels of a response. These include the following structures or their equivalent: the Humanitarian Country Team (HCT), the Inter-Cluster/-Sector Coordination Group (ICCG or ISCG), the Assessment (and Analysis) Working Group (AAWG or AWG), the Information Management Working Group (IMWG), the Cash Working Group (CWG), the Access Working Group (AWG) and/or other system-wide Working Groups, and Clusters, Areas of Responsibility (AoRs), sectors, Steering Committees (SC), and/or Strategic Advisory Groups (SAGs).

All personnel of humanitarian organizations and humanitarian actors, as well as other individuals (e.g., contractors, deployees from stand-by partners, and secondees) should refer to the Operational Guidance when managing data. The Operational Guidance targets different roles and functions at the system-wide, cluster/sector, and organization levels. These include Resident Coordinators/Humanitarian Coordinators (RC/HC), Heads of Office and Country Representatives, Program Managers and Officers (e.g., Program Officers, Sectoral/Technical Experts, Humanitarian Affairs Officers, and similar roles), Cluster/Sector (Co-)Coordinators and (Co-)Leads, and Technical Staff (e.g., Information Management Officers, Data Analysts, Data Scientists, Statisticians, Data Protection Officers or focal points, Information Technology Staff, Registration Officers, Community Feedback & Response Mechanism Operators, Monitoring & Evaluation Officers, Enumerators, and similar roles).

## How to Use this Operational Guidance

This Operational Guidance aims to help humanitarian staff, organizations, and their partners implement data responsibility in practice. It offers a set of Principles to guide data management in humanitarian contexts and a set of recommended actions that system-wide entities, clusters and/or sectors, and organizations can implement to advance data responsibility in their work. It does not aim to replace or supersede organizational policies and guidance,[11] nor does it account for specific organizational mandates or relevant national or regional laws.

10. A literature review of 55 documents identified 18 different data management processes and cycles, each varying in complexity, scope, and steps. The list of reviewed documents is available in **Annex D**.

11. In the case of data protection, these include, for example, the UN Privacy and Data Protection Principles, data protection policies and laws as they apply to UN agencies and NGOs, and data protection frameworks such as Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), Strasbourg* (1981), the General Data Protection Regulation (GDPR), or equivalent documents, including those of a non-binding nature.

| Scenario | How to use the Operational Guidance |
|---|---|
| New response | Staff in a new response context should focus on actions at the system-wide level (Level 1), as described in the **section** on Recommended Actions of the Operational Guidance:<br><br>• Developing and maintaining a data management registry will help keep track of the data management activities undertaken by different actors in the response context, promoting transparency as well as coordination and collaboration.<br><br>• Endorsement of an Information Sharing Protocol early in the response helps humanitarian actors align on the sensitivity of data types, as well as the ways to share data with different stakeholders. This helps promote accountability in data management as the response develops.<br><br>Implementing these actions early in a response will set a high standard for data management and promote alignment with the Principles for data responsibility. |
| Existing response without any established actions for data responsibility | Staff in response contexts where no actions for data responsibility have yet been established have two options for starting to use the Operational Guidance:<br><br>• Start with the system-wide actions (Level 1), such as an Information Sharing Protocol, and then support actions at the cluster/sector level (Level 2) and the organization level (Level 3) to promote alignment and coherence across actors and data management activities.<br><br>• Design for data responsibility by first introducing actions for data responsibility in a specific data management activity (such as a coordinated needs assessment) to demonstrate the value of this work, and then initiate further actions at the system-wide level.<br><br>Staff may decide to start implementing actions at the system-wide or cluster/sector level and to introduce actions for a specific data management activity at the same time. It is important to align and sequence the actions to avoid undertaking inconsistent or conflicting activities at the different levels. |
| Existing response with some established actions for data responsibility | Most responses will have at least some actions for data responsibility in place. For example, humanitarian organizations may have a registry of the data management activities being conducted, or an access policy for data stored by the organization. In such contexts, staff should conduct a system-wide Data Responsibility Diagnostic to determine which actions are missing or insufficiently implemented, and could be prioritized. |

# PRINCIPLES FOR DATA RESPONSIBILITY IN HUMANITARIAN ACTION

The Principles for Data Responsibility (the Principles) reflect the collective commitment of humanitarian actors to data responsibility at the system-wide, cluster/sector and organization levels. They are based on a review of existing principles for data management across the humanitarian and development sectors.[12]

The Principles guide actors in their data management activities and inform the implementation of the recommended actions for data responsibility set out in this Operational Guidance. They reinforce humanitarians' overarching commitment to Do No Harm, and reaffirm the centrality of affected people and their rights and well-being with a view to maximizing the benefits and minimizing the risks of data management in humanitarian action.[13] Organizations should uphold the Principles in accordance with their mandates, the context of the response, governing instruments, and global norms and standards, including the Humanitarian Principles.[14] Like other IASC guidance, the Principles established in this Operational Guidance do not represent a compliance standard.

The Principles are presented in alphabetical order. Wherever these Principles conflict with one another in their interpretation or application, the Principles should be interpreted, applied and balanced against each other in a manner that results in the most positive impact for affected populations.[15] In the event that the Principles conflict with either internal organizational policies or applicable legal obligations, these policies or legal obligations take precedence.

While the Principles presented below apply to both personal and non-personal data, humanitarian organizations must always adhere to the specific requirements and obligations related to the processing of personal data, as described in the Personal Data Protection principle. Although some of the Principles use the same or similar language as established principles for personal data protection (e.g., data security, proportionality, fairness, legitimacy), they are not the same. The similarity in the terms used in data responsibility and in data protection illustrates that responsible data management reflects a core set of underlying norms that are common to all data, regardless of type and the extent to which these norms are codified into law.

## Principles for Data Responsibility in Humanitarian Action

### Accountability

In accordance with relevant applicable rules, humanitarian organizations have an obligation to accept responsibility and be accountable for their data management activities. Humanitarian organizations are accountable to affected populations, to internal governance structures, and to national, regional and international actors and authorities, as applicable. Humanitarian organizations should put in place all measures required to achieve their accountability commitments in line with these Principles. Such measures include establishing adequate policies, guidance, and processes, and ensuring that sufficient and appropriate competencies and capacities are available, including but not limited to financial, human and technological resources.[16] Establishing competencies and capacities should include offering training and learning opportunities to ensure that staff have the expertise, skills, knowledge and attitudes needed to manage data responsibly.

12. A complete list of the documents compiled and analyzed by the IASC Sub-Group on Data Responsibility in 2020 to inform the drafting of the Principles is available in **Annex D**. While no principles were added or removed in the 2023 revision of this Operational Guidance, the Principles have been edited for clarity and consistency.

13. For the purposes of this document, the term 'Do No Harm' is used as follows: Data management in humanitarian response should not cause or exacerbate risk for affected people and communities, host communities, humanitarian personnel or other stakeholders, neither through actions nor omissions. 'Maximizing the benefits' of humanitarian data management entails that data is shared when a purpose requires it, in an appropriate and safe way, upholding the necessary data protection and data security requirements. It also entails that data is managed in ways that enable and increase the likelihood of positive impact for affected populations.

14. For more information on the humanitarian principles, see OCHA, *OCHA on Message: Humanitarian Principles*, available at: **https://www.unocha.org/sites/unocha/files/OOM_Humanitarian%20Principles_Eng.pdf**.

15. See **Annex C** for *Examples of Principles in Practice*.

**Confidentiality**
Humanitarian organizations should implement appropriate organizational safeguards and procedures to keep sensitive data confidential at all times, including through clear and consistent access restrictions. Measures should be in line with applicable organizational policies and legal requirements, while taking into account the relevant data and information sensitivity classification system(s) in the response context.

**Coordination and Collaboration**
Coordinated and collaborative data management entails the meaningful inclusion of humanitarian partners, national and local authorities, people affected by crisis, and other stakeholders in data management activities, where appropriate and without compromising the humanitarian principles[17] or this Operational Guidance. Humanitarian organizations should coordinate and collaborate to ensure that appropriate connections are established between humanitarian operational data management activities and longer-term development-oriented data processes and data investments. Local and national capacity should be strengthened wherever possible, and not be undermined.

**Data Security**
Humanitarian organizations should implement appropriate organizational and technical safeguards, procedures and systems to prevent, mitigate, report and respond to security breaches of both digital and non-digital data.[18] These measures should be designed to protect against material external breaches as well as unauthorized or inappropriate internal access or manipulation, accidental disclosure, damage, alteration, loss, and other security risks related to data management. Measures should be based on the sensitivity of the data and updated as data security standards and best practice evolve.

**Defined Purpose, Necessity and Proportionality**
Humanitarian data management and its related activities should have a clearly defined purpose. The design of processes and systems for data management should contribute to improved humanitarian outcomes, be consistent with relevant mandates, respect and promote rights and freedoms, and carefully balance those where needed. In line with the concept of data minimization, the management of data in humanitarian response should be relevant, limited and proportionate to the specified purpose(s).

**Fairness and Legitimacy**
Humanitarian organizations should manage data in a fair and legitimate manner. Fair data management enables the delivery of humanitarian action in a neutral and impartial manner. Legitimate grounds for data management include, for example: the best and/or vital interests of communities and individuals affected by crisis, consistent with the organization's mandate; public interest in furtherance of the organization's mandate; and any other legitimate ground specifically identified by an organization's regulatory framework and/or applicable laws.

**Human Rights-Based Approach**
Data management should be designed and implemented in ways that respect, protect and promote the fulfillment of human rights, including fundamental freedoms and the principles of equality and non-discrimination as defined in human rights frameworks, as well as data-specific rights promulgated in applicable legislation.

16. This includes upholding the IASC, *Commitments on Accountability to Affected People and Protection from Sexual Exploitation and Abuse* (2017), available at: https://interagencystandingcommittee.org/accountability-affected-populations-including-protection-sexual-exploitation-and-abuse/doc uments-56.

17. For more information on the humanitarian principles, see OCHA, *OCHA on Message: Humanitarian Principles* (2022) available at: https://www.unocha.org/sites/unocha/files/OOM_Humanitarian%20Principles_Eng.pdf.

18. Humanitarian organizations have developed distinct approaches to incidents related to data management, which should be followed accordingly. See the OCHA Centre for Humanitarian Data's *Guidance Note on Data Incident Management* (2019) for further information on managing data incidents, available at: https://centre.humdata.org/guidance-note-data-incident-management/.

**People-Centered and Inclusive**

Affected populations should be afforded an opportunity to participate and be included, represented, and empowered to exercise agency in all steps of data management for a given activity, whenever the operational context permits. The human autonomy of people affected by crisis should guide humanitarian data management. Special efforts should be made to support the participation and engagement of people who are not well represented or may be marginalized in a given data management activity (e.g., due to age, gender and other diversity characteristics such as disability, ethnicity, religion or sexual orientation), or are otherwise 'invisible', consistent with commitments to leave no one behind. These should include fostering data literacy across and within communities.

**Personal Data Protection**

When managing personal data, humanitarian organizations have an obligation to adhere to (i) applicable national and regional data protection laws, or (ii) if they enjoy privileges and immunities such that national and regional laws do not apply to them, to their own data protection policies.[19] These laws and policies contain the principles for personal data protection, such as a list of equally valid legal bases for the processing of personal data, including but not limited to consent.[20] Humanitarian organizations subject to national or regional legislation should also take into account the guidelines and advisories issued by relevant data protection authorities within their applicable jurisdiction. When designing data management systems, humanitarian organizations should meet the standards of privacy and data protection by design and by default. Humanitarian organizations should take personal data protection into consideration when developing open data frameworks. In line with their commitment to ensure accountability to affected people, inclusivity and respect for human rights, humanitarian organizations should uphold data subjects' rights to be informed, in an easily accessible and appropriate manner, about the processing of their personal data, to be able to request to access, correct, delete, object to or request information about the processing of their personal data, and to not be subject to automated decision-making except under the specific conditions set out in the legal frameworks applicable to an organization.

**Quality**

Data quality should be maintained such that the owners, users and other key stakeholders are able to trust data management activities and their resulting products. Data quality entails that data is relevant, accurate, timely, complete, standardized, interoperable, well-documented, up-to-date and interpretable, in line with the intended use and bearing in mind the given operational context. Where feasible and appropriate, and without compromising these Principles, organizations should strive to collect and analyze data by age, sex and disability disaggregation, as well as by other diversity characteristics as relevant to the defined purpose(s) of an activity.

**Retention and Destruction**

Organizations should establish a data retention and destruction schedule that indicates how long data will be retained and when data should be destroyed, as well as how to do so in a way that renders data retrieval impossible. Sensitive data should only be retained for as long as it is necessary to the specified purpose(s) for which it is managed or as required by applicable laws or audit regulations. When retaining sensitive data, organizations should specify and ensure its safe and secure storage to prevent misuse or exposure. Non-sensitive data may be retained indefinitely, in line with applicable laws, regulations and policies, and provided that access rights are established and the sensitivity of the data is reassessed on a regular basis.

19. In respect to UN-system organizations, the HLCM adopted the *Personal Data Protection and Privacy Principles*, which should serve as a foundational framework for the processing of personal data by UN entities. For organizations that do not enjoy privileges and immunities, reference should be made to applicable data protection legislation as well as sets of principles and other guidance such organizations are subject to.

20. Humanitarian organizations may not be in a position to rely on consent for all personal data processing. For further details about the legal bases for personal data processing see the ICRC *Handbook on Data Protection in Humanitarian Action* (2nd edition, 2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook. Regardless of the selected legitimate basis, data subject rights ensure the agency and involvement of individuals with regards to how their personal data is processed.

**Transparency**
Organizations should manage data in ways that offer meaningful transparency toward humanitarian actors and stakeholders, particularly affected populations. This should include the provision of timely and accurate information about the data management activity such as its purpose(s), the intended use(s) of and approaches to sharing the data, as well as any associated limitations and risks.

### EXAMPLE OF BALANCING THE PRINCIPLES IN PRACTICE

*The example below illustrates how the Principles interact and can be considered jointly when making decisions about data management in humanitarian action. See **Annex C** for more examples.*

In building an interactive dashboard with information about humanitarian operations in a response context, an organization needs to decide whether to allow external access, since the dashboard shows sensitive data as well as non-sensitive data. On the one hand, the Confidentiality principle indicates that access should be restricted. On the other, the Coordination and Collaboration principle as well as the Transparency principle indicate that non-sensitive data should be made available.

To resolve this tension in the application of the Principles, the developer adds a feature that allows access control to be specified for each layer of data included in the dashboard. The developer then limits access to the layer showing sensitive data to selected trusted humanitarian partners that require the information to inform their response and for specified and legitimate purposes. The layer showing non-sensitive data is made publicly available. In line with the Accountability principle, an SOP is prepared to document the data management process related to the development and dissemination of this dashboard, with clear roles, accountabilities and authorities for each step and for the decisions that were taken in designing the dashboard, including those pertaining to access restrictions.

Through this considered decision process, the Principles are balanced in a way that enables a safe, ethical and effective approach to data visualization and the dissemination of other information products.

# RECOMMENDED ACTIONS FOR DATA RESPONSIBILITY IN HUMANITARIAN RESPONSE CONTEXTS

This section presents the recommended actions for data responsibility at the system-wide level (1), the cluster/sector level (2) and the organization level (3). Through the implementation of these actions, humanitarian actors promote and work towards the safe, ethical and effective management of data.

The actions are applicable in all humanitarian response contexts and to all actors involved in operational data management. The actions are meant to serve as a common reference for the implementation of data responsibility in a given humanitarian response context. Implementation will vary across response contexts and require adaptation based on the nature of a particular crisis or situation. While some of the actions may be new at the system, cluster/sector, or organization levels in different contexts, all the actions are designed to build on and complement existing practices, processes and tools. Humanitarian actors and their partners will need to identify appropriate entry points for implementing these actions based on their shared assessment of the state of data responsibility in their context.[21]

The implementation of these actions at different levels should be informed by the Principles presented in the previous section. Actors should promote the centrality of affected people and their rights and well-being when tailoring the actions to different contexts. To ensure the sustained implementation and impact of these actions for data responsibility, humanitarian actors should identify the financial, human and technological resources that are required and take measures to make those resources available.

The table below provides a description of each action and its purpose in relation to data responsibility. The following subsections describe how the actions should be adapted and implemented at the system-wide, cluster/sector, and organizational levels and who should be involved. Annex B offers templates to support the implementation of the actions. Annex C offers examples of how these actions have been implemented in different settings and programmatic areas, such as Accountability to Affected People (AAP) and Cash and Voucher Assistance.

| Actions for Data Responsibility in Humanitarian Response Contexts | |
|---|---|
| **Action** | **Description and Purpose** |
| Data responsibility diagnostic<br>[Data Responsibility Diagnostic Template] | A data responsibility diagnostic provides an overview of actions for data responsibility that have been implemented in the response context.<br><br>This diagnostic helps to inform the prioritization of actions to be implemented at the three levels. |
| Data management registry<br>[Data Management Registry Template] | A data management registry provides a summary list of the key data management activities led by different actors in the response context, including the data managed in those activities. The registry supports complementarity and convergence (including with longer term development-oriented processes), facilitates collaboration, and enables prioritization and strategic decision-making regarding responsible data management. The registry also supports a common understanding of the data ecosystem in the response. |

21. See also the scenarios in the section on 'How To Use This Operational Guidance'.

| | |
|---|---|
| Data impact assessment<br>[Data Impact Assessment Template] | A data impact assessment[22] aims to determine the expected impacts of a data management activity and helps identify recommendations to mitigate the potential negative impacts. It should inform the design and implementation of a data management activity in order to maximize its benefits and minimize the risks. |
| Designing for data responsibility<br>[Template for Designing for Data Responsibility]<br>[Standard Operating Procedure for a Data Management Activity] | Designing for data responsibility entails following a set of steps and developing related outputs to ensure safe, ethical and effective data management in a given activity.<br><br>Including data responsibility considerations in the design, implementation, monitoring and evaluation of data management activities helps maximize their benefits and minimize the risks. |
| Information Sharing Protocol<br>[Information Sharing Protocol Template] | The system-wide Information Sharing Protocol (ISP) serves as the primary document of reference governing data and information sharing in the response. It should include a context-specific Data and Information Sensitivity Classification[23] outlining the sensitivity of specific data and information, as well as a recommended approach for sharing different types of data in the response.<br><br>While typically established at the system-wide level, ISPs may also be established at the cluster/sector level. |
| Data Sharing Agreement<br>[Data Sharing Agreement Template] | A data sharing agreement establishes the terms and conditions that govern the sharing of specific personal data and sensitive non-personal data between two or more parties. Many data protection frameworks require a DSA as a necessary safeguard for sharing personal data, in which case the DSA needs to adhere to the key concepts, definitions and principles established in the data protection frameworks applicable to the parties.<br><br>This type of agreement is essential to upholding legal, policy and normative requirements related to the sharing of personal and sensitive non-personal data. |
| Data incident management<br>[Template SOP for data incident management] | Data incident management refers to the processes and tools for identifying, resolving, tracking and communicating about data incidents.[24] These include a standard operating procedure for data incident management, and a registry or log that captures key details about the nature, severity and resolution of each incident.<br><br>Data incident management enables actors to address incidents and supports the development of a knowledge base to prevent and better address future incidents. Communicating about data incidents fosters more coordinated approaches to incident management over time and creates awareness across the sector.<br><br>Where the data incident constitutes a personal data breach, obligations established in the relevant data protection framework and in applicable data sharing agreements need to be adhered to. |
| Coordination and decision-making on collective action for data responsibility | Coordination and decision-making for data responsibility entails using different mechanisms to foster collective action in this area. Relevant mechanisms include the HCT, the ICCG/ISCG, and clusters/sectors, among others.<br><br>Coordination and collective actions help actors involved in a response to identify opportunities for improving data responsibility, monitor progress and challenges, and align on priorities. They also help foster accountability for and joint investment in the implementation of the other actions in this Operational Guidance. |

22. 'Data impact assessment' is a generic term that refers to multiple types of assessments, as defined in Annex A. Note that a Data Protection Impact Assessment (DPIA) is the established tool and process in data protection law that should be used (specifically) to assess personal data protection risks and compliance with the relevant data protection framework. Given the scope of DPIAs (limited to personal data), a DIA can complement a DPIA by covering the expected benefits, risks, and harms of the management of non-personal data.

23. The Data and Information Sensitivity Classification indicates the level of sensitivity of different types of data and information for a given context. This is a key component of an ISP and should be developed through a collective exercise in which different stakeholders agree on what constitutes sensitive data in their context.

24. For more information on data incident management, see: OCHA Centre for Humanitarian Data, *Guidance Note: Data Incident Management* (2019), available at: https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf.

## Level 1: System-Wide Level Actions for Data Responsibility

Supporting data responsibility at the system-wide level of a response requires collective action in a number of areas. The RC/HC's Office, the HCT, OCHA or UNHCR,[25] and various coordination structures such as the ICCG/ISCG and the IMWG have important roles to play in supporting these actions.

Humanitarian organizations should also work with the ICCG/ISCG and the IMWG, HCT and government liaison officers in-country to ensure meaningful engagement with national organizations and authorities, as appropriate in the specific context.[26] This can strengthen the response capacity of national actors, build trust, and create space for productive collaboration and management of issues related to data.

Because the adoption of data responsibility varies within and across response contexts, the actions below are meant to serve as a common reference for adaptation and implementation in a given response context. While some of these system-wide actions may be new in the response context, all the actions are designed to build on and complement existing practices, processes and tools within the humanitarian system. Specific roles and responsibilities for implementing each action are presented in the table below.

| System-Wide Level Actions for Data Responsibility | |
|---|---|
| **Action** | **Recommended Approach** |
| Conduct a system-wide data responsibility diagnostic. [Data Responsibility Diagnostic Template] | The system-wide data responsibility diagnostic provides an overview of inter-agency/ inter-cluster/inter-sector actions for data responsibility. It supports joint decision-making on how to focus and prioritize collective action on data responsibility.<br><br>This diagnostic should be completed on an annual basis by the **relevant interagency mechanism(s)** (including both the **ICCG/ISCG** and the **IMWG**) with support from **OCHA**. The diagnostic should be presented to the **HCT** and, where possible, shared with the broader response community through appropriate channels as a tool for monitoring progress on key issues related to data responsibility. |
| Generate and maintain a system-wide data management registry. [Data Management Registry Template] | The system-wide data management registry provides an overview of data management activities taking place in the response. The registry requires inputs from clusters/sectors and other inter-agency entities.<br><br>TThe system-wide data management registry should be updated on a rolling basis by the **relevant interagency mechanism(s)** (both the **ICCG/ISCG** and the **IMWG**) and presented to the **HCT** for reference.<br><br>A public version of the data management registry should be made available on ReliefWeb. |

25. The Operational Guidance proposes roles and responsibilities in line with the coordination structures introduced through the cluster approach. It recognizes the overall responsibility of national authorities, which it seeks to support by promoting coordinated action for data responsibility. In situations concerning refugees and other persons under its mandate, UNHCR is responsible for coordinating all aspects of the humanitarian response.

26. This engagement should align with the IASC *Operational Guidance For Cluster Lead Agencies on Working With National Authorities* (2011), available at: https://reliefweb.int/report/world/operational-guidance-cluster-lead-agencies-working-national-authorities-july-2011, depending on the role of national authorities in a given response.

| | |
|---|---|
| Develop and maintain a system-wide Information Sharing Protocol.<br>[Information Sharing Protocol Template] | The system-wide Information Sharing Protocol (ISP) serves as the primary document of reference governing data and information sharing in the response. It should include a context-specific Data and Information Sensitivity Classification outlining the sensitivity of specific data and information, as well as a recommended approach for sharing different types of data in the response.<br><br>The ISP should be developed through a collective exercise led by the **relevant interagency mechanism(s)** (both the **ICCG/ISCG** and the **IMWG**), with support from **OCHA** and in consultation with local authorities as appropriate. Once finalized, the ISP should be presented to the **HCT** for endorsement. All stakeholders involved in data management in the response should be aware of the ISP and their respective roles and obligations. An ISP should be reviewed on an annual basis or more frequently as needed.<br><br>Where appropriate, a public version of the ISP should be made available on ReliefWeb. |
| Track and communicate about data incidents.<br>[Template SOP for data incident management] | At the system-wide level, track data incidents using a central registry/log that captures key details about the nature, severity and resolution of incidents. When appropriate, this may be linked with other system-wide incident monitoring processes and tools, e.g., security and access monitoring systems. Measures for confidentiality and the protection of sensitive data should be taken when establishing such a registry. Where the data incident constitutes a personal data breach, obligations established in the relevant data protection framework and in applicable data sharing agreements need to be adhered to.<br><br>The **ICCG/ISCG** and **IMWG** are responsible for establishing and maintaining a central registry of data incidents and providing regular updates to the **HCT**. This registry requires inputs from the clusters/sectors and individual organizations. |
| Support coordination and decision-making on collective action related to data responsibility through existing inter-agency mechanisms. | Inter-agency and inter-cluster/sector structures should provide a common forum or platform for coordination and decision-making on data responsibility at the system-wide level. These structures should also monitor collective progress and/or challenges and opportunities for data responsibility in the context.<br><br>The **HCT** is responsible for monitoring issues related to data responsibility. The **ICCG/ISCG** and **IMWG** are responsible for providing regular updates to the HCT on their respective areas of focus in data responsibility. |

### EXAMPLE OF ACTIONS FOR DATA RESPONSIBILITY AT THE SYSTEM-WIDE LEVEL

Parts of a country have been under the control of an armed faction for the past five years. The population in the north is in need of humanitarian assistance, with the most severe needs related to protection and nutrition. The humanitarian community has faced access issues, since the armed faction has put in place restrictions on the number of aid workers allowed into the region, as well as the type of assistance provided.

To enforce these restrictions and to gather information on the population in the region under its control, the armed faction has contacted the Humanitarian Country Team (HCT) demanding that beneficiary lists as well as detailed needs assessment data at the individual or household level be shared on a monthly basis. The HCT has also received an increasing number of reports of convoys being stopped and held up at checkpoints as they leave the northern region. During these holdups, members of the armed faction have been demanding that staff of humanitarian organizations hand over electronic devices storing data, along with the passwords to information management systems. The HCT aims to determine whether there is a way to structure data and information sharing with the armed faction in order to prevent future blockades all the while upholding humanitarian principles.

Before doing so, the IMWG members take joint responsibility to conduct a data protection impact assessment (DPIA), since beneficiary lists constitute personal data. The DPIA aims to understand the impact of data sharing on beneficiaries and produce recommendations for risk mitigation. Following the DPIA, IMWG members decide to proceed with the sharing of personal data in order to ensure continued access to the territory for humanitarian purposes and to avoid endangering humanitarian workers. As jointly responsible for this decision, IMWG members document their roles and responsibilities for implementing the DPIA recommendations, for example: by ensuring that beneficiaries, as data subjects, are notified about the data sharing and by implementing other operational, technical and legal safeguards to prevent unauthorized access and misuse of personal data by the armed group.

## Level 2: Cluster/Sector Level Actions for Data Responsibility

Supporting data responsibility at the cluster/sector level requires collective action in a number of areas that complement the actions undertaken at the system-wide level and the organization level. These actions should be implemented in line with relevant existing guidance from the IASC and the global clusters. Global cluster counterparts should be consulted as appropriate in the design and/or implementation of actions at this level.

Because the implementation of data responsibility varies within and across response contexts, the actions below for the cluster/sector level are meant to serve as a common reference for adaptation and implementation in a given context. While some of the actions may be new in certain contexts, all the actions are designed to build on and complement existing practice, processes and tools within the broader humanitarian system. Depending on the nature of the response context, these actions may be completed at both the national and sub-national levels by cluster/sector Lead and Co-Lead Agencies/ entities and their respective members.

Cluster/Sector Lead and Co-Lead Agencies are responsible for ensuring the actions are implemented within the scope of a given cluster/sector's operational data management. They are also responsible for ensuring adherence to global, regional and national data protection laws (where applicable), as well as relevant humanitarian policies, standards and norms. Clusters/Sectors should ensure meaningful engagement[27] with national and local organizations and authorities, and other relevant stakeholders. Such engagement can strengthen the response capacity of national actors, build trust, and create space for productive collaboration and management of issues related to data management.

| Cluster/Sector Level Actions for Data Responsibility | |
|---|---|
| **Action** | **Recommended Approach** |
| Conduct a cluster/sector level data responsibility diagnostic. [Data Responsibility Diagnostic Template] | The cluster/sector level data responsibility diagnostic provides an overview of existing actions for data responsibility implemented within the cluster/sector. It informs the prioritization of additional actions and support activities provided by the cluster/sector on data responsibility in the context. It complements and informs the system-wide diagnostic. Clusters/Sectors should also refer to this diagnostic before undertaking any new data collection to avoid duplication, and use it to identify gaps in available data.<br><br>This diagnostic should be conducted by the **cluster/sector Lead** and **Co-Lead Agencies** in collaboration with their **members**, and made available on appropriate sharing platforms for cluster/sector members. It should be updated on an annual basis, or more frequently as needed. |
| Create and maintain a cluster/sector data management registry. [Data Management Registry Template] | The cluster/sector data management registry should include all data management activities led by the cluster/sector and those led by its members. The data management registry helps avoid duplication of efforts, and supports data and information sharing both within the cluster/sector and across the response more broadly. It also enables the cluster/sector to contribute to the system-wide data management registry.<br><br>The cluster/sector data management registry should be completed by the **cluster/sector Lead** and **Co-Lead Agencies** in collaboration with their members, and subsequently updated on an annual basis or more frequently as needed. |

27. This engagement should align with the IASC Operational Guidance for Cluster Lead Agencies on Working With National Authorities (2011), available at: https://reliefweb.int/report/world/operational-guidance-cluster-lead-agencies-working-national-authorities-july-2011, depending on the role national authorities are taking in the response, and be carried out in coordination with relevant inter-cluster/inter-sector mechanisms.

| | |
|---|---|
| Develop and maintain a cluster/sector-specific Information Sharing Protocol.<br>[Information Sharing Protocol Template] | In cases where a cluster/sector's data and information sharing needs are not sufficiently met by the system-wide ISP, an additional ISP should be developed and endorsed by all cluster/sector members. The cluster/sector-specific ISP should align with and complement the system-wide level ISP,[28] and be compatible with relevant applicable laws, policies, standards and norms in the context.<br><br>This type of ISP should be developed through a collective exercise led by the **cluster/sector Lead** and **Co-Lead Agencies**, in collaboration with their **members**. Once drafted, the ISP should be endorsed by all cluster/sector members and presented to the relevant inter-agency mechanism(s) for reference. Where appropriate, a public version of the ISP should be made available via ReliefWeb.<br><br>*Note: If cluster/sector members plan to share personal data with each other, they should establish data sharing agreements (see Level 3: Organization Level Actions for Data Responsibility, below).* |
| Offer technical and advisory support to cluster/sector members on data responsibility. | Human, financial and technological resources for data responsibility at the cluster/sector level are essential to strengthen data responsibility within the cluster/sector itself and across its members. This is particularly important when members undertake or participate in joint data management activities on behalf of or for the use of the cluster/sector overall.<br><br>Support also includes providing content on data responsibility (e.g., how to conduct data impact assessments and securely transfer sensitive data), which should be incorporated into cluster/sector level capacity development activities.<br><br>The **cluster/sector Lead** and **Co-Lead Agencies** have a responsibility to advocate for the necessary resources for the cluster/sector and for its members to be able to manage data responsibly and to promote related capacity development activities. |
| Design for data responsibility in cluster/sector-led data management activities.<br>[Template for Designing for Data Responsibility]<br>[Template Data Responsibility SOP] | Clusters/Sectors may wish to develop and support the use of common standards and tools for cluster/sector-led data management activities to foster a consistent approach among members and with the government, as relevant and appropriate.<br><br>The **cluster/sector Lead** and **Co-Lead Agencies** should aim to design cluster-led data management activities that are aligned with this Operational Guidance. This could be done for example by including data responsibility in cluster/sector strategies. |
| Track and communicate about data incidents within the cluster/sector.<br>[Template SOP for data incident management] | Tracking and communicating about data incidents within the cluster/sector helps reduce the risk of occurrence or recurrence. Activities on data incidents include establishing a common registry with details about the nature, severity, and resolution of incidents. Any such registry should ensure adequate measures for confidentiality and prevent unauthorized disclosure of sensitive data.<br><br>A cluster/sector level mechanism for data incidents should contribute to the system-wide level tracking of data incidents by sharing information with the broader community about incidents as well as good practices for mitigating risks. The **cluster/sector Lead** and **Co-Lead Agencies** have a responsibility to establish and maintain a registry of data incidents that occur in the context of data management activities that are led by the cluster/sector. They should also ensure that these incidents and the related lessons learned are shared with relevant system-wide entities and forums. |

28. For an example, see the ISP developed in 2021 for the Somalia response: https://reliefweb.int/report/somalia/somalia-information-sharing-protocol-september-2021

### EXAMPLE OF ACTIONS FOR DATA RESPONSIBILITY AT THE CLUSTER/SECTOR LEVEL

Humanitarian needs in a country have decreased and the security situation has stabilized to the point that the international community decides to scale down humanitarian assistance. A development approach will be set up to replace the humanitarian coordination structures. This means the cluster-system will be phased out and organizations with a humanitarian mandate will downsize their presence significantly. Organizations with a dual mandate will remain in-country and in some cases scale up their development activities. Development assistance will focus on the risk of seasonal flooding leading to displacement, as well as repairing physical and social infrastructure. The government is closely involved in the provision of development assistance, including, increasingly, in data and information management activities.

The clusters and humanitarian partners are determining how to responsibly manage the data they have collected in the decade since the humanitarian crisis first started. One cluster Lead Agency decides to develop a data management registry for their cluster to establish an overview of their data management activities and the data managed within each activity. Using the data management registry template in this Operational Guidance, the cluster information management focal point develops the registry. Based on the registry and the Information Sharing Protocol available in the response, the cluster lead determines for each non-personal non-personal data asset whether it should be handed over to partners remaining in-country, retained, or destroyed.

Each organization is responsible for the decision to retain or delete the personal data they collected in accordance with their own retention schedules, and for providing information to the data subjects.

Sharing the personal data with the government will likely require a data protection impact assessment, and a notification to the data subjects that their data will be transferred.

## Level 3: Organization Level Actions for Data Responsibility

Upholding data responsibility at the organization level in a given response context is critical to the implementation of the actions for data responsibility at both the system-wide and cluster/sector levels. The actions in the table below should be implemented in line with relevant organizational policies and guidelines. They do not in any way affect or replace the obligations contained in applicable organizational policies or legal and regulatory frameworks.

Because the state of data responsibility varies within and across response contexts, the actions below for individual organizations are meant to serve as a common reference for adaptation and implementation in a given context. While some of the actions may be new for an organization, all the actions are designed to build on and complement existing practices, processes and tools within the broader humanitarian system.

Given the variety of staff functions and capacities across humanitarian organizations, this Operational Guidance does not assign specific roles and responsibilities for data responsibility at the organization level. Wherever possible, organizations should integrate the actions below into the roles and responsibilities of existing teams and functions that are involved in operational data management in the response context. Additionally, organizations should liaise with coordination bodies (such as the ICCG/ISCG and IMWG), partners, donors, and other organizations in their response context in order to request technical or advisory support where needed.

| Organization Level Actions for Data Responsibility | |
|---|---|
| **Action** | **Recommended Approach** |
| Conduct an organization level data responsibility diagnostic. [Data Responsibility Diagnostic Template] | The organization level data responsibility diagnostic provides an overview of existing actions for data responsibility within an organization in a given response context. It helps an organization prioritize the implementation of additional actions for data responsibility and identify opportunities for collaboration and collective action on data responsibility within the cluster(s)/sector(s) and other inter-agency forums in which it participates.<br><br>This diagnostic should be completed on an annual basis or when the circumstances in a response context or an organization's own data management policies or practices change significantly. |
| Create and maintain an organization level data management registry. [Data Management Registry Template] | Organizations should track all data management activities they are leading or contributing to in a data management registry. They should refer to this registry when providing inputs to cluster/sector and system-wide data management registries. Organizations should also refer to this registry before undertaking any new data collection to avoid duplication, and use it to identify gaps in available data.<br><br>The organization level data management registry should be updated on a rolling basis and shared widely within a given organization as an institutional reference. |
| Conduct a data impact assessment for organization-led data management activities. [Data Impact Assessment Template] | Data impact assessments should be conducted for all data management activities involving sensitive data. DIAs should be conducted in an inclusive manner, involving affected populations where feasible. A data management activity should be redesigned or stopped if its foreseeable risks and harms outweigh its intended benefits, despite prevention and mitigation measures.<br><br>The results of a DIA should be shared with key actors involved in the data management activity and, where appropriate, with counterparts planning a similar activity in the context. This supports consistency in the assessment, monitoring, and mitigation of data-related risks over time.<br><br>*Note: Many organizations have specific policies, requirements and guidelines for how DIAs should be conducted. For those that do not, the DIA template can serve as a useful reference (see Annex B).* |

| | |
|---|---|
| Design for data responsibility in organization-led data management activities.<br>[Template for Designing for Data Responsibility]<br>[Template Data Responsibility SOP] | Organizations should incorporate data responsibility into data management *by design* as part of the planning stage for any data management activity. Designing for data responsibility includes, for example, the following steps and considerations:<br>• Address concerns identified in the Data Impact Assessment for a data management activity through appropriate, feasible, and robust prevention and mitigation measures for all major risks identified.<br>• When selecting tools for data management, foster complementarity, interoperability (where appropriate, including with governmental and other local systems), and harmonization (including on terminology, typologies and data structure).<br>• Support measures for the safe management of data (e.g., for data anonymization,[29] provision of secure storage and data transfer solutions, etc.).<br>• Adhere to relevant guidance and protocols on data responsibility and related processes and procedures, including ISPs. This includes ensuring all data that needs to be shared for defined purposes is made available through appropriate channels in a responsible manner, with the necessary safeguards for personal data and in compliance with applicable data protection frameworks.<br>• Establish clear and replicable standard operating procedures and training material for staff, as well as a designated time frame for training new staff on data responsibility.<br>• Ensure that individuals can request to access, verify, rectify and delete their personal data. |
| Establish data sharing agreements to govern the transfer of personal data and/or sensitive non-personal data.<br>[Data Sharing Agreement Template] | Organizations should establish data sharing agreements to enable the responsible sharing of personal data and/or sensitive non-personal data with other parties, in line with relevant institutional, legal and regulatory requirements as well as the Principles in this Operational Guidance. DSAs can be context-specific or established globally to govern data sharing in multiple response contexts.<br>*Note: While the purposes, modalities and circumstances for data sharing differ too much to provide a single template for DSAs, the DSA Template in Annex B offers a set of points to consider in developing such agreements, should templates and models not already exist in the organization.* |
| Establish Standard Operating Procedures for data incident management.<br>[Template SOP for Data Incident Management] | Organizations should develop and implement their own Standard Operating Procedures (SOPs) to manage data incidents. These should include a process for notification, classification, treatment, and closure of the incident. They should also include a means to log incidents into their organization's knowledge base (e.g., using a registry that captures key details about the nature, severity, and resolution of each incident). Appropriate channels for rectification and redress for individuals impacted by a data incident should also be included in the SOPs, in line with the applicable data protection and privacy framework.<br>Organizations should share their experience in managing and mitigating data incidents with other actors, i.e., at the cluster/sector and system-wide levels. |

29. This may include technical approaches such as Statistical Disclosure Control, which is a technique used in statistics to assess and lower the risk of a person or organization being re-identified from the results of an analysis of survey or administrative data, or in the release of microdata. For more information, see The Centre for Humanitarian Data, Guidance Note: Statistical Disclosure Control (2019), available at: https://centre.humdata.org/guidance-note-statistical-disclosure-control/.

### EXAMPLE OF ACTIONS FOR DATA RESPONSIBILITY AT THE ORGANIZATION

In a country long suffering from protracted crises, conflict is expected to flare up again in relation to controversial elections to be held by the end of the year. A particularly vulnerable group has been subjected to violence for decades and fears that these elections will lead to the further deterioration of their situation. Across the border, where this group faces less discrimination, there is a refugee camp where this group comprises a majority.

As part of its contingency planning, a humanitarian organization is expecting an influx of refugees into the camp and has asked for emergency relief funding to modify its registration system. The organization proposes to use iris-scans as part of a registration and identity management system. The functional ID anchored in a biometric identifier will be essential to managing the delivery of non-food items (NFIs) in the camp ensuring that NFI assistance is received only by individuals who are registered as official recipients on behalf of their household and in the quantities to which the household is entitled.

To assess the foreseeable risks and harms associated with the proposed collection of biometric data, the organization conducts a data protection impact assessment which is led by their data protection focal point. The organization's data protection toolkit contains a template data protection impact assessment (DPIA) to use for personal data. The DPIA starts with evaluating the defined purposes and proportionality of biometric data collection, and considers whether the same purposes could be achieved through less privacy intrusive means than biometrics. The DPIA then looks into the legitimate basis for using iris scans, and whether the organization is in a position to provide alternative modalities of identity verification and give beneficiaries a free choice as to how to authenticate themselves to receive assistance. The contextual analysis shows that the use of biometrics is proportionate to the stated purposes, and that no other available authentication modalities provide the same level of assurance as biometric data. Since the organization cannot base the processing of biometric data on consent, it needs to establish procedures for handling data subjects' objections to biometric enrollment. The organization also needs to consider the longer-term implications of collecting biometric data, such as, for example, the foreseeable pressure from national authorities to hand over the biometrics of the entire camp population.

# MONITORING, EVALUATION AND LEARNING

Monitoring, evaluation and learning (MEL) are essential to impactful data responsibility practice, given the rapidly evolving nature of the humanitarian data ecosystem and the increasing importance of data management in all areas of humanitarian action.

The **data responsibility diagnostic** (tool available in **Annex B**) should form the basis of MEL for data responsibility. A data responsibility diagnostic provides an overview of actions for data responsibility at the system-wide, cluster/sector or organization levels in a given response context. In addition to helping identify opportunities and challenges vis-a-vis data management and informing the prioritization of additional actions for data responsibility in the context (see previous section), a data responsibility diagnostic can also serve as a baseline for monitoring the adoption status and maturity of different actions for data responsibility. This baseline can then be used by organizations, clusters/sectors, and system-wide entities to monitor and evaluate their progress over time.

In a given response context:

- A **system-wide level** diagnostic should be completed jointly by the **ICCG/ISCG** and the **IMWG** with support from OCHA, and presented to the **HCT** for reference.
- A **cluster/sector level** diagnostic should be completed by the **cluster/sector Lead** and **Co-Lead Agencies** in collaboration with their **members** and shared with relevant system-wide entities to support for peer-to-peer learning.
- An **organization level** diagnostic should be completed by a cross-functional group of staff involved in data management and presented to management for review.

At each level, the diagnostic should be completed and then updated on an annual basis, or sooner if required, e.g., in cases of significant changes in the operational context or response.

In addition to monitoring whether and, if so, when and how different actions for data responsibility have been adopted, actors at different levels of humanitarian response must also evaluate the impact of these actions over time. System-wide entities, clusters/sectors, and organizations should define indicators for evaluating *impact* that are appropriate in the context and can be tracked and verified consistently as part of overall programme and results management activities.

# ANNEX A: TERMS AND DEFINITIONS

**Accountability to Affected Populations:** AAP is a commitment by humanitarians to use power responsibly: to take account of, give account to, and be held to account by the people we seek to assist.[30]

**Anonymization:** Process by which personal data is irreversibly altered, either by removing or modifying the identifying variables, in such a way that a data subject can no longer be identified directly or indirectly.[31]

**Anonymous data:** Data that has undergone a technical 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. This is a result of a context-specific process where such technical process is complemented, as necessary, by other technical, organizational or legal measures or otherwise binding commitments to render the risks of reidentifying data subjects insignificant.[32]

**Automated decision-making:** The process of making a decision through the processing of personal data by automated means and without review or intervention by an individual.[33]

**Biometric data:** Data used for the automated recognition of individuals based on their biological and behavioral characteristics.[34]

**Consent:** Any freely given, specific, informed and clear indication of an agreement by the data subject to the processing of their personal data.[35]

**Data:** Re-interpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.[35] [36]

**Data asset:** Data assets are a body of data or information, defined and managed as a single unit so it can be understood, shared, protected and used efficiently.[38]

**Data ethics:** Data ethics is the branch of ethics that studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including artificial intelligence, artificial agents, machine learning and robots) and corresponding practices (including responsible innovation, programming, hacking and professional codes).[39]

30. IASC, *Strengthening Accountability to Affected People (n.d.):* https://interagencystandingcommittee.org/strengthening-accountability-affected-people.

31. UN OCHA Centre for Humanitarian Data, *Glossary:* https://centre.humdata.org/glossary/.

32. UNHCR, *General Policy on Personal Data Protection and Privacy* (2022), https://www.refworld.org/docid/63d3bdf94.html.

33. UNHCR, *General Policy on Personal Data Protection and Privacy* (2022), https://www.refworld.org/docid/63d3bdf94.html.

34. ICRC, *Handbook on Data Protection in Humanitarian Action* (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

35. UNHCR, *General Policy on Personal Data Protection and Privacy* (2022), https://www.refworld.org/docid/63d3bdf94.html.

36. Children often depend on other people's consent for their participation in programmes and services which may generate and record personal data. Even when children are offered a choice to opt-in or out of a service, it might be difficult for them, depending on their development stage, to assess associated risks and benefits. Therefore, children need adequate attention on how they are provided information on their data subject rights. These UNICEF templates can help ensure that the information related to consent/ascent is provided in an appropriate and intelligible way.

37. UN, *Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity*, 2020-22 (2020), https://www.un.org/en/content/datastrategy/index.shtml.

38. Adapted from United Kingdom National Archives, *Information Asset Fact Sheet* (2017), https://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf.

39. Floridi L., Taddeo M. *What is data Ethics?* (2016) Phil. Trans. R. Soc. A 374: 20160360. http://dx.doi.org/10.1098/rsta.2016.0360.

**Data impact assessment:** A data impact assessment is a generic term to refer to a variety of tools that are used to determine the potential positive and negative impacts of a data management activity. These include commonly used – and sometimes legally required – tools such as Data Protection Impact Assessments and Privacy Impact Assessments.

**Data incidents:** Events involving data management, such as the loss, destruction, alteration, acquisition, or disclosure of data and information, caused by accidental or intentional, unlawful or otherwise unauthorized purposes that have caused harm or have the potential to cause harm.[40]

**Data management activity:** Any distinct activity involving the management of data and information as part of humanitarian response. This includes the design of the activity, as well as the collection, receipt, storage, quality assurance, analysis, sharing, use, retention and destruction of data and information by humanitarian actors.

**Data management registry:** A data management registry provides a summary of the key data management activities led by different actors in the response context, including the data managed in those activities.[41]

**Data minimization:** The objective of ensuring that only the minimum amount of data is processed to achieve the objective and purposes for which the data was collected.[42]

**Data protection:** The systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the processing of personal data.[43]

**Data protection impact assessment:** A tool and process for assessing the protection impacts on data subjects in processing their personal data and for identifying remedial actions as necessary in order to avoid or minimize such impacts.[44]

**Data responsibility:** The safe, ethical and effective management of personal and non-personal data for operational response.

**Data security:** A set of physical, technological and procedural measures that safeguard the confidentiality, integrity and availability of data and prevent its accidental or intentional, unlawful or otherwise unauthorized loss, destruction, alteration, acquisition, or disclosure.[45]

**Data Sharing Agreement:** Agreement that establishes the terms and conditions that govern the sharing of personal data and sensitive non-personal data. It is primarily used for data sharing between two or more parties. In accordance with data protection frameworks, signing a DSA may be required for the sharing of personal data.

40. The Centre for Humanitarian Data, *Guidance Note: Data Incident Management* (2019), https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf.

41. Based on the definition from Centre for Humanitarian Data, *Tip Sheet on Understanding Data Ecosystems* (2022), https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/3281e066-2643-46f0-aecf-43ee7374a453/do wnload/tip-sheet-understanding-data-ecosystems.pdf?_gl=1*cgh816*_ga*MTE2OTY5MjM0My4xNjcyNzU2NDcz*_ga_E60ZNX2F68*MTY3MzYxODU0MS4xMy4xLjE2NzM2MTk0OTUuNjAuMC4w.

42. ICRC, *Handbook on Data Protection in Humanitarian Action* (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

43. UNHCR, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* (2015), https://www.refworld.org/pdfid/55643c1d4.pdf.

44. UNHCR, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* (2015), https://www.refworld.org/pdfid/55643c1d4.pdf.

45. The Centre for Humanitarian Data. *Glossary:* https://centre.humdata.org/glossary/.

**Data subject:** A natural person (i.e., an individual) whose personal data is subject to processing, and who can be identified, either directly or indirectly, by reference to this data and reasonably likely measures. The nomination as a data subject is linked to a set of specific data subject rights to which this natural person is entitled with regards to his/her personal data, even when this data is gathered, collected or otherwise processed by others.[46]

**Harm:** The negative implications of a data processing initiative on the rights of a data subject or a group of data subjects, or other individuals, including but not limited to physical and psychological harm, discrimination and denial of access to services.[47]

**Information Sharing Protocol:** The primary document of reference governing data and information sharing in a response context, including a data and information sensitivity classification and modalities for sharing.

**Microdata:** Observation data on the characteristics of statistical units of a population, such as individuals, households, or establishments, gathered through exercises such as household surveys, needs assessment or monitoring activities.[48]

**Non-Personal Data:** Any information that does not relate to a data subject.[49]

**Operational data management:** The collection or receipt, storage, quality assurance, analysis, sharing, use, retention and destruction of data and information by humanitarian actors for operational response. Operational data management occurs as part of humanitarian action throughout the planning and response cycle and includes activities such as situational analysis, needs assessments, population data management, registration and enrollment, case management, communicating with affected populations, protection monitoring, and response monitoring and evaluation.

**Personal data:** Any information relating to an identified or identifiable natural person ('data subject').[50]

**Privacy:** The concept that states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.[51]

**Privacy impact assessment:** A process which assists organizations in identifying and minimizing the privacy risks of new projects or policies.[52]

46. ICRC, *Handbook on Data Protection in Humanitarian Action* (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

47. UN OCHA, OCHA Data Responsibility Guidelines (2021), https://centre.humdata.org/the-ocha-data-responsibility-guidelines/.

48. The OCHA Centre for Humanitarian Data, Guidance Note: Statistical Disclosure Control (2019), https://centre.humdata.org/guidance-note-statistical-disclosure-control/.

49. Based on the definition of 'personal data' in ICRC, Handbook on Data Protection in Humanitarian Action (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

50. ICRC, Handbook on Data Protection in Humanitarian Action (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

51. UN General Assembly, International Covenant on Civil and Political Rights (1976), https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

52. United Kingdom, Information Commissioner's Office (ICO), Conducting Privacy Impact Assessments Code of Practice, undated, https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf.

**Re-identification:** A process by which de-identified, pseudonymous or anonymous data can be traced back or linked to an individual(s) or group(s) of individuals through reasonably available means at the time of data re-identification.[53]

**Sensitive Data:** Data that, if disclosed or accessed without proper authorization, is likely to cause:

- harm (such as sanctions, discrimination) to any person, including the source of the information or other identifiable persons or groups; and/or
- a negative impact on an organization's capacity to carry out its activities or on public perceptions of that organization.[54]

Both personal and non-personal data can be sensitive. Data sensitivity is defined in relation to the response context. The same types of data may have different levels of sensitivity in different contexts and sensitivity may change over time. Many organizations have specific classification systems and tools to assess what constitutes sensitive data in order to facilitate responsible data management practices.[55]

53. With minor edits, based on UN OCHA, OCHA Data Responsibility Guidelines (2021), https://centre.humdata.org/the-ocha-data-responsibility-guidelines/.

54. Based on the definition in the ICRC-led Advisory Group on "Professional Standards", Professional Standards for Protection Work (2018, 3rd edition), https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights.

55. The OCHA Centre for Humanitarian Data, Glossary, https://centre.humdata.org/glossary/.

# ANNEX B: TEMPLATES FOR DATA RESPONSIBILITY

The following templates are designed to support the implementation of the recommended actions for data responsibility presented in this Operational Guidance.

These templates are provided as examples to help system-wide entities, clusters/sectors, and organizations put into practice the actions presented in this Operational Guidance. They do not replace existing templates when these already exist in an organization, either by practice or by policy.

These templates will continue to be updated based on feedback received and lessons learned on their use over time. Each template includes an introductory section describing its purpose, its source(s), and instructions for its adaptation and use.

- **Data Responsibility Diagnostic Template**
- **Data Management Registry**
- **Data Impact Assessment Template**
- **Designing for Data Responsibility**
- **Standard Operating Procedure for Data Management Activity**
- **Information Sharing Protocol Template (including a Data Sensitivity Classification)**
- **Data Sharing Agreement Template**
- **Standard Operating Procedure for Data Incident Management**

# ANNEX C: EXAMPLES OF DATA RESPONSIBILITY IN PRACTICE

The Data Responsibility Working Group (DRWG) will continue to monitor the implementation of data responsibility in practice in different response contexts and update **this list of examples**. The examples illustrate the practical nature of the Principles by showing how they can inform and impact operational data management.

Humanitarian actors interested in sharing their experiences in advancing data responsibility can submit their examples via **this form**.

# ANNEX D: RESOURCES AND REFERENCES

The following resources[56] informed the development of the IASC Operational Guidance on Data Responsibility in Humanitarian action:


Abraham, R., Schneider, J. and Vom Brocke, J., 2019. Data Governance, A Conceptual Framework, Structured Review and Research Agenda, https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Ada Lovelace Institute, 2021. Participatory Data Stewardship: https://www.adalovelaceinstitute.org/report/participatory-data-stewardship/

African Union (AU-ISC), 2018. AU Data Policy Framework: https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf

ASEAN TELMIN (AEC), 2016. ASEAN Framework on Personal Data Protection: https://www.dataguidance.com/legal-research/asean-framework-personal-data-protection

Baker, E. and Nia, G. (Atlantic Council), 2022. Attacks on Hospitals from Syria to Ukraine: https://www.atlanticcouncil.org/wp-content/uploads/2022/06/Attacks-on-Hospitals-from-Syria-to-Ukraine-Improving-Prevention-and-Accountability-Mechanisms.pdf

Brussels Privacy Hub (VUB) and International Committee of the Red Cross (ICRC), 2020. Handbook on Data Protection in Humanitarian Action (2nd edition): https://www.icrc.org/en/data-protection-humanitarian-action-handbook

CARE (Church, K.) and Raftree, L., 2019. Responsible Data Maturity Model: https://careinternational.sharepoint.com/:b:/t/Digital/EeATyuHMQSFIoiBzgKHVFKwBuRgwhvQ8mHgTfloFglS1WQ?e=x0yEvz

Catholic Relief Services, 2019. Responsible Data Values & Principles: https://www.crs.org/about/compliance/crs-responsible-data-values-principles

Commission Nationale Informatique & Libertés (CNIL). DPIA/PIA Guides and open source PIA software: https://www.cnil.fr/en/privacy-impact-assessment-pia

Core Humanitarian Standard Alliance, Group URD and the Sphere Project, 2014. The Core Humanitarian Standard on Quality and Accountability: https://corehumanitarianstandard.org/files/files/Core%20Humanitarian%20Standard%20-%20English.pdf

Council of Europe, 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) and Protocols, Strasbourg: https://www.coe.int/en/web/data-protection/convention108-and-protocol

DLA Piper, 2020. Data Protection Laws of the World: https://www.dlapiperdataprotection.com/

ELAN/Cash Learning Partnership, 2018. Data Starter Kit for Humanitarian Field Staff: https://www.calpnetwork.org/wp-content/uploads/2020/06/DataStarterKitforFieldStaffELAN.pdf


56. The resources in Annex D include the resources for the literature review conducted by the Data Responsibility Working Group in collaboration with Yale University. The results from the literature review are available from the DRWG on request via centrehumdata@un.org.

European Centre for Development Policy Management (ECDPM), 2022. Digitalisation in humanitarian aid: opportunities and challenges in forgotten crises: https://ecdpm.org/wp-content/uploads/Digitalisation-humanitarian-aid-ECDPM-Briefing-note-143-2022.pdf

European Union, 2018. General Data Protection Regulation (GDPR): https://ec.europa.eu/info/law/law-topic/data-protection_en and https://gdpr-info.eu/

Fast, L., 2022. Data Sharing between humanitarian organizations and donors: https://www.humanitarianstudies.no/resource/data-sharing-between-humanitarian-organisations-and-donors/

Floridi L., Taddeo M. 2016. What is data Ethics? Philosophical Transactions of the Royal Society A: 20160360: http://dx.doi.org/10.1098/rsta.2016.0360

Gazi, T., 2022. Data To The Rescue: How Humanitarian Organizations Should Collect Information Based on the GDPR: https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00078-0

Geiß, R. and Lahmann, H., 2021. Protection of Data in Armed Conflict: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2964&context=ils

Global Public Policy Institute (GPPI), 2021. Risks associated with humanitarian data sharing with donors: https://gppi.net/2021/09/06/data-sharing-with-humanitarian-donors

Global Migration Group (GMG) & OHCHR, 2018. Principles and Guidelines, Supported by Practical Guidance, on the Human Rights Protection of Migrants in Vulnerable Situations: https://www.ohchr.org/en/migration/migrants-vulnerable-situations

Global Partnership for Sustainable Development Data (Data4SDGs), 2022. The Data Values Project White Paper Reimagining Data and Power: A roadmap for putting values at the heart of data: https://www.data4sdgs.org/reimagining-data-and-power-roadmap-putting-values-heart-data

Grand Bargain Working Group on Workstream 5, co-convened by ECHO and OCHA, 2019: https://interagencystandingcommittee.org/grand-bargain/workstream-5-improve-joint-and-impartial-needs-assessments-january-2020-update

Grand Bargain, 2019. Principles for Coordinated Needs Assessment Ethos: https://interagencystandingcommittee.org/system/files/ws5_-_collaborative_needs_assessment_ethos.pdf

Harvard Humanitarian Initiative (HHI), 2017. The Signal Code: A Human Rights Approach to Information During Crisis: https://hhi.harvard.edu/publications/signal-code-human-rights-approach-information-during-crisis

Harvard Humanitarian Initiative (HHI), 2018. Signal Code: Ethical Obligations for Humanitarian Information Activities: https://hhi.harvard.edu/publications/signal-code-ethical-obligations-humanitarian-information

Human Rights Watch, 2014. Data privacy policies and procedures for handling data: https://www.hrw.org/privacy-policy-0

International Committee of the Red Cross (ICRC)-led Advisory Group on Professional Standards, 2018, 3rd edition. Professional Standards for Protection Work; Chapter 6: Managing Data and Information for Protection Outcomes: https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights

International Committee of the Red Cross (ICRC), 2015. Data Protection Framework: **https://www.icrc.org/en/document/icrc-data-protection-framework**

International Federation of Red Cross and Red Crescent Societies (IFRC), 2021. Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief: **https://www.ifrc.org/code-conduct-international-red-cross-and-red-crescent-movement-and-ngos-disaster-relief**

Institute of Development Studies (by Iffat Idris), 2021. Documentation of survivors of gender-based violence (GBV): **https://reliefweb.int/report/world/documentation-survivors-gender-based-violence-gbv**

Inter-Agency Standing Committee (IASC), 2008. Operational Guidance On Responsibilities Of Cluster/Sector Leads & OCHA In Information Management: **https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/IASC_operational_guidance_on_information_management.pdf**

Inter-Agency Standing Committee (IASC), 2011. Operational Guidance for Cluster Lead Agencies on Working With National Authorities: **https://reliefweb.int/report/world/operational-guidance-cluster-lead-agencies-working-national-authorities-july-2011**

Inter-Agency Standing Committee (IASC), 2016. Policy on Protection in Humanitarian Action: **https://interagencystandingcommittee.org/protection-priority-global-protection-cluster/documents/iasc-policy-protection-humanitarian-action**

Inter-Agency Standing Committee (IASC), 2017. Commitments on Accountability to Affected People and Protection from Sexual Exploitation and Abuse, available at: **https://interagencystandingcommittee.org/accountability-affected-populations-including-protection-sexual-exploitation-and-abuse/documents-56**

International Conference on Data Protection and Privacy Commissioners, 2009. Madrid Resolution: International Standards on the Protection of Personal Data and Privacy: **http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf**

International Medical Corps (IMC), 2022. Privacy Policy: **https://internationalmedicalcorps.org/privacy-policy/**

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

International Organization for Migration (IOM), 2018. DTM & Partners Toolkit: Do No Harm Checklist and Guiding Questions for DTM and Partners: **https://displacement.iom.int/dtm-partners-toolkit/field-companion-sectoral-questions-location-assessment**

International Organization for Migration (IOM), 2018. DTM & Partners Toolkit: Enhancing Responsible Data Sharing: **https://displacement.iom.int/dtm-partners-toolkit/enhancing-responsible-data-sharing**

International Organization for Migration (IOM), 2018. DTM & Partners Toolkit: DTM Data Sharing Forms: **https://displacement.iom.int/dtm-partners-toolkit/dtm-data-sharing-forms**

International Red Cross and Red Crescent Movement, 1994. Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief: **https://www.icrc.org/en/doc/resources/documents/publication/p1067.htm**

International Rescue Committee (IRC), 2018. Obtaining meaningful informed consent: https://www.rescue.org/resource/obtaining-meaningful-informed-consent

Krishnan, A, 2022. Humanitarian Digital Ethics: A Foresight and Decolonial Governance Approach: https://carrcenter.hks.harvard.edu/publications/humanitarian-digital-ethics

Médecins Sans Frontières (MSF), 2013. Data Sharing Policy: https://www.msf.org/sites/default/files/msf_data_sharing_policy_final_061213.pdf

Médecin Sans Frontières (MSF), 2021. Information on how DWB handles data collection and management of personal information: https://www.doctorswithoutborders.ca/privacy-notice#:~:text=We%20collect%20personal%20information%20in,for%20which%20it%20was%20collected

Mercy Corps, 2022. Data Protection and Privacy Guides. https://github.com/mercycorps/DPP-guides Alternate format: https://www.mercycorps.org/research-resources/data-protection-privacy-guides

Mercy Corps, 2020. Responsible Data Toolkit: https://www.mercycorps.org/research-resources/responsible-data-toolkit

MERL Tech, 2022. Responsible Data Governance for M&E in Africa: https://merltech.org/new-guides-responsible-data-governance-for-me-in-africa/

MERL Tech/various. Responsible Data Hackpad: https://paper.dropbox.com/doc/Responsible-Data-Hackpad-SA6kouQ4PL3SOVa8GnMEY

Office of the Australian Information Commissioner, Undertaking a Privacy Impact Assessment (Training): https://www.oaic.gov.au/s/elearning/pia/welcome.html

Organization for Economic Cooperation and Development (OECD), 2013. Data Protection Principles for the 21st century: https://www.repository.law.indiana.edu/facbooks/23/

Oxfam, 2015. Responsible Data Program Policy: https://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950

Oxfam, 2017. Responsible Data Management Training Pack: https://policy-practice.oxfam.org.uk/our-approach/toolkits-and-guidelines/responsible-data-management

Principles for Digital Development, 2017: https://digitalprinciples.org

Protection Cluster (Ukraine), 2022. Protecting and Prioritising People with Specific Needs in the Ukrainian Humanitarian Response: https://reliefweb.int/report/ukraine/protecting-prioritising-people-specific-needs-ukrainian-humanitarian-response-may-2022-enuk

Protection Information Management (PIM) Initiative, 2015. PIM Principles: http://pim.guide/guidance-and-products/product/principles-protection-information-management-may-2015/

Protection Information Management (PIM) Initiative, 2017. PIM Quick Reference Flyer (PIM Process, Matrix & Principles): http://pim.guide/essential/principles-matrix-process-quick-reference-flyer/

Protection Information Management (PIM) Initiative, 2017. PIM Principles in Action: http://pim.guide/guidance-and-products/product/pim-principles-action/

Protection Information Management (PIM) Initiative, 2018. PIM Framework for Data Sharing in Practice: http://pim.guide/essential/a-framework-for-data-sharing-in-practice/

Terre des Hommes and CartONG, 2017. Data Protection Starter Kit: https://www.im-portal.org/blogs/data-protection-starter-kit-introduction-pack

The Engine Room: Responsible Data Program, 2016. Responsible Data in Development Toolkit: https://responsibledata.io/resources/handbook/

The Sphere Project, 2018. The Humanitarian Charter and Minimum Standards in Humanitarian Response (Sphere): https://handbook.spherestandards.org/en/sphere/#ch001

United Kingdom, Information Commissioner's Office (ICO), undated. Conducting Privacy Impact Assessments Code of Practice: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

United Kingdom, Foreign, Commonwealth & Development Office (FCDO). Personal Information Charter: https://www.gov.uk/government/organisations/foreign-commonwealth-development-office/about/personal-information-charter

Adapted from United Kingdom National Archives, 2017. Information Asset Fact Sheet: https://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf

United Nations, 2020. Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020-22: https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf

United Nations Department of Management, Archives and Records Management Section, 2012. User Guide to Retention Schedule Implementation: https://archives.un.org/sites/archives.un.org/files/general/documents/guideline_retention_schedule_implementation.pdf

United Nations Department of Management, Archives and Records Management Section. Examples of Retention Schedules: https://archives.un.org/content/retention-schedules

UN General Assembly, 1976. International Covenant on Civil and Political Rights: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

United Nations Global Pulse, 2020. Risks, Harms and Benefits Assessment: https://www.unglobalpulse.org/policy/risk-assessment/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), 2021. OCHA Data Responsibility Guidelines: https://centre.humdata.org/the-ocha-data-responsibility-guidelines/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2019. Guidance Note: Data Incident Management: https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note: Humanitarian Data Ethics: https://centre.humdata.org/guidance-note-humanitarian-data-ethics/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2019. Guidance Note on Statistical Disclosure Control: **https://centre.humdata.org/guidance-note-statistical-disclosure-control/**

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note on Data Responsibility in Public-Private Partnerships: **https://centre.humdata.org/guidance-note-data-responsibility-in-public-private-partnerships/**

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note on Data Impact Assessments: **https://centre.humdata.org/guidance-note-data-impact-assessments/**

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note on Data Responsibility in Cash and Voucher Assistance: **https://centre.humdata.org/guidance-note-data-responsibility-in-cash-and-voucher-assistance/**

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note on Responsible Data Sharing with Donors: **https://centre.humdata.org/guidance-note-responsible-data-sharing-with-donors/**

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note on Responsible Approaches to Data Sharing: **https://centre.humdata.org/guidance-note-responsible-approaches-to-data-sharing/**

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2022. Tip Sheet on Understanding Data Ecosystems: **https://centre.humdata.org/tip-sheet-understanding-data-ecosystems/**

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), 2022. OCHA on Message: Humanitarian Principles: **https://www.unocha.org/sites/unocha/files/OOM_Humanitarian%20Principles_Eng.pdf**

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA) / World Economic Forum (WEF), prepared for IASC, 2007. Guiding Principles for Public-Private Collaboration for Humanitarian Action: **https://digitallibrary.un.org/record/613220?ln=en**

United Nations Office of Human Rights (OHCHR), 2010. Manual on Human Rights Monitoring (with updated chapters): **http://www.ohchr.org/EN/PublicationsResources/Pages/MethodologicalMaterials.aspx**

United Nations Office of Human Rights (OHCHR), 2018. A Human-Rights Based Approach to Data: Leaving No One Behind in the 2030 Agenda for Sustainable Development: **https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf**

United Nations Children's Fund (UNICEF), 2018. Industry Toolkit: Children's Online Privacy and Freedom of Expression: **https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf**

United Nations Children's Fund (UNICEF)/NYU Governance Laboratory (GovLab), 2019. Responsible Data for Children Synthesis report: **https://rd4c.org/files/rd4c-report-final.pdf**

United Nations Children's Fund (UNICEF), 2020. UNICEF Policy on Personal Data Protection: **https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf.pdf**

United Nations Children's Fund (UNICEF), 2020. Do-It-Yourself Toolkit: **https://data.unicef.org/wp-content/uploads/2020/12/Data-for-Children-Do-It-Yourself-Toolkit.pdf**

United Nations Children's Fund (UNICEF), 2021. Procedures for Ethical Standards in Research, Evaluation, Data Collection and Analysis: **https://www.unicef-irc.org/files/documents/d-4165-Final%20Procedure%20Ethical%20Standards%20Evidence%2004%202021.pdf**

United Nations Children's Fund (UNICEF), 2022. The Administrative Data Maturity Model (ADaMM): **https://data.unicef.org/resources/the-administrative-data-maturity-model-adamm/**

United Nations Children's Fund (UNICEF)/NYU Governance Laboratory (GovLab), 2022. RD4C Toolkit: **https://rd4c.org/tools/**

United Nations Children's Fund (UNICEF)/NYU Governance Laboratory (GovLab)/United Nations Office for the Coordination of Humanitarian Affairs (OCHA), 2021. Comparative Assessment of the IASC and RD4C Principles: **https://rd4c.org/articles/rd4c-brief-data-responsibility-in-humanitarian-action-to-improve-childrens-lives/index.html**

United Nations High Commissioner for Refugees (UNHCR), 2022. General Policy on Personal Data Protection and Privacy: **https://www.refworld.org/docid/63d3bdf94.html**

United Nations High Commissioner for Refugees (UNHCR), 2015. Policy on the Protection of Personal Data of Persons of Concern to UNHCR: **https://www.refworld.org/pdfid/55643c1d4.pdf**

United Nations High Commissioner for Refugees (UNHCR), 2018. Guidance on the Protection of Personal Data of Persons of Concern to UNHCR: **https://www.refworld.org/docid/5b360f4d4.html**

United Nations High Commissioner for Refugees (UNHCR), 2019. Data Transformation Strategy 2020-2025: Supporting protection and solutions: **https://www.unhcr.org/5dc2e4734.pdf**

United Nations Conference on Trade and Development (UNCTAD), 2020. Data Protection and Privacy Legislation Worldwide: **https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx**

United Nations Development Group (UNDG). Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda: **https://unsdg.un.org/resources/data-privacy-ethics-and-protection-guidance-note-big-data-achievement-2030-agenda**

United Nations General Assembly, 1945. Charter of the United Nations: **https://www.un.org/en/charter-united-nations/**

United Nations General Assembly, 1948. Universal Declaration of Human Rights: **https://www.un.org/en/universal-declaration-human-rights/**

United Nations General Assembly, 1990. General Assembly Resolution on Guidelines for the Regulation of Personalized Data Files, A/RES/45/95: **http://www.refworld.org/pdfid/3ddcafaac.pdf**

United Nations General Assembly, 1991. General Assembly Resolution 46/182 December 19, 1991: https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/GA%20Resolution%2046-182.pdf

United Nations High-Level Committee on Management (HLCM), 2018. Personal Data Protection and Privacy Principles: https://www.unsystem.org/personal-data-protection-and-privacy-principles

United Nations International Civil Service Commission, 2013. Standards of Conduct for the International Civil Service: https://icsc.un.org/Resources/General/Publications/standardsE.pdf

United Nations Secretariat, 2004. Secretary-General's Bulletin on the Use of Information and Communications Technology Resources and Data, ST/SGB/2004/15: https://digitallibrary.un.org/record/537886?ln=en

United Nations Secretariat, 2010. UN Information Sensitivity Toolkit: https://archives.un.org/sites/archives.un.org/files/RM-Guidelines/information_sensitivity_toolkit_2010.pdf

United Nations Secretariat, 2017. Secretary-General's Bulletin on Information Sensitivity, Classification and Handling, ST/SGB/2007/6: http://undocs.org/ST/SGB/2007/6

United Nations Secretariat, 2007. Secretary-General's Bulletin on Record-Keeping and the Management of United Nations Archives, ST/SGB/2007/5: http://www.wgarm.net/ccarm/docs-repository/doc/doc462548.PDF

United States Agency for International Development (USAID), 2019. Considerations for Using Data Responsibly at USAID: https://www.usaid.gov/responsibledata

World Food Programme (WFP), 2016. WFP Guide to Personal Data Protection and Privacy: https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

World Food Programme (WFP), 2022. Strategic Evaluation of WFP's use of technology in constrained environments: https://www.wfp.org/publications/strategic-evaluation-wfps-use-technology-constrained-environments

World Health Organization (WHO), 2007. WHO Ethical and safety recommendations for researching, documenting and monitoring sexual violence in emergencies: https://www.who.int/gender/documents/OMS_Ethics&Safety10Aug07.pdf

World Health Organization (WHO) (European Region), 2020. Collection and Integration of Data on Refugee and Migrant Health in the WHO European Region: https://apps.who.int/iris/bitstream/handle/10665/337694/9789289055369-eng.pdf

World Bank Group, 2018. Personal Data Privacy Policy: http://documents.worldbank.org/curated/en/466121527794054484/pdf/Privacy-Board-Paper-050318-vF-05042018.pdf

World Refugee Council and Centre for International Governance (Dragana Kaurin), 2019. Data Protection and Digital Agency for Refugees: https://www.cigionline.org/static/documents/documents/WRC%20Research%20Paper%20no.12.pdf

World Vision International, 2017. Data Protection, Privacy, and Security for Humanitarian and Development Programs: https://www.wvi.org/health/publication/data-protection-privacy-and-security-humanitarian-development-programs

# ANNEX E: BACKGROUND ON THE DEVELOPMENT AND REVISION OF THIS OPERATIONAL GUIDANCE

**Background on the First Edition (developed in 2020 and endorsed in February 2021)**
The IASC Results Group 1 established the Sub-Group on Data Responsibility in January 2020 to lead the development of joint, system-wide operational guidance on data responsibility in humanitarian action. The Sub-Group was co-led by the International Organization for Migration, the OCHA Centre for Humanitarian Data, and the United Nations High Commissioner for Refugees. It was comprised of twenty member organizations[57] representing different stakeholders within the humanitarian system.

The Sub-Group developed this Operational Guidance through a collaborative and consultative process with IASC members and the broader humanitarian community, NGOs, United Nations entities, other international organizations, and donors at the global, regional and national levels. The development of the Operational Guidance was informed by a literature review,[58] public-facing survey,[59] consultations, an open feedback period, and three rounds of structured, organizational review of the draft Operational Guidance at different stages of development.

The Operational Guidance was endorsed by the IASC in February 2021. The first edition is available for reference here.

**Background on the Second Edition (revised in 2022 and endorsed in April 2023)**
Given the dynamic and evolving nature of the challenges and opportunities for data responsibility in humanitarian action, the IASC agreed to review and update this Operational Guidance[60] in a collaborative and consultative manner every two years. In June 2022, the IASC OPAG formally delegated responsibility for leading this revision process to the global Data Responsibility Working Group (DRWG).[61]

The DRWG undertook the revision process between June 2022 and February 2023. The revision was informed by the following activities:

- A literature review;
- A public-facing survey with humanitarian practitioners from over 50 countries;
- A series of targeted consultations with different stakeholders from across the humanitarian system, including organizations, clusters/sectors, and system-wide structures;
- An open feedback period through which 100 colleagues from 25 different organizations provided inputs and feedback on the draft revised Operational Guidance; and
- Three rounds of structured review from DRWG members of the draft Operational Guidance at different stages of its revision.

57. The Sub-Group included representatives from: CARE, CRS, DRC, ICRC, IFRC, IRC, IOM, JIPS, Mercy Corps, MSF, NRC, OCHA, OHCHR, Oxfam, Save the Children, UNFPA, UNHCR, UNICEF, WFP and WHO.

58. The Sub-Group conducted the Literature Review of relevant existing guidance on data responsibility with support from the Technical University of Delft.

59. The public survey was conducted online from 27 February to 18 March 2020. Survey results are available here: https://centre.humdata.org/survey-results-on-priorities-for-data-responsibility-in-humanitarian-action/.

60. OCHA will be responsible for initiating the review and updating process for this Operational Guidance.

61. The DRWG is a global coordination body working to advance data responsibility across the humanitarian system. It brings together a diverse group of stakeholders including UN entities, other International Organizations, Non-Governmental Organizations, and other actors engaged in the coordination and implementation of humanitarian action. The DRWG is co-chaired by the Danish Refugee Council (DRC), IOM, OCHA and UNHCR. More information on the DRWG can be found here.