OCHA
DATA RESPONSIBILITY GUIDELINES

OCTOBER 2021

OCHA CENTRE FOR HUMANITARIAN DATA

OCHA

centre for humdata

TABLE OF CONTENTS

PREFACE **3**

Structure of the Guidelines 4
How to use the Guidelines 5
Acronyms 6

1. INTRODUCTION **7**

1.1 Data Responsibility in Humanitarian Action 8
1.2 OCHA's Role in Humanitarian Data Management 10
1.3 Scope of the Guidelines 11

2. PRINCIPLES FOR DATA RESPONSIBILITY IN HUMANITARIAN ACTION **12**

3. ACTIONS FOR DATA RESPONSIBILITY IN PRACTICE **14**

3.1 OCHA's Role in System-Wide Level Actions for Data Responsibility 17
3.2 OCHA's Role in Cluster/Sector Level Actions for Data Responsibility 22
3.3 Data Responsibility within OCHA Offices 23

4. ACCOUNTABILITY **29**

5. SERVICES TO SUPPORT ADOPTION OF THE GUIDELINES **33**

ANNEX A - DEFINITIONS 36

ANNEX B - PRINCIPLES FOR DATA RESPONSIBILITY IN HUMANITARIAN ACTION 40

ANNEX C - DATA RESPONSIBILITY IN OCHA'S DATA MANAGEMENT 43

ANNEX D - TEMPLATES FOR DATA RESPONSIBILITY 45

ANNEX E - FOUNDATIONS FOR DATA RESPONSIBILITY AT OCHA 46

ANNEX F - ADDITIONAL RESOURCES 48

PREFACE

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

The OCHA Data Responsibility Guidelines ('the Guidelines') offer a set of principles, processes and tools that support data responsibility in OCHA's work.[1]

The core audience for the Guidelines is OCHA staff involved in managing data across OCHA's core functions of coordination, advocacy, policy, humanitarian financing and information management, with a primary focus on the field.

The Guidelines are informed by a series of gap analysis studies, research and field testing conducted by OCHA over the past several years.[2] This includes extensive piloting of a working draft[3] of the Guidelines by OCHA offices in ten different response contexts in 2019 and 2020, with support from the OCHA Centre for Humanitarian Data ('the Centre'). These pilots informed the revision of the Guidelines for finalization and endorsement in 2021.

The Guidelines reflect the latest global guidance and policy instructions within the United Nations (UN) Secretariat and the broader humanitarian system, including:

- The Secretary-General's Roadmap for Digital Cooperation[4]
- The Secretary-General's Data Strategy[5]
- The Inter-Agency Standing Committee Operational Guidance on Data Responsibility[6]

The Guidelines also reflect forthcoming administrative issuances of the organization related to data protection and privacy. See Annex E for a list of the references that informed the development of the Guidelines and Annex F for a selection of additional resources related to data responsibility in humanitarian action.

The Guidelines will be revised every two years.

[1] As an office within the United Nations Secretariat, OCHA is subject to applicable policies and directives of the Secretariat. For the purposes of the OCHA Data Responsibility Guidelines, the term Office is used to refer to OCHA. However, references to principles and actions for data responsibility within and across 'humanitarian organization(s)' apply to OCHA as an office of the UN Secretariat.

[2] This includes: (a) research conducted in 2016 with the NYU Governance Lab (GovLab) and Leiden University to understand the policy and privacy landscape, and to understand related best practices of partner organizations; (b) a survey conducted by the Centre for Humanitarian Data in March 2018 amongst OCHA staff working with information and/or data; and (c) field research conducted in 2018 with the Centre and OCHA offices to better understand how sensitive data is shared and used by OCHA staff and humanitarian partners in conflict environments.

[3] UN Office for the Coordination of Humanitarian Affairs (2019), **Working Draft Data Responsibility Guidelines**.

[4] United Nations, General Assembly (2020), Report of the Secretary-General, **Road Map for Digital Cooperation: Implementation of the Recommendations of the High Level Panel on Digital Cooperation**.

[5] United Nations, **Data Strategy of the Secretary-General, 2020-2022**.

[6] Inter-Agency Standing Committee (2021), **Operational Guidance on Data Responsibility in Humanitarian Action**.

STRUCTURE OF THE GUIDELINES

The Guidelines contain five sections and a series of supporting Annexes.

Section 1: Introduction offers an overview of key concepts related to data responsibility in humanitarian action, explains the role of OCHA in humanitarian data management and clarifies the scope of the Guidelines.

Section 2: Principles for Data Responsibility in Humanitarian Action introduces the system-wide principles meant to inform the implementation of the Guidelines.

Section 3: Data Responsibility in Practice provides practical guidance on how OCHA should support actions for data responsibility at the system-wide level, cluster/sector level, and organizational level (e.g. in OCHA offices and in OCHA's own data management activities).

Section 4: Accountability outlines the key roles and responsibilities for ensuring the adoption of the Guidelines and explains how these relate to the governance and oversight functions established by forthcoming administrative issuances for the United Nations Secretariat related to data protection and privacy.

Section 5: Services to Support Adoption of the Guidelines provides an overview of the services available to OCHA staff implementing the Guidelines. These services are offered by the OCHA Centre for Humanitarian Data and are available upon request.

Annex A - Definitions provides definitions of key terms used in the Guidelines.

Annex B - Principles for Data Responsibility in Humanitarian Action provides a detailed description of the Principles.

Annex C - Data Responsibility in OCHA's Data Management presents a set of steps that OCHA staff should take to uphold data responsibility in a given data management activity.

Annex D - Templates for Data Responsibility brings together the different templates referenced throughout the Guidelines. Editable versions of each template are available via links included in this Annex.

Annex E - Foundations for Data Responsibility at OCHA presents an overview of existing instruments that directly or indirectly guide OCHA's data management.

Annex F - Additional Resources offers a set of references related to data responsibility in the sector.

HOW TO USE THE GUIDELINES

The Guidelines offer an overall approach and minimum standard for data responsibility across OCHA. Because data responsibility varies across functions and responses, use of the Guidelines will take different forms. The table below offers some recommendations for effective use of the Guidelines in different scenarios in which OCHA staff manage data.

Scenario	How to use the Guidelines
Emergency Response Preparedness	Staff involved in Emergency Response Preparedness should consider the actions included in Sections 3.1 and 3.3 of the Guidelines. • In the Risk Profiling and Monitoring element, conduct a system-wide data responsibility diagnostic. • In the Minimum Preparedness Actions element, develop a system-wide Information Sharing Protocol and Standard Operating Procedures for any OCHA-led data management activities. • In the Advanced Preparedness Actions and Contingency Planning element, develop a Standard Operating Procedure for Data Incident Management. The OCHA templates in Annex D include notes on their use in Emergency Response Preparedness.
New response environment	Staff in a new response environment should focus on the system-wide actions outlined in Section 3.1 of the Guidelines. Supporting these actions early in a response will set a high standard for data management and position OCHA as a facilitator of data responsibility.
Existing response environment with no established actions for data responsibility	Staff in response environments with no established actions for data responsibility have two options for starting to use the Guidelines: • Start with the system-wide actions, such as an Information Sharing Protocol, then build down to support actions for data responsibility within the different data management activities led or coordinated by OCHA. • Start by introducing actions for data responsibility in a specific data management activity (such as a coordinated needs assessment) to demonstrate the value of this work, then initiate actions at the system-wide level.
Existing response environment with some established actions for data responsibility	Most protracted crisis environments where OCHA is present will have at least some actions for data responsibility in place. In such contexts, staff should conduct a system-wide Data Responsibility Diagnostic (see Section 3.1) to determine which actions to prioritize.

[7] Instructions for use in Emergency Response Preparedness are aligned with the **IASC Guidelines on Emergency Response Preparedness (draft for field testing)**, July 2015.

Global or regional teams leading or supporting humanitarian data management activities	Staff at headquarters and in regional offices working on data management should focus on the step-wise guidance in Section 3.3 of the Guidelines and adapt the tips and outputs to their data management activities.

A range of support services are available to staff using the Guidelines in these and other scenarios. See **Section 5: Services to Support Implementation of the Guidelines** for more information.

PREFACE

ACRONYMS

3W	Who is doing What, Where?
4W	Who is doing What, Where, When?
AWG	Access Working Group
AAWG	Assessment & Analysis Working Group
DIA	Data impact assessment
DII	Demographically Identifiable Information
DPIA	Data Protection Impact Assessment
DSA	Data sharing agreement
HAO	Humanitarian Affairs Officer
HCT	Humanitarian Country Team
HoO	Head of Office
IASC	Inter-Agency Standing Committee
ICCG	Inter-Cluster Coordination Group
IM	Information Management
IMB	Information Management Branch
IMO	Information Management Officer
IMWG	Information Management Working Group
ISCG	Inter-Sector Coordination Group
ISP	Information Sharing Protocol
NGO	Non-Governmental Organization
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
SOP	Standard Operating Procedure
UN	United Nations

1. INTRODUCTION

1.1 DATA RESPONSIBILITY IN HUMANITARIAN ACTION

Data is a critical component of humanitarian response. The management of data relating to crisis contexts, affected people and humanitarian operations allows the humanitarian community to respond more effectively and efficiently. However, as organizations manage increasingly large volumes of data, they also face more complex challenges and risks.

Irresponsible data management in humanitarian responses can place already vulnerable people and communities at greater risk of harm or exploitation, e.g. by exposing their location or identifying a key vulnerability. This is of particular concern when humanitarian actors handle sensitive data[8] — data that is likely to lead to harm when exposed.

Both personal and non-personal data can be sensitive in humanitarian action. While there is a common understanding in the sector regarding the sensitivity of personal data, determining the sensitivity of non-personal data is more complex. For example, locations of medical facilities in conflict settings can expose patients and staff to risk, whereas this data is typically less sensitive in natural disaster response settings. The Guidelines support OCHA staff in determining the sensitivity of data and taking actions to ensure responsible data management.

In recent years we have seen the development of principles, policies and strategies for data responsibility in humanitarian action. These include system-wide guidance, such as the Inter-Agency Standing Committee Operational Guidance on Data Responsibility in Humanitarian Action, as well as global strategies and policies to guide data management within the UN system, such as the Secretary-General's Roadmap for Digital Cooperation and forthcoming administrative issuances for the organization related to data protection and privacy. Despite considerable progress, gaps remain between global frameworks and their practical application in field operations.

The OCHA Data Responsibility Guidelines ('the Guidelines') are designed to help bridge these gaps by supporting OCHA staff to apply global frameworks for data responsibility in their day-to-day work.

DEFINITIONS

Data responsibility 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.

- **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[9] and data ethics.
- **Effective** | Data management activities achieve the purpose(s) for which they were carried out.

[8] See the **Information Sharing Protocol template** for more information on how to develop a data and information sensitivity classification.

[9] 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. For additional guidance on humanitarian data ethics see The Centre for Humanitarian Data, **Guidance Note: Humanitarian Data Ethics** (2019).

Data responsibility requires the implementation of principled actions at all levels of a humanitarian response. These include for example actions to ensure data protection and data security, as well as strategies to mitigate risks while maximizing benefits in all steps of operational data management. While data responsibility is linked to data protection and data security, these terms are used differently.

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.

Data security is applicable to both personal and non-personal data and refers to technical and organizational measures that aim to preserve the confidentiality, availability, and integrity of data.

Operational data management is the design of data management activities and subsequent collection or receipt, storage, processing, analysis, sharing, use, and retention and destruction of data and information by humanitarian actors. Such activities occur as part of humanitarian action throughout the planning and response cycle across clusters/sectors and include, but are not limited to, 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 is any information relating to an identified or identifiable natural person ('data subject'). 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 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 is any information which does not relate to a data subject. Non-personal data can be categorized in terms of origin, namely: data that has never related to a data subject, such as data about the context in which a response is taking place and data about humanitarian response actors and their activities; or data that was initially personal data but later made 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 is classified as such based on the likelihood and severity of potential harm that may materialize as a result of its exposure in a particular context. Both personal and non-personal data can be sensitive. Many organizations have specific classification systems regarding what constitutes sensitive data in order to facilitate data management practices.

A full list of definitions is available in Annex A.

1.2 OCHA'S ROLE IN HUMANITARIAN DATA MANAGEMENT

OCHA plays an important and unique role in humanitarian data management across its core functions of advocacy, coordination, financing, information management, and policy. Whereas other humanitarian organizations process data primarily for their own use, OCHA's data management is mainly focused on aggregation and analysis for the wider humanitarian community.

In most responses, UN agencies, funds and programmes, and non-governmental organization (NGO) partners collect cluster/sector-specific data, such as data on shelter requirements or food consumption, to inform their own response activities. OCHA brings together data from these different partners to create a common operational picture of a humanitarian situation. This service helps avoid duplication and supports decision-making by operational and policy leaders in the field and at headquarters.

OCHA also plays a critical role in coordinating data management activities across a diverse group of stakeholders. With more actors engaging in crisis response, the hub and spoke model of coordination has shifted to a network model. In this model, OCHA continues to aggregate data for situational awareness but also takes on the added role of network enabler. OCHA's data role in a network is to connect partners to one another through the provision of services such as common standards and cloud-based infrastructure for storing and transferring data responsibly. In the age of digital data, OCHA's network enabler role must take into account the risk of hosting or acting as a passthrough for sensitive data from humanitarian partners and third-parties. The Guidelines are designed to support this role.

1.3 SCOPE OF THE GUIDELINES

The Guidelines apply to all operational data managed directly by OCHA, managed on OCHA's behalf, or managed by humanitarian actors within activities coordinated by OCHA in different responses. This includes the following types of data:

- **Data about the context** in which a response is taking place (e.g., legal frameworks, political, social and economic conditions, infrastructure, etc.) and relevant dynamics in the area of focus (e.g., security incidents, protection risks, 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 (e.g., needs assessment data, population figures, mobility data).

- **Data about the humanitarian response** (e.g. 3W data, access data, community perception data and data on humanitarian funding).

Common operational data management activities for OCHA include situational analysis, needs assessments, 3W/4W, communicating with affected populations, access monitoring, and response monitoring and evaluation. OCHA's management of corporate data, such as human resources and financial data, is regulated by existing UN Secretariat rules and is outside the scope of the Guidelines.

The Guidelines also address how OCHA should support the implementation of the IASC Operational Guidance on Data Responsibility[10] at the system-wide, cluster/sector and OCHA office (organization) level.

The core audience for the Guidelines is OCHA staff involved in managing data across OCHA's core functions, with a primary focus on the field.

[10] Inter-Agency Standing Committee (IASC), **Operational Guidance on Data Responsibility in Humanitarian Action** (2021).

2. PRINCIPLES FOR DATA RESPONSIBILITY IN HUMANITARIAN ACTION

2 PRINCIPLES FOR DATA RESPONSIBILITY IN HUMANITARIAN ACTION

The following Principles for Data Responsibility in Humanitarian Action ('the Principles') are designed to inform safe, ethical and effective operational data management in humanitarian action. They were developed and endorsed as part of the IASC Operational Guidance on Data Responsibility. The Principles should serve as a normative guide to OCHA staff and partners in implementing actions for data responsibility outlined in the Guidelines. Implementation of these Principles is without prejudice to the privileges and immunities of the UN. They are presented in alphabetical order; no hierarchy is intended.

PRINCIPLES FOR DATA RESPONSIBILITY IN HUMANITARIAN ACTION	
Accountability	Confidentiality
Coordination and Collaboration	Data Security
Defined Purpose, Necessity and Proportionality	Fairness and Legitimacy
Human Rights-Based Approach	People-Centered and Inclusive
Personal Data Protection	Quality
Retention and Destruction	Transparency

See Annex B for a detailed description of the Principles.

These Principles are based on a review of existing principles for data management across the humanitarian and development sectors.[11] They are designed to reinforce humanitarians' overarching commitment to **Do No Harm** while **maximizing the benefits** of data.[12] The Principles also reaffirm the centrality of affected people and their rights and well-being in humanitarian action.

The management of **personal data** should be informed by the principle on Personal Data Protection,[13] while the management of **non-personal data** should be informed by the other principles.

Wherever these Principles conflict with one another in their interpretation or application, they should be balanced against each other based on the particular dynamics of the response. In the event that the Principles conflict with either internal policies or applicable legal obligations, the latter take precedent.

[11] A complete list of the documents analyzed by the Sub-Group on Data Responsibility is available in the IASC Operational Guidance on Data Responsibility.

[12] See Mary B. Anderson, *Do No Harm: How Aid Can Support Peace - Or War*, (1999).

[13] This includes the UN Personal Data Protection and Privacy Principles.

3. IASC RECOMMENDED ACTIONS FOR DATA RESPONSIBILITY IN HUMANITARIAN RESPONSE CONTEXTS

3 IASC RECOMMENDED ACTIONS FOR DATA RESPONSIBILITY IN HUMANITARIAN RESPONSE CONTEXTS

The IASC Operational Guidance on Data Responsibility in Humanitarian Action recommends **eight actions** for data responsibility, summarized in the table below. The actions are designed for implementation at three levels in a given response: the system-wide level (e.g. Humanitarian Country Team, Inter-Cluster/Inter-Sector Coordination Group), the cluster/sector level, and the organization level. This section of the Guidelines provides additional guidance for OCHA staff on facilitating or implementing actions for data responsibility at these different levels. In the Guidelines, the organization level applies to OCHA offices.

DATA RESPONSIBILITY DIAGNOSTIC

A data responsibility diagnostic entails the identification and review of existing laws, norms, policies and standards in the response; processes and procedures; and technical tools for data management.

DATA ECOSYSTEM MAP AND DATA ASSET REGISTRY

A data ecosystem map provides a summary of major data management activities, including the scale, scope, and types of data being processed, stakeholders involved, data flows between different actors, and processes and platforms in use.

A data asset registry provides a summary of the key datasets being generated and managed by different actors in a response.

DATA IMPACT ASSESSMENT[14]

A data impact assessment helps determine the expected risks, harms and benefits, as well as privacy, data protection and/or human rights impacts of a data management activity.

DESIGNING FOR DATA RESPONSIBILITY

Designing for data responsibility entails accounting for the *Principles for Data Responsibility in Humanitarian Action* from the outset of a data management activity and monitoring adherence to the Principles throughout the process.

INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION

An Information Sharing Protocol (ISP) should include a context-specific Data and Information Sensitivity Classification[15], articulate common actions for data responsibility, contain clauses on personal data protection if applicable and specify how to handle breaches to the protocol.

DATA SHARING AGREEMENT

A data sharing agreement (DSA) establishes the terms and conditions that govern the sharing of personal data or sensitive non-personal data. It is primarily used for data sharing between two parties and typically established at the country level.

DATA INCIDENT MANAGEMENT[16]

Managing, tracking, and communicating about data incidents requires standard operating procedures for incident management and a central registry or log that captures key details about the nature, severity, and resolution of each incident.

COORDINATION AND DECISION-MAKING ON COLLECTIVE ACTION FOR DATA RESPONSIBILITY

Existing coordination mechanisms can be used to make decisions about collective action for data responsibility at different levels of a response. This includes the Humanitarian Country Team, the Inter-Cluster Coordination Mechanism and clusters/sectors, among others.

[14] 'Data impact assessment' is a generic term that refers to multiple types of assessments, as defined in Annex A.

[15] The Data and Information Sensitivity Classification indicates the level of sensitivity of different types of data and information for a given response. This should be developed through a collective exercise in which different stakeholders agree on what constitutes sensitive data in their context.

[16] For more information on data incident management, see: **OCHA Centre for Humanitarian Data, Guidance Note: Data Incident Management** (2019).

3.1 OCHA'S ROLE IN SYSTEM-WIDE LEVEL ACTIONS FOR DATA

The system-wide level refers to the highest-level coordination structures in a given response, e.g. the Humanitarian Country Team (HCT) and the Inter-Cluster/Inter-Sector Coordination Group (ICCG/ISCG). As the convener of the ICCG/ISCG and various technical working groups (e.g. the Information Management Working Group [IMWG], the Access Working Group [AWG], the Assessment & Analysis Working Group [AAWG], etc.), OCHA has an important role to play in supporting actions for data responsibility at the system-wide level. There are **five actions** that should be prioritized by OCHA staff at the system-wide level.

3.1 OCHA'S ROLE IN SYSTEM-WIDE LEVEL ACTIONS FOR DATA 01

CONDUCT A SYSTEM-WIDE DATA RESPONSIBLITY DIAGNOSTIC

Purpose:

A system-wide data responsibility diagnostic helps identify common opportunities and challenges for responsible data management, informs the prioritization of actions for data responsibility, and provides the HCT with a holistic understanding of data responsibility in the response.

OCHA's Role:

OCHA is responsible for initiating and facilitating the system-wide data responsibility diagnostic and presenting it to the HCT for review once finalized.

Recommended Approach:

- ☐ Prepare a draft of the diagnostic based on information available using the IASC OG Data Responsibility Diagnostic Template. This will likely require inputs from both the Coordination and Information Management (IM) teams in the office.
- ☐ Circulate the draft to ICCG/ISCG and IMWG members for inputs.
- ☐ Consolidate inputs and finalize the draft diagnostic for collective review and validation during a joint meeting of the ICCG/ISCG, the IMWG and other thematic or technical working groups as relevant, e.g. the AWG and AAWG.
- ☐ Share the final diagnostic with the HCT and offer to provide a briefing on the key findings and related recommendations for data responsibility in the response.
- ☐ Ideally, share the diagnostic jointly with the data ecosystem map (see below).

Relevant Tool or Template:

IASC OG Data Responsibility Diagnostic Template

GENERATE AND MAINTAIN A SYSTEM-WIDE DATA ECOSYSTEM MAP

Purpose:

A system-wide data ecosystem map provides a summary of major data management activities undertaken in the response. It helps identify data gaps and possible duplication, supports complementarity and convergence, facilitates collaboration, and enables prioritization and strategic decision-making on responsible data management.

OCHA's Role:

OCHA is responsible for supporting the relevant coordination mechanism(s) in completing a system-wide data ecosystem map. Upon completion, OCHA should present the ecosystem map to the HCT for reference. OCHA should also support periodic updates/revisions to the ecosystem map as the response evolves.

Recommended Approach:

- ☐ Prepare an initial draft of the ecosystem map based on information available using the IASC OG Data Responsibility Diagnostic Template. This should be led by the IM team with input and feedback from the Coordination team.
- ☐ Circulate the draft data ecosystem map to IMWG members for inputs.
- ☐ Consolidate inputs and finalize the draft data ecosystem map for collective review and validation during a joint meeting of the ICCG/ISCG, the IMWG and other thematic or technical working groups as relevant, e.g. the AWG and AAWG.
- ☐ Share the validated ecosystem map with the HCT for reference. As the response evolves, facilitate periodic updates to the ecosystem map as necessary.

Relevant Tool or Template:

IASC OG Data Ecosystem Map and Asset Registry Template

NEGOTIATE AND MAINTAIN A SYSTEM-WIDE INFORMATION SHARING PROTOCOL

Purpose:

A system-wide Information Sharing Protocol (ISP) serves as the primary document of reference governing data and information sharing in a response. It includes a context-specific Data and Information Sensitivity Classification outlining the sensitivity and related disclosure protocol for key data types.

OCHA's Role:

OCHA is responsible for supporting the ICCG/ISCG and the IMWG in jointly drafting a system-wide ISP for the response.

Recommended Approach:

- ☐ Introduce the concept of developing a system-wide ISP in the relevant coordination forum(s) and agree on an approach and timeline for the process with members. Circulate the draft to ICCG/ISCG and IMWG members for inputs.
- ☐ Develop an initial draft using the **IASC OG Information Sharing Protocol template** and circulate with the ICCG/ISCG, the IMWG and other thematic or technical working groups as relevant, e.g. the AWG and AAWG.
- ☐ Present the ISP to the HCT for review and endorsement once it has been reviewed by the ICCG/ISCG.
- ☐ All stakeholders involved in data management should be made aware of the ISP and their respective obligations. Depending on the response, OCHA should make the endorsed ISP publicly available (e.g. on ReliefWeb, HRInfo or another response-specific site).

Relevant Tool or Template:

IASC OG Information Sharing Protocol Template

MONITOR DATA INCIDENTS

Purpose:

Tracking and communicating about data incidents fosters learning, supports coordinated approaches to data incident management and helps reduce the risk of incidents occurring.

OCHA's Role:

OCHA is responsible for establishing and maintaining a registry of data incidents and providing periodic reports to the HCT.

Recommended Approach:

- ☐ Create a registry that captures key details about the nature, severity, and resolution of different incidents. Where appropriate, this may be linked with other system-wide incident monitoring processes and tools, e.g. security and access monitoring systems. Limit access to the registry to prevent unnecessary disclosure of information about incidents.
- ☐ Introduce the registry to the ICCG/ISCG and the IMWG and ensure that all relevant stakeholders are aware of the process for providing inputs, including thematic or technical working groups as relevant, e.g. the AWG and AAWG.
- ☐ Encourage inputs by the clusters/sectors on behalf of their members. Individual organizations may also provide inputs based on their own incident management tracking where these inputs are not already covered by contributions from the relevant cluster/sector.
- ☐ Prepare periodic reports summarizing the nature, severity and resolution tactics that stakeholders are using. When reporting, uphold confidentiality and do not share sensitive data.

Relevant Tool or Template:

IASC SOP for Data Incident Management Template

OCHA Data Incident Registry Template

3.1 OCHA'S ROLE IN SYSTEM-WIDE LEVEL ACTIONS FOR DATA

05

SUPPORT COORDINATION AND DECISION-MAKING ON COLLECTIVE ACTION

Purpose:

Coordination and collective action help the response community to monitor progress and identify challenges and opportunities for improving data responsibility. This also helps foster accountability and joint investment in the implementation of the recommended actions for data responsibility.

OCHA's Role:

OCHA is responsible for providing regular updates on data responsibility to the HCT. OCHA should also promote alignment across clusters/sectors and between actions at the system-wide and cluster/sector levels.

Recommended Approach:

- ☐ Provide regular updates on data responsibility to the HCT. These updates should cover collective progress, and challenges and opportunities for data responsibility in the response.
- ☐ Ensure a consolidated approach by liaising with the ICCG/ISCG, the IMWG and other relevant technical working groups for inputs ahead of HCT briefings and coordinate follow-up actions as required.
- ☐ Incorporate data responsibility as a priority topic in security briefings and other relevant presentations in the response.

Relevant Tool or Template:

Briefing Pack on Data Responsibility, OCHA's role and the IASC Operational Guidance

2-page high-level summary of the Guidelines for OCHA management

2-page high-level summary of the Guidelines for external use

3.2 OCHA'S ROLE IN CLUSTER/SECTOR LEVEL ACTIONS FOR DATA RESPONSIBILITY

Supporting data responsibility at the *cluster/sector level* will complement actions articulated at the system-wide and organization levels. Cluster/Sector Lead and Co-Lead Agencies are responsible for ensuring the actions for data responsibility are undertaken within the scope of a given cluster/sector response, in-line with the IASC Operational Guidance on Data Responsibility in Humanitarian Action. While the actions at this level are primarily designed for national-level clusters/sectors, regional clusters (covering multiple countries) and sub-national clusters may also implement these actions in certain responses.

OCHA has no direct role in completing actions at this level but should raise awareness of the IASC-recommended actions for data responsibility at the cluster/sector level. OCHA can support cluster/sector Lead and Co-Lead Agencies through the provision of technical advisory support and liaising with relevant coordination structures as needed. This includes considering the cluster/sector level actions for data responsibility when providing information management support to clusters/sectors.

OCHA may also advise on the development of cluster/sector specific ISPs and other actions at this level. OCHA should monitor the adoption and implementation of actions for data responsibility at this level and promote alignment with system-wide level actions wherever possible.

3.3 DATA RESPONSIBILITY WITHIN OCHA OFFICES

Upholding data responsibility at the *organization level* in a given response setting is critical to the success of the actions for data responsibility at the system-wide and cluster/sector levels. Given the focus of this level in the IASC Operational Guidance on Data Responsibility in Humanitarian Action, the recommended actions for data responsibility are meant for OCHA offices.[17] Some actions at this level, such as the development of a Standard Operating Procedure for data incident management, will also be relevant to OCHA headquarters sections in their operational data management.

There are **seven actions** in particular that should be prioritized by OCHA staff at the office level.

3.3 DATA RESPONSIBILITY WITHIN OCHA OFFICES 01

CONDUCT A DATA RESPONSIBLITY DIAGNOSTIC FOR THE OFFICE

Purpose:

A data responsibility diagnostic provides an overview of existing data responsibility measures within the OCHA office and supports prioritization of additional actions for data responsibility in the response. Conducting a diagnostic helps OCHA gain an understanding of the policy and governance, tools and infrastructure, and competency and capacity related to data management in a response. In turn, this understanding helps prioritize subsequent actions for data responsibility.

Recommended Approach:

- ☐ The data responsibility diagnostic should be conducted jointly by a Humanitarian Affairs Officer (HAO) and Information Management Officer (IMO).
- ☐ Use the OCHA data responsibility diagnostic template to conduct a diagnostic at this level.
- ☐ Update the diagnostic on an annual basis or when circumstances and/or OCHA's own data management policies and practices change.

Relevant Tool or Template:

OCHA Data Responsibility Diagnostic Template

[17] Data sharing between OCHA offices and/or with headquarters sections should be informed by the Guidelines and also follow the forthcoming administrative issuances on data protection and privacy for the UN Secretariat.

3.3 DATA RESPONSIBILITY WITHIN OCHA OFFICES 02

DEVELOP A DATA ASSET REGISTRY FOR THE OFFICE

Purpose:

A data asset registry provides an overview of the operational data managed by an OCHA office promotes responsible data management within the office, and informs the cluster/sector and system-wide data ecosystem maps.

Recommended Approach:

- ☐ The data asset registry should be developed and maintained by an IMO. All staff involved in data management should be aware of the registry and know how to update it.
- ☐ The data asset registry should at a minimum include the name of each dataset managed by the office, the data source, a brief description, the method for collection or receipt, the storage location, accessibility of the dataset, the sensitivity classification and a timeline for retention and destruction.
- ☐ Data sharing should also be recorded, either in the registry or in a separate data sharing log. Information on data sharing should include, at a minimum, the recipient, sharing method and date of sharing.
- ☐ Note that data with *low or no sensitivity* should be retained and remain publicly available by default.

Relevant Tool or Template:

OCHA Data Asset Registry Template

3.3 DATA RESPONSIBILITY WITHIN OCHA OFFICES 03

DESIGN DATA MANAGEMENT ACTIVITIES WITHIN THE OFFICE FOR DATA RESPONSIBILITY

Purpose:

Including data responsibility considerations in the design, implementation, monitoring and evaluation of data management activities helps minimize risks and maximize benefits. For OCHA, common operational data management activities include but are not limited to situational analysis, coordinated needs assessments, 3W/4W, communicating with affected populations, access monitoring, and response monitoring and evaluation (including through third parties). These activities typically consist of the following eight steps: Planning, Collecting, Receiving and Storing, Assuring Quality, Sharing, Analyzing, Presenting, Retaining and Destroying, and Evaluating.[18]

Recommended Approach:

- ☐ When designing a data management activity, responsible staff should follow the tips along the eight steps presented in the cycle on page 29 and outlined in Annex C.
- ☐ These tips and related outputs help staff identify and mitigate risks, select appropriate technical tools, use and share data in safe, ethical, and effective ways, and adhere to relevant guidance and protocols throughout a data management activity.
- ☐ Contact the Centre for guidance on how to adapt these tips to suit the response environment and the data management activity.

[18] There are a variety of data cycles and processes used in documentation across OCHA's different functions. The Guidelines present this cycle set of steps to offer a frame for tips and outputs that support data responsibility within a given data management activity.

3.3 DATA RESPONSIBILITY WITHIN OCHA OFFICES 04

ESTABLISH DATA SHARING AGREEMENTS

Purpose:

Data sharing agreements are essential to upholding legal, policy and normative requirements in operational data management. Such requirements typically relate to the sharing of personal data and, in some cases, sensitive non-personal data. For an OCHA office, such data may include raw survey results, beneficiary lists or detailed data on access restrictions, among others.

Recommended Approach:

- ☐ Establish data sharing agreements whenever sharing personal data or sensitive non-personal data with other organizations.
- ☐ Data sharing agreements should be developed jointly by an HAO and IMO and negotiated with the data sharing partner.
- ☐ Always consult OCHA's Executive Office to review data sharing agreements before signing.

Relevant Tool or Template:

OCHA Data Sharing Agreement Template

3.3 DATA RESPONSIBILITY WITHIN OCHA OFFICES 05

ESTABLISH A STANDARD OPERATING PROCEDURE FOR DATA INCIDENT MANAGEMENT WITHIN THE OFFICE

Purpose:

A Standard Operating Procedure (SOP) for data incident management helps reduce the risk of incidents occurring and supports the development of a knowledge base.

Recommended Approach:

- ☐ The SOP should be developed jointly by an HAO and IMO and be confirmed by the Head of Office.
- ☐ The SOP should include a process for notification, classification, treatment, and closure of the incident. It should also specify appropriate channels for rectification and redress for individuals impacted by data incidents as determined by the forthcoming administrative issuances on data protection and privacy for the UN Secretariat.
- ☐ Establish a data incident registry is used to capture key details about the nature, severity and resolution of each incident.
- ☐ OCHA offices should share their experience in managing and mitigating data incidents with other actors, i.e., at the cluster/sector and system-wide levels to foster more coordinated approaches to incident management.

Relevant Tool or Template:

IASC SOP for Data Incident Management Template

OCHA Data Incident Registry Template

[19] The action 'Ensure the availability of appropriate tools for data management' is included here as an addition to the Actions for Data Responsibility at the Organization level included in the IASC Operational Guidance on Data Responsibility in Humanitarian Action.

3.3 DATA RESPONSIBILITY WITHIN OCHA OFFICES 06

ENSURE THE AVAILABILITY OF APPROPRIATE TOOLS FOR DATA MANAGEMENT WITHIN THE OFFICE[19]

Purpose:

OCHA uses a variety of tools and guidance to support effective and efficient data management (e.g. the IM Toolbox). Using the right tool helps support safe, ethical, and effective data management, and ensure alignment with internal standards, including the Policy Instruction on Technology Standards.

Recommended Approach:

- ☐ Staff involved in data management should indicate which tools they require. The Chief of IMB will monitor implementation of the Policy Instruction on Technology Standards and delegate the management of OCHA specific standards to appropriate members of IMB.
- ☐ Use tools that are approved by the UN Office of Information and Communications Technology and included in the approved list of current software and hardware standards maintained on the OCHA IMB SharePoint page on Technology Standards.
- ☐ If a tool is not cleared and absolutely required for a given data management activity, follow the process described on OCHA IMB SharePoint page on technology standards to request review and approval of the tool.
- ☐ Confirm the use of specific tools with IMB's Digital Services Section if needed.

Relevant Tool or Template:

OCHA IMB SharePoint page on Technology Standards

3.3 DATA RESPONSIBILITY WITHIN OCHA OFFICES 07

SUPPORT KNOWLEDGE MANAGEMENT OF DATA RESPONSIBILITY WITHIN THE OFFICE[20]

Purpose:

The documents generated from the actions and processes related to data responsibility should be filed in a central repository within the office. This includes the data responsibility diagnostic, data sharing agreements, Standard Operating Procedures and data impact assessments for different data management activities, and the data asset registry, among others.

Recommended Approach:

- ☐ All colleagues involved in data management should contribute to the repository.
- ☐ Onboarding procedures for new staff in the response should include reference to the documents in the repository as well as a briefing on data responsibility.
- ☐ Offices are also encouraged to share these documents with the Centre to promote learning and consistent practice within OCHA.

[20] The action 'Support knowledge management on data responsibility within the office' is included here as an addition to the Actions for Data Responsibility at the Organization level included in the IASC Operational Guidance.

DATA RESPONSIBILITY IN OCHA'S DATA MANAGEMENT CYCLE

PLANNING

This includes identifying and documenting the various components (e.g. data sources and flows, tools and capacities, etc.) that make up the data management activity, as well as assessing impact and taking risk mitigation measures.

TIPS
- Complete a data impact assessment for the activity.
- Ensure the availability of required infrastructure.
- Use Standard Operating Procedures.
- Take additional precautions for data management activities involving the management of sensitive data.

OUTPUTS
- A completed data impact assessment.
- A data sharing agreement, Standard Operating Procedure and/or Terms of Reference, including a Data Retention and Destruction Schedule.

COLLECTING, RECEIVING AND STORING

This entails the collection, receipt and storage of data.

TIPS
- Confirm the sensitivity level of data before collection or receipt.
- Use secure tools and channels.
- Store data responsibly.
- Take additional precautions for the management of personal data or non-personal data in a sensitive context.

OUTPUTS
- The required data for the data management activity.

ASSURING QUALITY

This entails data cleaning and documenting limitations and caveats in line with relevant SOPs and standards.

TIPS
- Clean data using methods and tools appropriate to the activity and in-line with relevant criteria.
- Document all limitations or caveats.

OUTPUTS
- Datasets ready for sharing and/or analysis, including metadata.

SHARING

This involves sharing data privately with partners or making it available publicly for open access.

TIPS
- Select a responsible approach to sharing based on the relevant ISP or other applicable guidance.
- Use data sharing agreements and licenses.
- Provide metadata.
- Take additional precautions when sharing sensitive data.
- Log data sharing in the data asset registry.

OUTPUTS
- Responsibly shared data.
- Entry on data sharing in data asset registry.

ANALYZING

This focuses on the extraction of information as required for the development of information products.

TIPS
- Ensure clear documentation of methods used.
- Prevent exposure of sensitive data during analysis or visualization.
- Take extra precautions when using advanced analytical methods.

OUTPUTS
- Charts, graphs or maps displaying information, accompanied by appropriate documentation.

PRESENTING

This involves incorporating insights from the data into internal or public information products and websites.

TIPS
- Include context and data sources in published products.
- Ensure appropriate approval before release and select an appropriate license.

OUTPUTS
- Responsibly published information products.

RETAINING AND DESTROYING

This entails keeping data available for future use, or ensuring the removal of data in a way that renders retrieval impossible.

TIPS
- Assess the potential future value of data.
- Balance the risk and utility of data.
- Select the right means for long-term storage.
- Regularly reassess the sensitivity level of the data retained.
- Ensure effective destruction of data.

OUTPUTS
- Securely retained datasets.
- Effectively destroyed datasets, with clear documentation of this step and the datasets concerned.

EVALUATING

This entails internal review of the data management activity or joint review with partners as appropriate.

TIPS
- Include data responsibility considerations in any evaluation exercise conducted for the activity.
- Communicate the use of data with stakeholders.
- Record any data incidents that occurred throughout the activity.

OUTPUTS
- Finalized data management activity with documentation of any data incidents.

4. ACCOUNTABILITY

4 ACCOUNTABILITY

All OCHA staff and supporting personnel (e.g. contractors, stand-by partners, and secondments) who are authorized to manage data and related resources across OCHA should follow the Guidelines. Although effective adoption of the Guidelines requires action from all OCHA staff, accountability for adherence to the Guidelines rests with senior managers at headquarters and office level.

The **Chief of the Information Management Branch and Lead for the Information Management Function is accountable for the adoption of the Guidelines across OCHA**. Every year, the **Chief of the Information Management Branch will submit a report to the OCHA Data Steward**[21] on progress in the adoption of the Guidelines as well as any data incidents that have been reported.

The **OCHA Centre for Humanitarian Data** will track and support the adoption of the Guidelines and support the Chief of the Information Management Branch in reporting on progress as outlined above. The Centre will liaise with the **Data Protection Focal Point(s)** as necessary to complete these tasks. The Centre will also provide regular updates to the global **Data Responsibility Working Group**[22] on OCHA's progress and lessons learned in implementing the Guidelines.

At the global level, all **Functional Leads, and Branch or Section Chiefs** whose teams manage data are responsible for ensuring adoption of the Guidelines.

At the field-level, **Heads of Office** are responsible for ensuring adherence within their office.

Unit Heads are responsible for ensuring the appropriate application of the Guidelines in OCHA's day-to-day data management work.

Humanitarian Affairs Officers and **Information Management Officers** are responsible for supporting implementation of the Guidelines in their respective areas of focus.

The table below summarizes key responsibilities of different groups/units in supporting adoption of the Guidelines.

[21] The forthcoming administrative issuances for the organization related to data protection and privacy establish a set of *Data Protection Functions* for different UN entities. These include a *Data Steward (typically the head of entity)* and *Data Protection Focal Point(s)*.

[22] The Data Responsibility Working Group (DRWG) is a global coordination body working to advance data responsibility across the humanitarian system. It brings together a diverse group of stakeholders including United Nations (UN) entities, other International Organizations (IOs), Non-Governmental Organizations (NGOs), and other stakeholders engaged in the coordination and implementation of humanitarian action. The DRWG began as an Inter-Agency Standing Committee (IASC) Sub-Group in 2020 and transitioned into a system-wide working group in early 2021. The primary aim of the DRWG is to coordinate, support, and monitor collective action on data responsibility, primarily through the lens of the IASC Operational Guidance on Data Responsibility in Humanitarian Action. Learn more about the DRWG here: **https://reliefweb.int/topics/data-responsibility-working-group-drwg**.

ACCCOUNTABILITIES RELATED TO THE ADOPTION OF THE OCHA DATA RESPONSIBILITY GUIDELINES

Group / Unit	Responsibilities
Chief of IMB and head of IM Function	• Provides an annual report on adoption of the Data Responsibility Guidelines to the OCHA Data Steward. • Conduct an assessment of the effectiveness of the adoption of the Guidelines after two years.
Functional Leads, Directors and Branch Chiefs	• Promote staff awareness of and familiarity with the Guidelines. • Take corrective action and make related resources available for the management of data incidents.
Heads of Office and Section Chiefs	• Promote awareness and consultation of the Guidelines in day-to-day data management. • Ensure the availability of the required skills and resources for data responsibility. • Promote data responsibility beyond OCHA when engaging with partners.
Unit Heads	• Ensure appropriate application of the Guidelines in day-to-day data management work. • Promote data responsibility beyond OCHA when engaging with partners in the data ecosystem. • Support the HoO or Section Chief in the systematic reporting of any data incidents. • Systematically report any data incidents via the appropriate channel for tracking and support.
Humanitarian Affairs Officers and Information Management Officers	• Implement the actions for data responsibility at the relevant level(s) and in the context of their respective areas of focus (e.g. Access, Coordination, Information Management, etc.) • Apply the 'Design for Data Responsibility' action in the design and implementation of data management activities • Report any data incidents via the appropriate channel

OCHA Centre for Humanitarian Data	• Provide input and feedback on annual report to the Data Steward, to be sent out by the Chief of IMB. • Advise on best approaches to implement the Guidelines across OCHA. • Advocate for the use of the Guidelines. • Advise on data incident management. • Advise on priority areas for training and capacity development related to data responsibility.

See Section 5 for additional information on the services offered by the Centre for Humanitarian Data to support adoption of the Guidelines.

5. SERVICES TO SUPPORT ADOPTION OF THE GUIDELINES

5 SERVICES TO SUPPORT ADOPTION OF THE GUIDELINES

The Centre is committed to supporting offices and sections across OCHA in adopting the Guidelines. The Centre offers the following services upon request.

- **Introductory briefing**
  The Centre will provide introductory webinars to offices or sections upon request. This service focuses on supporting a broad understanding of the Guidelines and answering general questions on how staff can begin implementation in their context.

- **Diagnostic and assessment exercise**
  Many OCHA offices already have a number of the key actions and outputs for data responsibility in place (see Section 3 of the Guidelines). Conducting a diagnostic and assessment of the level of data responsibility in a given office can help colleagues determine what actions to prioritize in their efforts to adopt and uphold the Guidelines. The Centre is available to conduct or accompany OCHA teams in running this exercise.

- **Ad-hoc advisory services**
  Offices or sections can contact the Centre with specific questions regarding the interpretation or application of the Guidelines. The Centre will log questions and related guidance so that staff can learn from the experience of other offices.

- **Support missions**
  For contexts in which more in-depth support is required, the Centre offers support missions geared towards adapting and adopting the Guidelines, and to facilitate conversations and workshops with OCHA staff and partners on issues related to data responsibility. The missions can be used to develop context-specific protocols for responsible data management.

- **Tools and templates**
  The Centre will continue to develop tools and templates to facilitate the application of the Guidelines to specific activities.

- **Training**
  The Centre has a range of training material on data responsibility skills for OCHA staff and partners. It also offers targeted training support upon request.

- **Development of thematic guidance on data responsibility**
  The Centre will work with different teams within OCHA to develop more specific guidance[23] on adoption of data responsibility in different thematic areas.

[23] The Centre has developed a series of guidance notes on data responsibility, available here: **https://centre.humdata.org/tag/guidance-note/**.

ANNEX

ANNEX A DEFINITIONS

Aggregate data: Accumulated data acquired by combining individual-level data. It refers to data that is (1) collected from multiple sources and/or on multiple measures, variables, or individuals and (2) compiled into data summaries or summary reports, typically for the purposes of public reporting or statistical analysis.[24]

Consent: Consent is any freely given, specific and informed indication of an agreement by the data subject to the processing of their personal data.[25]

Data: Re-interpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.[26]

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 exploited efficiently.[27]

Data asset registry: A data asset registry provides a summary of the key datasets being generated and managed by different actors in a context.[28]

Data breach: The loss, destruction, alteration, acquisition, or disclosure of information caused by accidental or intentional, unlawful or otherwise unauthorized purposes , which compromise the confidentiality, integrity and/or availability of information.

Data cleaning: The process of detecting and correcting (or removing) corrupt or inaccurate records from a record set, table, or database and refers to identifying incomplete, incorrect, inaccurate or irrelevant parts of the data and then replacing, modifying, or deleting the dirty or coarse data.

Data consumer: A person or organization that uses data to make decisions, take actions, or increase awareness.

Data ecosystem map: A data ecosystem map provides a summary of major data management activities, including the scale, scope, and types of data being processed, stakeholders involved, data flows between different actors, and processes and platforms in use.[29]

Data impact assessment: A data impact assessment is a generic term to refer to a variety of tools that are used to determine the positive and negative consequences of a data management activity. These include commonly used – and sometimes legally required – tools such as Data Protection Impact Assessments and Privacy Impact Assessments.[30]

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.[31]

Data management: The data management cycle consists of the following steps: planning, collecting and receiving, storing, cleaning, transfer, analysis, communicating and disseminating, feedback and evaluation, and retention and destruction.

[24] IASC, *Operational Guidance on Data Responsibility in Humanitarian Action* (2021).

[25] Forthcoming administrative issuances for the organization.

[26] UN, ***Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020-22*** (2020).

[27] Adapted from United Kingdom National Archives, ***Information Asset Fact Sheet*** (2017).

[28] IASC, **Operational Guidance on Data Responsibility in Humanitarian Action** (2021).

[29] IASC, **Operation Guidance on Data Responsibility in Humanitarian Action** (2021).

[30] IASC, **Operational Guidance on Data Responsibility in Humanitarian Action** (2021).

[31] The Centre for Humanitarian Data, **Guidance Note: Data Incident Management** (2019).

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 were collected.[32]

Data processing: Any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collecting, registering, storing, adapting or altering, cleaning, filing, retrieving, using, disseminating, transferring and retaining or destroying.

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.[33]

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.[34]

Data provider: A person or organization that shares data directly or on behalf of another entity.

Data quality: A set of characteristics that make the data fit for the purpose for which it is processed. Data quality includes components such as accuracy, relevance, sufficiency, integrity, completeness, usability, validity, coherence, punctuality, accessibility, comparability, and timeliness.

Data responsibility: A set of principles, processes and tools that support the safe, ethical and effective management of data in humanitarian 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.[35]

Data sensitivity: Classification of data based on the likelihood and severity of potential harm that may materialize as a result of its exposure in a particular context.[36]

Data sharing agreement: Agreement that establishes the terms and conditions that govern the sharing of personal data or sensitive non-personal data. It is primarily used for data sharing between two parties and typically established at the country level.[37]

Data source: The original collector of the data concerned.

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).

Data transfer: The act of transferring data or making it accessible to a partner using any means, such as in hard copy, electronic means or the internet.

[32] ICRC, **Handbook on Data Protection in Humanitarian Action** (2020).

[33] Definition developed by the UN Privacy Policy Group (2017).

[34] UNHCR, **Policy on the Protection of Personal Data of Persons of Concern to UNHCR** (2015).

[35] The Centre for Humanitarian Data, **Glossary**.

[36] The Centre for Humanitarian Data, **Glossary**.

[37] IASC, **Operational Guidance on Data Responsibility in Humanitarian Action** (2021).

Harm: Negative implications of a data processing initiative on the rights of a data subject, or a group of data subjects, including but not limited to physical and psychological harm, discrimination and denial of access to services.

Information management: Gathering, sharing and using data and information, underpinning coordination, decision-making and advocacy.

Information product: Product derived from raw data that is organized in a way that conveys intended information to users (e.g., infographics, charts, maps, situation reports, etc.).

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.[38]

Non-personal data: Any information which does not relate to a data subject. Non-personal data can be categorized in terms of origin, namely: data that has never related to a data subject, such as data about the context in which a response is taking place and data about humanitarian response actors and their activities; *or* data that was initially personal data but later made 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.[39]

Operational data management: The design of data management activities and subsequent collection or receipt, storage, processing, analysis, sharing, use, and retention and destruction of data and information by humanitarian actors. Such activities occur as part of humanitarian action throughout the planning and response cycle across clusters/sectors and include, but are not limited to, situational analysis, needs assessments, population data management, registration and enrollment, case management, communicating with affected populations, protection monitoring, and response monitoring and evaluation.[40]

Personal data: Any information relating to an identified or identifiable natural person ('data subject').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 online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Primary data: Data that has been generated by the researcher himself/herself, surveys, interviews, experiments, specially designed for understanding and solving the research problem at hand.[41]

Privacy: 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.[42]

Re-identification: A process by which de-identified (anonymized) data becomes re-identifiable again and thus 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.

[38] The Centre for Humanitarian Data, **Guidance Note: Statistical Disclosure Control** (2019).

[39] IASC, **Operational Guidance on Data Responsibility in Humanitarian Action** (2021).

[40] IASC, **Operational Guidance on Data Responsibility in Humanitarian Action** (2021).

[41] **Public Health Research Guide, Primary & Secondary Data Definitions**.

[42] UN General Assembly, **International Covenant on Civil and Political Rights** (1976).

Risk mitigation: A process for applying specific measures to prevent and/or minimize the likelihood of likely risks related to the processing of data and prevent occurrence of harms or otherwise minimize their magnitude and severity.

Secondary data: Data that was originally collected for a specific research purpose or alternatively for no specific research purpose (e.g., national census), and is now used by other researchers for a different purpose.[43]

Sensitive data: Data classified as sensitive based on the likelihood and severity of potential harm that may materialize as a result of its exposure in a particular context. Both personal and non-personal data can be sensitive. Many organizations have specific classification systems regarding what constitutes sensitive data in order to facilitate data management practices.[44] For the UN Secretariat, the classification system is defined in ST/SGB/2007/6 on Information Sensitivity, Classification and Handling,[45] and forthcoming administrative issuances for the organization related to data protection and privacy.

Statistical Disclosure Control: 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.[46]

[43] IASC, **Operational Guidance on Data Responsibility in Humanitarian Action** (2021).

[44] The Centre for Humanitarian Data, **Glossary**.

[45] The UN **ST/SGB/2007/6**.

[46] The Centre for Humanitarian Data, **Guidance Note on Statistical Disclosure Control** (2019).

ANNEX B

PRINCIPLES FOR DATA RESPONSIBILITY IN HUMANITARIAN ACTIONS[47]

Accountability
In accordance with relevant applicable rules, humanitarian organizations have an obligation to account and accept responsibility for their data management activities. Humanitarian organizations are accountable to people affected by crisis, to internal governance structures, to national and international humanitarian partners, and, if applicable, to national governments and regulatory bodies. To achieve their accountability commitments, humanitarian organizations should put in place all measures required to uphold and monitor adherence to these Principles. This includes establishing adequate policies and mechanisms and ensuring the availability of sufficient competencies and capacities, including but not limited to personnel, resource and infrastructure capacity.[48]

Confidentiality
Humanitarian organizations should implement appropriate organizational safeguards and procedures to keep sensitive data confidential at all times. Measures should be in line with general confidentiality standards as well as standards specific to the humanitarian sector[49] and applicable organizational policies and legal requirements, while taking into account the context and associated risks.

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, all where appropriate and without compromising the humanitarian principles[50] or these Principles. Coordination and collaboration should also aim 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. These measures should be sufficient to protect against external breaches as well as unauthorized or inappropriate internal access or manipulation, accidental disclosure, damage, alteration, loss, and other risks related to data management.[51] Measures should be adjusted based on the sensitivity of the data managed and updated as data security best practice develops, both for digital data and analogue data.

[47] These Principles were developed and endorsed as part of the IASC Operational Guidance on Data Responsibility. The text of the Principles is reproduced as endorsed, with minor additions in the form of references to OCHA-specific policies and guidance where relevant. These Principles should be interpreted in-line with forthcoming administrative issuances for the organization related to data protection and privacy.

[48] This includes upholding the IASC, **Commitments on Accountability to Affected People and Protection from Sexual Exploitation and Abuse** (2017).

[49] The ICRC Handbook on Data Protection in Humanitarian Action (2020) and the IASC Policy on Protection in Humanitarian Action (2016) offer guidance on confidentiality. These standards should be interpreted in line with existing organizational policies and guidelines. This includes forthcoming administrative issuances for the organization related to data protection and privacy.

[50] For more information on the humanitarian principles, see **OCHA on Message**.

[51] Data security is specifically important when transferring and sharing data.

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 and relevant rights and freedoms, and carefully balance those where needed.[52] In line with the concept of data minimization, the management of data in humanitarian response should be relevant, limited and proportionate – in terms of required investment as well as identified risk – to the specified purpose(s).

Fairness and Legitimacy
Humanitarian organizations should manage data in a fair and legitimate manner, in accordance with their mandates, the context of the response, governing instruments, and global norms and standards, including the humanitarian principles. Legitimate grounds for data management include, for example: the best interests of people affected by crisis, consistent with the organization's mandate; public interest in furtherance of the organization's mandate; the vital interests of communities and individuals not able to make a determination about data management themselves; and any other legitimate ground specifically identified by the organization's regulatory framework or applicable laws.

Human Rights-Based Approach
Data management should be designed and implemented in ways that respect, protect and promote the fulfilment of human rights, including the fundamental freedoms and principles of equality and non-discrimination as defined in human rights frameworks, as well as the more specific right to privacy and other data-related rights, and data-specific rights promulgated in applicable data protection legislation and other applicable regulation.[53]

People-Centered and Inclusive
Affected populations should be afforded an opportunity to be included, represented, and empowered to exercise agency throughout data management whenever the operational context permits. Special efforts should be made to support the participation and engagement of people who are not well represented and may be marginalized in the data management activity at hand (e.g., due to age, gender and other diversity factors such as disability, ethnicity, religion, sexual orientation or other characteristics), or are otherwise 'invisible', consistent with commitments to leave no one behind. A people-centered and inclusive approach is particularly important in the development of context-specific norms and standards for data management.

Personal Data Protection
Humanitarian organizations have an obligation to adhere to (i) applicable national and regional data protection laws,[54] 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.[55] These laws and policies contain the list of legitimate bases for the processing of personal data, including but not limited to consent.[56] 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 inclusivity and respect for human rights, they should ensure the rights of data subjects to be informed about the processing of their personal data, and to be able to access, correct, delete, or object to the processing of their personal data.

[52] This includes that data management must be relevant, limited and adequate to the intended purpose of data management, which for non-personal data in a sensitive context must be in line with forthcoming administrative issuances for the organization related to data protection and privacy.

[53] As part of the United Nations Secretariat, OCHA enjoys privileges and immunities which entail that national and regional legislation on the handling of data do not apply.

[54] As part of the United Nations Secretariat, OCHA enjoys privileges and immunities which entail that national and regional legislation on the handling of data do not apply.

[55] OCHA must always manage personal data in accordance with applicable guidance, including forthcoming administrative issuances for the organization related to data protection and privacy and the Personal Data Protection and Privacy Principles, which should serve as a foundational framework for the processing of personal data by UN entities.

[56] For more information on processing of personal data and the use of 'consent' as a legitimate basis in humanitarian response, see the ICRC Handbook on Data Protection in Humanitarian Action (2nd edition, 2020).

Quality
Data quality should be maintained such that users and key stakeholders are able to trust operational data management and its resulting products. Data quality entails that data is relevant, accurate, timely, complete, up-to-date and interpretable, in line with the intended use and as appropriate within the given 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
Sensitive data should only be retained for as long as it is necessary to the specified purpose for which it is being managed or as required by applicable law or donor audit regulations. When its retention is required, safe and secure storage should be ensured to safeguard sensitive data from being misused or irresponsibly exposed. All other data may be retained indefinitely, provided that its level of sensitivity is reassessed at appropriate moments, that access rights can be established, and – for anonymized or aggregate data – that a re-identification assessment is conducted. Regardless of the sensitivity level, a retention schema should indicate when data should be destroyed and how to do so in a way that renders data retrieval impossible. Specific durations for retention should be defined where possible and, where this is not the case, specific periods for review of necessity should be set.

Transparency
Data management in humanitarian response should be carried out in ways that offer meaningful transparency toward stakeholders, notably affected populations. This should include provision of information about the data management activity and its outputs, as well as data sharing in ways that promote genuine understanding of the data management activity, its purpose, intended use and sharing, as well as any associated limitations and risks.

ANNEX C

DATA RESPONSIBILITY IN OCHA'S DATA MANAGEMENT CYCLE

The table below provides a summary of the tips and outputs for data responsibility along the steps of a data management cycle as introduced on page 32. Tools to support responsible data management across the steps of a data management cycle are listed on the OCHA IMB SharePoint page on Technology Standards.

TIPS AND OUTPUTS FOR DATA RESPONSIBILITY ACROSS THE DATA MANAGEMENT CYCLE

STEPS IN THE DATA MANAGEMENT CYCLE	TIPS AND OUTPUTS FOR DATA RESPONSIBILITY
1. PLANNING This includes identifying and documenting the various components (e.g. data sources and flows, tools and capacities, etc.) that make up the data management activity, as well as assessing impact and taking risk mitigation measures.	**TIPS** ☐ Complete a data impact assessment for the activity. ☐ Ensure the availability of required infrastructure. ☐ Use Standard Operating Procedures. ☐ Take additional precautions for data management activities involving the management of sensitive data. **OUTPUTS** ☐ A completed data impact assessment. ☐ A data sharing agreement, Standard Operating Procedure and/or Terms of Reference, including a Data Retention and Destruction Schedule.
2. COLLECTING, RECEIVING AND STORING This entails the collection, receipt and storage of data.	**TIPS** ☐ Confirm the sensitivity level of data before collection or receipt. ☐ Use secure tools and channels. ☐ Store data responsibly. ☐ Take additional precautions for the management of personal data or non-personal data in a sensitive context. **OUTPUTS** ☐ The required data for the data management activity.
3. ASSURING QUALITY This entails data cleaning and documenting limitations and caveats in line with relevant SOPs and standards.	**TIPS** ☐ Clean data using methods and tools appropriate to the activity and in-line with relevant criteria. ☐ Document all limitations or caveats. **OUTPUTS** ☐ Datasets ready for sharing and/or analysis, including metadata.
4. SHARING This involves sharing data privately with partners or making it available publicly for open access.	**TIPS** ☐ Select a responsible approach to sharing based on the relevant ISP or other applicable guidance. ☐ Use data sharing agreements and licenses. ☐ Provide metadata. ☐ Take additional precautions when sharing sensitive data. ☐ Log data sharing in the data asset registry. **OUTPUTS** ☐ Responsibly shared data. ☐ Entry on data sharing in data asset registry.

5. ANALYZING This focuses on the extraction of information as required for the development of information products.	**TIPS** ☐ Ensure clear documentation of methods used. ☐ Prevent exposure of sensitive data during analysis or visualization. ☐ Take extra precautions when using advanced analytical methods. **OUTPUTS** ☐ Charts, graphs or maps displaying information, accompanied by appropriate documentation.
6. PRESENTING This involves incorporating insights from the data into internal or public information products and websites.	**TIPS** ☐ Include context and data sources in published products. ☐ Ensure appropriate approval before release and select an appropriate license. **OUTPUTS** ☐ Responsibly published information products.
7. RETAINING AND DESTROYING This entails keeping data available for future use, or ensuring the removal of data in a way that renders retrieval impossible.	**TIPS** ☐ Assess the potential future value of data. ☐ Balance the risk and utility of data. ☐ Select the right means for long-term storage. ☐ Regularly reassess the sensitivity level of the data retained. ☐ Ensure effective destruction of data. **OUTPUTS** ☐ Securely retained datasets. ☐ Effectively destroyed datasets, with clear documentation of this step and the datasets concerned.
8. EVALUATING This entails internal review of the data management activity or joint review with partners as appropriate.	**TIPS** ☐ Include data responsibility considerations in any evaluation exercise conducted for the activity. ☐ Communicate the use of data with stakeholders. ☐ Record any data incidents that occurred throughout the activity. **OUTPUTS** ☐ Finalized data management activity with documentation of any data incidents.

ANNEX D TEMPLATES FOR DATA RESPONSIBILITY

The following templates are designed to support adoption of the OCHA Data Responsibility Guidelines. Some of the templates are OCHA-specific while others are drawn from the IASC Operational Guidance on Data Responsibility in Humanitarian Action.

Templates from the IASC Operational Guidance:

- Data Responsibility Diagnostic (System-Wide Level)
- Data Ecosystem Map and Asset Registry Template
- Information Sharing Protocol (including Information and Data Sensitivity Classification)
- Standard Operating Procedure for Data Incident Management

Templates specific to OCHA:

- Data Responsibility Diagnostic (Office Level)
- Data Impact Assessment
- Data Asset Registry
- Data Sharing Agreement
- Data Incident Registry

ANNEX E

FOUNDATIONS FOR DATA RESPONSIBILITY AT OCHA

Data management within OCHA is guided directly and indirectly by a variety of instruments. The Guidelines complement and are informed by the existing documents listed here.

Legal framework:

UN General Assembly, 1945. Charter of the United Nations: https://www.un.org/en/about-us/un-charter.

UN General Assembly, 1948. Universal Declaration of Human Rights: https://www.un.org/en/about-us/universal-declaration-of-human-rights.

UN 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.

Existing guidance from the UN Secretariat:

UN, 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.

UN 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.

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

UN Office of Information Communication Technology (OICT). Technical Guidance on Information Security: https://iseek-external.un.org/department/policies.

UN Office for the Coordination of Humanitarian Affairs (OCHA), Policy Instruction on Technology Standards, https://unitednations.sharepoint.com/sites/OCHAHub/IMB%20Resources/Forms/AllItems.aspx?id=%2Fsites%2FOCHAHub%2FIMB%20Resources%2FShared%20Documents%2FOCHA%20Policy%20Instruction%20on%20Technology%20Standards%20%2D%20September%2-02021%2Epdf&parent=%2Fsites%2FOCHAHub%2FIMB%20Resources%2FShared%20Documents.

UN Secretariat, 2004. Secretary-General's Bulletin on the Use of Information and Communications Technology Resources and Data, ST/SGB/2004/15: https://undocs.org/pdf?symbol=en/st/sgb/2004/15.

UN 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.

UN Secretariat, 2010. UN Information Sensitivity Toolkit: http://dag.un.org/handle/11176/387401.

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

Inter-Agency Standing Committee guidance:

Inter-Agency Standing Committee (IASC), 2021. Operational Guidance on Data Responsibility in Humanitarian Action: https://interagencystandingcommittee.org/system/files/2021-02/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action-%20February%202021.pdf.

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

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.

ANNEX F ADDITIONAL RESOURCES

Humanitarian-specific sector guidance:

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 (Kelly Church) and Linda Raftree, 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.

CHS 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.

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

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://elan.cashlearning.org/.

European Union, 2018. General Data Protection Regulation (GDPR): https://eur-lex.europa.eu/eli/reg/2016/679/oj.

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

Grand Bargain Working Group on Workstream 5, co-convened by ECHO and OCHA, 2019: https://interagencystandingcommittee.org/grand-bargain-official-website/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.

ICRC-led Advisory Group incl. DRC on "Professional Standards", 2018. Professional Standards for Protection Work; Chapter 6: Managing Data and Information for Protection Outcomes: https://reliefweb.int/sites/reliefweb.int/files/resources/0999_002_Protection_web.pdf.

International Conference on Data Protection and Privacy Commissioners, 2009. Madrid Resolution: International Standards on the Protection of Personal Data and Privacy: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf.

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: Do_No_Harm_ChecklistandGuidingQuestionsforDTMandPartners.docx.

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.alnap.org/help-library/irc-research-toolkit-obtaining-meaningful-informed-consent.

Médecins Sans Frontières, 2013. Data Sharing Policy: https://fieldresearch.msf.org/bitstream/handle/10144/306501/MSF+data+sharing+policy+final+061213.pdf?sequence=1.

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

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

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

Oxfam, 2017. Responsible Data Management Training Pack: https://policy-practice.oxfam.org/resources/responsible-data-management-training-pack-620235/.

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

Protection Information Management (PIM) Initiative, 2015. PIM Principles: http://pim.guide/guidance-andproducts/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.

USAID, 2019. Considerations for Using Data Responsibly at USAID: https://www.usaid.gov/responsibledata.

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.

Additional UN guidance:

UN 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.

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

UN 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.

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

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

UNICEF, 2015. Procedures for Ethical Standards in Research, Evaluation, Data Collection and Analysis: https://www.unicef.org/media/54796/file.

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.

UNICEF/GovLab, 2019. Responsible Data for Children Synthesis report: https://rd4c.org/files/rd4c-reportfinal.pdf.

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

UNHCR, 2018. Guidance on the Protection of Personal Data of Persons of Concern to UNHCR: https://www.refworld.org/docid/5b360f4d4.html.

UN 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-ProtectionLaws.aspx.

UN 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.