OCHA DATA RESPONSIBILITY GUIDELINES

MAR 2019

WORKING DRAFT

THE CENTRE FOR HUMANITARIAN DATA

OCHA

centre for humdata

TABLE OF CONTENTS

PREFACE

The OCHA Data Responsibility Guidelines (the Guidelines) offer a set of principles, processes and tools that support the safe, ethical and effective management of data in humanitarian response.

The core audience for the Guidelines is OCHA staff involved in managing humanitarian 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 and research conducted by OCHA over the past several years:

- In 2016, OCHA partnered with the NYU Governance Lab (GovLab) and Leiden University to understand the policy and privacy landscape, and to understand related best practice of partner organizations. The results of this research pointed to the need for a new framework that could balance the benefits and risks of data and could assist humanitarian organizations and others to develop responsible approaches to data.

- In a survey conducted by the Centre for Humanitarian Data (the Centre) in March 2018 among OCHA staff working with information and/or data, less than 20% of respondents indicated that their Offices and Sections have guidance for handling personal or sensitive data. The absence of adequate guidance for data processing in general and for sensitive humanitarian data in particular may create significant risks for affected people and other stakeholders in humanitarian response efforts.

- In field research conducted in 2018, the Centre worked with OCHA field offices to better understand how sensitive data is shared and used by OCHA staff and humanitarian partners in conflict environments. The research focused on different types of risks and threats related to humanitarian data and how to mitigate potential harms to affected people and aid workers.

The Guidelines are released in working draft in March 2019, after which the Centre for Humanitarian Data will facilitate targeted field support in at least 3 pilot country offices, to guide colleagues in the implementation of the Guidelines. These pilots will allow for structured feedback and revision of the working draft based on hands-on experience, ensuring that the Guidelines are fit for the purpose of guiding responsible data management throughout the organization.

STRUCTURE OF THE GUIDELINES

The Guidelines contain six substantive 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 outlines the scope of issues that the Guidelines are designed to cover.

Section 2: Foundations for Data Responsibility at OCHA presents an overview of existing guidance, and their influence on the development of the Guidelines. In addition, this section introduces a set of foundational principles meant to inform the implementation of the Guidelines and responsible data practice in the humanitarian sector more broadly.

Section 3: Data Responsibility Across the Data Management Process is the most practical portion of the Guidelines. It offers a concrete set of key actions, outputs, and tools for data responsibility at each step in the data management process.

Section 4: Accountability outlines the key roles and responsibilities for ensuring the uptake and implementation of the Guidelines. It also introduces the Data Responsibility Advisory Group, a cross-functional structure to monitor and support data responsibility across OCHA.

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

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

Annex C - Data Responsibility Advisory Group ToR outlines the key objectives, composition, and main activities of the Data Responsibility Advisory Group (DRAG) established in the Guidelines.

HOW TO USE THE GUIDELINES

The Guidelines offer an overall approach and minimum standard for data responsibility across OCHA. Because levels of data responsibility vary considerably across functions and response environments, use of the Guidelines will take a variety of different forms. The table below offers some basic recommendations for effective use of the Guidelines in different common scenarios in which OCHA staff manage data.

Scenario	How to use the Guidelines
New response environment	In a new response environment, staff have the opportunity to embed data responsibility in different data management exercises from the outset. For staff helping to establish a new response, emphasis should be placed on the Fundamentals outlined in section 3.1 of the Guidelines. Getting these different fundamental pieces in place early will set a high standard for data responsibility in the response and position OCHA as a key facilitator of inter- and intra-cluster / sector data management.
Existing response environment with no established measures for data responsibility	In some response environments, there may be no clearly established measures for data responsibility -- such as Information Sharing Protocols or Standard Operating Procedures. In such contexts, staff have two options for starting to use the Guidelines: 1. Start with the Fundamentals, such as a response-level Information Sharing Protocol including a Sensitivity Classification, then build down to the different, specific data management exercises led or coordinated by OCHA 2. Start improving one specific data management exercise, then work towards applying the Fundamentals to the response at large When starting with a specific exercise, focus first on completing a Data Responsibility Plan, even if a data management process is already underway.
Existing response environment with some established measures for data responsibility	Most protracted crisis environments where OCHA operates will have at least some measures for data responsibility in place. In such contexts, staff should use the Key Actions and Outputs table in Section 3 for an initial 'self-assessment' of what pieces are in place and what pieces are missing. Then, prioritize the steps in the data management process with the fewest actions and related outputs in place in order to improve data responsibility across the exercise or context in question.

Global or regional teams leading or supporting humanitarian data management activities	Staff at Headquarters and in regional offices working on data management can make use of the Guidelines as follows: • Unless there is already a Data Responsibility Plan in place for the specific exercise, develop one as a first step • Next, conduct a self-assessment for the activity of focus to determine the areas where more action is needed to ensure data responsibility, using the Key Actions and Outputs checklist • Review the existing documentation and guidance for the data management exercise in question and identify steps in the existing workflow where actions for data responsibility can be taken

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.

ACRONYMS

3W	Who is doing What, Where?
4W	Who is doing What, Where, When?
CBPF	Country-Based Pooled Funds
DII	Demographically Identifiable Information
DPIA	Data Protection Impact Assessment
DRAG	Data Responsibility Advisory Group
EU	European Union
GDPR	General Data Protection Regulation
HNO	Humanitarian Needs Overview
HPC	Humanitarian Programme Cycle
HRP	Humanitarian Response Plan
IASC	Inter-Agency Standing Committee
ICRC	International Committee of the Red Cross
ICT	Information and Communications Technology
IM	Information Management
IMWG	Information Management Working Group
ISP	Information Sharing Protocol
MSNA	Multi-Sector Needs Assessment
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
OICT	Office of Information and Communications Technology
OLA	Office of Legal Affairs
PPG	Privacy Policy Group
SOP	Standard Operating Procedure
UNHCR	United Nations High Commissioner for Refugees

1. INTRODUCTION

1.1 DATA RESPONSIBILITY IN HUMANITARIAN ACTION

Data is a critical component of humanitarian response. The management of digital data relating to crisis contexts, affected people and humanitarian response operations allows the humanitarian community to respond in a more effective and efficient manner. However, as organizations process increasingly large volumes of data, they also face more complex challenges and risks with managing and using this data.

Irresponsible or inappropriate processing of data in humanitarian contexts 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 -- data that is likely to lead to harm when exposed. While personal data can categorically be considered sensitive, more nuanced issues arise for non-personal data. For example, locations of medical facilities in conflict settings can expose patients and staff to risk, even if this data is not personal.

The technical tools and methods for managing data have evolved faster than the institutional policy instruments and guidelines that govern their use. While significant efforts have been made in recent years to improve data governance in different contexts, these efforts have focused primarily on promoting data protection and privacy as opposed to more comprehensive responsible data management.

1. 'Building Data Responsibility into Humanitarian Action' OCHA Think Brief (2016).

2. 'Mapping and Comparing Responsible Data Approaches', NYU GovLab, Leiden University (2016).

The need for **data responsibility** has now been recognized by a wide variety of organizations, both within and outside the humanitarian space. Data responsibility goes beyond the concepts of "data privacy" and "data protection". It **entails a set of principles, processes and tools that support the safe, ethical and effective management of data in humanitarian response.**[1] Whereas many humanitarian organizations have developed policies and guidelines focused on the management of personal data,[2] guidance has been lacking on how to ensure data responsibility in the management of other forms of humanitarian data such as survey results and datasets containing information that could be used to target individuals in conflict areas. The OCHA Data Responsibility Guidelines aim to fill this gap.

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 work is mainly focused on aggregation and analysis for the wider humanitarian community.

In most response contexts, United Nations (UN) and non-governmental organization (NGO) partners collect 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.

Given this primary role as an aggregator in humanitarian data management, OCHA must be clear about the type of data it manages and is responsible for. The Data Responsibility Guidelines focus on data that is directly relevant to humanitarian work. Management of other data by OCHA, such as human resources and financial data, is regulated by existing Secretariat and OCHA guidance.[3]

3. See Section 2.1 on Existing Guidance, and https://centre.humdata.org/data-policy.

For the purpose of the Guidelines, humanitarian data is understood as:

1. Data about the context in which a humanitarian crisis is occurring (e.g., baseline/development data, damage assessments, geo-spatial data);
2. Data about the people affected by a crisis and their needs; and
3. Data about the response by organizations and people seeking to help.

Sensitive data is defined as data that, if disclosed or accessed without proper authorization, is likely to cause:

- harm (such as sanctions, discrimination, and security threats) to any person, including the source of the information or other identifiable persons or groups; or
- a negative impact on an organization's capacity to carry out its activities or on public perceptions of that organization.[4] Data from these different categories will have varying levels of sensitivity depending on the context.

4. International Committee of the Red Cross, "Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence," 2018. Available here: https://shop.icrc.org/professional-standards-for-protection-work-carried-out-by-humanitarian-and-human-rights-actors-in-armed-conflict-and-other-situations-of-violence-2540.html.

The table below presents a model for information and data sensitivity classification to be used in the implementation of the Guidelines. Staff may further adapt this model to fit their context.

Information and Data Sensitivity Classification

Sensitivity	Definition	Information and Data Sensitivity Classification
Low or No	Information or data that, if disclosed or accessed without proper authorization, are unlikely to cause any harm or negative impacts to affected people and/or humanitarian actors.[5]	**Public**
Moderate	Information or data that, if disclosed or accessed without proper authorization, are likely to cause minor harm or negative impacts and/or be disadvantageous for affected people and/or humanitarian actors.	**Restricted**
High	Information or data that, if disclosed or accessed without proper authorization, are likely to cause serious harm or negative impacts to affected people and/or humanitarian actors and/or damage to a response.[6]	**Confidential**
Severe	Information or data that, if disclosed or accessed without proper authorization, are likely to cause severe harm or negative impacts and/or damage to affected people and/or humanitarian actors and/or impede the conduct of the work of a response.[7]	**Strictly Confidential**

5. Relatedly, SG bulletin defines "unclassified" data and information as follows: "information or material whose unauthorized disclosure could reasonably be expected not to cause damage to the work of the United Nations."

6. Relatedly, the SG Bulletin defines "information or material whose unauthorized disclosure could reasonably be expected to cause damage to the work of the United Nations."

7. Relatedly, the SG Bulletin defines classified information as "information or material whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to or impede the conduct of the work of the United Nations."

OCHA also plays a critical role in coordinating humanitarian data management activities across a diverse group of stakeholders. With more actors bringing their resources to bear on a crisis response, the hub and spoke model of coordination is shifting 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. In the age of digital data, this 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.

Although the Guidelines are most relevant for staff who work directly with data, all staff have a role to play in ensuring the responsible use of data given the cross-cutting nature of OCHA's work.

1.3 SCOPE OF THE GUIDELINES

The Guidelines focus on all humanitarian data managed directly by OCHA, processed on OCHA's behalf, or processed by humanitarian actors coordinated by OCHA in different contexts. OCHA's "corporate" data, including data related to internal financial management, human resources & personnel, and other administrative functions are not covered by the Guidelines. For example, data generated internally by Umoja is not covered by the Guidelines, while data from the Country-Based Pooled Funds (CBPF) is covered.

Examples from each category of humanitarian data include the following:

Category of humanitarian data	Examples of data covered by the Guidelines
Data about the context in which a humanitarian crisis is occurring	• Secondary data feeding into Humanitarian Needs Overviews (HNOs) • Administrative boundaries • Locations of schools, health facilities and other infrastructure • Humanitarian access data • Development data • Political and socio-economic data
Data about the people affected by the crisis and their needs	• Needs assessment data • Population figures • Movement data • Locations of affected people
Data about the response by organizations and people seeking to help those who need assistance	• 3W and 4W data • Community perception data • Data feeding into Humanitarian Response Plans (HRPs) • Data feeding into Periodic Monitoring Reports • Cash and aid distribution locations • Humanitarian financing data • Financial tracking data

The Guidelines apply to data that is publicly available as well as data to which access is restricted. OCHA and its partners may restrict access to data for a variety of reasons, including sensitivity, intellectual property, or insufficient quality, among others. Regardless of whether such restrictions are in place, the Data Responsibility Guidelines still apply.

The Guidelines apply to all data management exercises conducted directly by OCHA or on OCHA's behalf. They should also inform data management activities that are directly coordinated by OCHA. The core audience for the Guidelines is OCHA staff involved in managing humanitarian data across OCHA's core functions of coordination, advocacy, policy, humanitarian financing and information management, with a primary focus on the field. OCHA should also promote the practices and tools outlined in the Guidelines amongst implementing partners involved in different stages of the data management process.

2. FOUNDATIONS FOR DATA RESPONSIBILITY AT OCHA

Data management within OCHA is currently guided directly and indirectly by a variety of instruments. These instruments are primarily focused on concepts of privacy, security and the protection of personal data. While these instruments do not explicitly call for 'data responsibility', they have informed different elements of the Guidelines and the overall thinking on how OCHA can practice responsible data management. This section provides a brief summary of the different foundational documents and how they contribute to the Guidelines.

2.1 OVERVIEW OF EXISTING GUIDANCE

Instrument	Summary and impact on OCHA Data Responsibility Guidelines
Legal framework	
Charter of the United Nations June 26th, 1945	The foundational document of the United Nations. The provisions of the Charter are to be observed in all activities conducted by or on behalf of the UN. The UN Charter is available here: http://www.un.org/en/sections/un-charter/un-charter-full-text/
Universal Declaration of Human Rights, December 10th, 1948	The primary purpose of the Guidelines is to provide protection in accordance with the rights and protections of affected people enshrined in international humanitarian law and the UDHR, including the right to privacy. The UDHR is available here: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217(III)
General Assembly Resolution 46/182, December 19th, 1991	The foundational document for OCHA's mandate and all OCHA activity, including data management, is grounded in the clauses contained in this Resolution, including importantly the Humanitarian Principles. The resolution is available here: http://www.un.org/documents/ga/res/46/a46r182.htm

Relevant existing guidance within the UN Secretariat	
Code of Conduct for the International Civil Service, July 2013	A key behavioral and ethical guide for all conduct of UN employees, including data management. The Code of Conduct is available here: http://www.un.org/en/ethics/pdf/StandConIntCivSE.pdf
Secretary-General's Bulletin on Record-Keeping and the Management of United Nations Archives, ST/SGB/2007/5, February 12th, 2007	This bulletin sets out the rules and procedures to be followed in respect of the creation, management and disposition of records, electronic records, archives and non-current records of the United Nations. The bulletin contains specific responsibilities related to records management for UN staff, departments and offices, and the UN Archives and Records Management Section. This bulletin helped define the record keeping requirements for data determined in the Guidelines under the 'retention and destruction' section. The bulletin is available here: https://undocs.org/ST/SGB/2007/5
Secretary-General's Bulletin on Information Sensitivity, Classification and Handling, ST/SGB/2007/6, February 12th, 2007	This bulletin is aimed at ensuring the classification and secure handling of confidential information entrusted to or originating from the United Nations. The classification schema contained in this bulletin helped inform the data sensitivity assessment and classification included in the Guidelines. The bulletin is available here: http://undocs.org/ST/SGB/2007/6
UN Information Sensitivity Toolkit, February 24th, 2010	This toolkit, used in conjunction with training, provides the requirements and means for staff members to manage sensitive records to ensure protection of the confidentiality and integrity of information contained therein, thereby meeting the requirements of ST/SGB/2007/6 on Information Sensitivity, Classification and Handling. The content of this toolkit helped

	develop the Data Sensitivity Classification component of the Information Sharing Protocol template annexed to this policy. The Information Sensitivity Toolkit is available here: https://archives.un.org/sites/archives.un.org/files/RM-Guidelines/information_sensitivity_toolkit_2010.pdf
Secretary-General's Bulletin on the Use of Information and Communications Technology Resources and Data, ST/SGB/2004/15, November 29th, 2004	This bulletin was developed for the purposes of defining the proper use of information technology and related resources and data, and of ensuring the security and technical integrity of the system. The bulletin provides instructions for appropriate use of UN ICT systems. The instructions on appropriate behaviour relating to ICTs helped frame the instructions for responsible behaviour relating to data throughout the Guidelines. The monitoring and investigation sections in the bulletin helped shape the oversight mechanism contained in the Guidelines. The bulletin is available here: https://undocs.org/ST/SGB/2004/15
General Assembly Resolution on Guidelines for the Regulation of Personalized Data Files, A/RES/45/95, December 14th, 1990	This resolution contains a set of 10 principles to guide the processing of personal data. These principles helped shape and adapt the principles contained in this document. The resolution is available here: http://www.refworld.org/pdfid/3ddcafaac.pdf
UN Office of Information Communication Technology technical guidance	Finally, the Office of Information Communication Technology (OICT) developed detailed technical guidance on information security, including the 'Minimum Security Requirements for Public Websites of the United Nations ICT Technical Procedure' and 'Access Control for the United Nations Secretariat ICT Technical Procedure'. An overview is available here (for those with access to iSeek): https://iseek-external.un.org/department/policies

Additional UN guidance	
United Nations Development Group - Data Privacy, Ethics and Data Protection	This document sets out general guidance on data privacy, data protection and data ethics for the United Nations Development Group (UNDG) concerning the use of big data. The document is available here: https://undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf
Inter-Agency Standing Committee guidance	
IASC Policy on Protection, October 14th, 2016	This policy upholds the centrality of protection in humanitarian response. It provided the framework for the Guidelines to further protect the rights of individuals in humanitarian data management by and for OCHA. The policy is available here: https://interagencystandingcommittee.org/protection-priority-global-protection-cluster/documents/inter-agency-standing-committee-policy
IASC Operational Guidance On Responsibilities Of Cluster/Sector Leads & OCHA In Information Management, December 4th, 2008	The Guidelines build on the responsibilities specified in this IASC guidance document. The IASC Operational Guidance is available here: https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/IASC_operational_guidance_on_information_management.pdf
Humanitarian-specific sector guidance	
The Humanitarian Charter and Minimum Standards in Humanitarian Response (Sphere), May 2018	These documents constitute the core sources of guiding considerations regarding quality and accountability in humanitarian response, which translate to data responsibility standards across the Guidelines. The protection principles -- in particular the 'do no harm' principle -- and Sphere Core Standard helped shape the Principles for Data Responsibility in Humanitarian Response included in the Guidelines.

	The Charter and Minimum Standards are available here: http://www.spherehandbook.org
The Core Humanitarian Standard, December 12th, 2014	This standard is another widely accepted source of guidance for the sector. While not data-specific, the CHS influenced the foundational principles and the overall approach to defining professional and protective practice throughout this document. The Core Humanitarian Standard is available here: https://corehumanitarianstandard.org/files/files/Core%20Humanitarian%20Standard%20-%20English.pdf

Beyond the instruments summarized above, the Guidelines are informed by the Protection Information Management initiative workshops hosted by the Danish Refugee Council, UNHCR and OCHA over the course of 2017 and 2018.[8]

Regional and national privacy and data protection frameworks, such as the EU General Data Protection Regulation (GDPR) which came into effect in May 2018, served as another source of inspiration in drafting the Guidelines.

Although the GDPR is not directly applicable to the work of OCHA given OCHA's privileges and immunities as part of the UN Secretariat, it still highly relevant for two key reasons. Firstly, the GDPR provides a high standard of practice that serves to inform the content of the Guidelines. Second, OCHA constantly interfaces with organizations that are subject to GDPR, and these organizations are only allowed to transfer personal data to OCHA under specific conditions. For this reason, several organizations have already requested data transfer agreements and data processing agreements. In considering such agreements, OCHA is indirectly impacted by GDPR.

A full list of relevant frameworks is available upon request from the Centre for Humanitarian Data.

8. Find more information on the Protection Information Management (PIM) initiative here: https://pim.guide/.

2.2 LIMITATIONS IN EXISTING GUIDANCE

While relevant to some of the challenges common to data processing activities within OCHA, the existing guidance is not tailored specifically to OCHA's role in humanitarian response. For example, while instructive as overall frameworks for professional conduct in the humanitarian sector, Sphere and the CHS do not provide explicit guidance on data responsibility. In addition, existing guidance does not provide the level of detail and specificity to OCHA's functions that is needed to support responsible data processing by OCHA staff. For example, these documents tend to focus on privacy infringement and personal data protection, while leaving other risks associated with data processing in humanitarian response unaddressed.

For OCHA, guidance is most needed for the management of non-personal but still sensitive humanitarian data. For example, when managing data on critical infrastructure such as hospital locations in conflict areas, data protection and privacy law will not provide some lessons will be valuable guidance since it is focused on protecting the rights of data subjects. The Guidelines therefore cover a broader scope of data.

2.3 PRINCIPLES FOR DATA RESPONSIBILITY IN HUMANITARIAN RESPONSE

The following Principles have been adapted from the UN Privacy Policy Group (PPG) Principles,[9] as well as the Humanitarian Principles, Sphere and the Core Humanitarian Standard. **The Principles for Data Responsibility in Humanitarian Response** are meant to serve as a benchmark for the processing of non-personal data, particularly in sensitive contexts that may put certain individuals or groups of individuals at risk of harms.

9. The UN Privacy Policy Group is led by UN Global Pulse and the Office for Information and Communication Technology. The PPG Principles were developed through a joint process involving 32 UN organizations over the course of 2017 and 2018 and were formally adopted by the UN High-Level Committee on Management in October 2018. The PPG Principles were designed to be adapted to UN entities specific requirements. They are available here: https://www.unsceb.org/privacy-principles.

FAIR AND LEGITIMATE PROCESSING OF DATA

OCHA should process humanitarian data in a fair manner, in accordance with our mandates and governing instruments, including the Humanitarian Principles, and on the basis of any of the following: (i) the consent of a data subject; (ii) the best interests of a data subject, consistent with the OCHA's mandates; (iii) OCHA's mandate and governing instruments, or; (iv) any other legal basis specifically identified by OCHA.

PURPOSE SPECIFICATION

Humanitarian data should be processed for specified purposes, which are consistent with OCHA's mandate and take into account the balancing of relevant rights, freedoms and interests. Humanitarian data should not be processed in ways that are incompatible with such purposes.

NECESSITY, RELEVANCY AND ADEQUACY OF DATA PROCESSING

The processing of humanitarian data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of humanitarian data processing.

RETENTION

Humanitarian data should be retained as long as reasonably possible. Sensitive humanitarian data should only be retained for the time that is necessary for the specified purpose.

ACCURACY
Humanitarian data should be accurate and, where necessary, up to date to fulfil the specified purposes.

CONFIDENTIALITY
Humanitarian data should be processed with due regard to confidentiality.

SECURITY
Appropriate organizational, administrative, physical and technical safeguards and procedures should be implemented to protect the security of humanitarian data, including against or from unauthorized or accidental access, damage, loss or other risks presented by data processing.

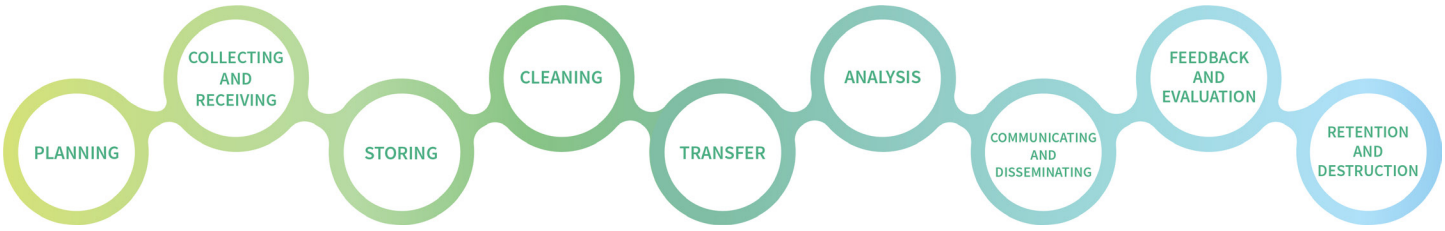
TRANSPARENCY
Processing of personal data should be carried out with transparency to data subjects, as appropriate and whenever possible. This should include, for example, provision of information about the processing of humanitarian data as well as information on how to request access, verification, rectification, and/or deletion of that humanitarian data, insofar as the specified purpose for which humanitarian data is processed is not frustrated.

DATA TRANSFERS
In carrying out its mandated activities, OCHA may transfer humanitarian data to a partner, provided that, under the circumstances, OCHA satisfies itself that the partner affords appropriate protection for the humanitarian data. A written agreement between OCHA and the partner to specify the conditions for the transfer should be concluded where appropriate.

ACCOUNTABILITY
OCHA should have adequate policies and mechanisms in place to adhere to these Principles.

3. DATA RESPONSIBILITY ACROSS THE DATA MANAGEMENT PROCESS

Across different functions and response contexts, the **data management process** within OCHA consists of the following common steps.[10]



- Planning
- Collecting and Receiving
- Storing
- Cleaning
- Transfer
- Analysis
- Communicating and Disseminating
- Feedback and Evaluation
- Retention and Destruction

10. There are a variety of data cycles and processes used in documentation from OCHA's different functions. As the steps and processes (and related terminology) for data management vary slightly across OCHA, this overall data management process is used as a structure for the Guidelines to ensure that all key actions taken with data are addressed. This may evolve or expand over time depending on demand and need from OCHA staff and partners.

The Guidelines are structured around these nine steps as this allows for more granular and actionable guidance for OCHA staff. While not all data projects will go through all of the above steps, this process provides a comprehensive overview of all steps that could be relevant. This means that guidance for individual steps may be used independently and steps do not necessarily need to follow each other.

The table below provides a summary of the **key actions for data responsibility** related to each step. Many of these actions will already be familiar to staff. For example, Information Sharing Protocols are frequently used in responses for which the cluster system is activated. And for many data management exercises, Standard Operating Procedures will already exist. In such cases, only a review of these existing assets is required. For cases where no asset exists yet, the Guidelines contain easy-to-use templates that can be quickly filled out to meet the data responsibility criteria.

The subsequent sections of the Guidelines provide more detail on these actions and offer practical tools for completing them across the range of scenarios within which OCHA manages humanitarian data. In particular, developing the **Data Responsibility Plan** is essential for a clear understanding of required capacities and resources, and to identify potential design or process flaws.

KEY ACTIONS & OUTPUTS FOR DATA RESPONSIBILITY IN THE DATA MANAGEMENT PROCESS	
Steps in the Data Management Process	**Key Actions and Outputs for Data Responsibility**
<u>Fundamentals</u> While getting the Fundamentals for data responsibility in place is not a step in the data management process itself, it is included in this overview as an essential preparatory component of data responsibility across the Humanitarian Programme Cycle.	**Fundamentals to get into place:** ☐ Data ecosystem map ☐ Information Sharing Protocol ☐ Tools for data management ☐ Required skills and training
Planning This step involves developing a plan for the data management exercise in question. This includes identifying and documenting the various components (e.g. data sources and flows, tools and capacities, etc.) that make up the exercise, as well as assessing and devising mitigation measures for risks related to the same.	**Actions:** ☐ Complete a Data Responsibility Plan (DRP) for the exercise *NB: If the details included in the DRP template are already addressed in another document (e.g. the Terms of Reference for an MSNA exercise in a particular country context), simply make a note of this and proceed to the next step* **Outputs:** ○ Data Responsibility Plan
Collecting and Receiving This step clarifies what primary and secondary data OCHA will collect and how that data will be assessed and received. OCHA frequently receive transfers of humanitarian data from partners.	**Actions:** ☐ Ensure compliance with relevant data standards and protocols ☐ Determine whether the data needs to be received ☐ Receive sensitive data in a secure manner ☐ Determine the accuracy and integrity of the data received ☐ Manage microdata using Statistical Disclosure Control ☐ In cases where OCHA needs to conduct primary data collection, take measures to prevent duplication, enhance data quality, and ensure protection of sensitive humanitarian data ☐ When managing microdata (individual survey results), take measures such as running Statistical Disclosure Control (SDC) to mitigate risk

	Outputs: ○ Datasets that are compliant with all relevant standards and protocols
Storing This step includes storage of data on OCHA's physical or cloud-based infrastructure.	**Actions:** ☐ Confirm and monitor the level of data protection required ☐ Select the appropriate means for data storage ☐ Assign and monitor adherence to access conditions ☐ Store sensitive humanitarian data appropriately **Outputs:** ○ Storage infrastructure in place and ready for use, in compliance with requirements and access conditions
Cleaning This step entails cleaning data, e.g. correcting errors, adding missing values, and standardizing data	**Actions:** ☐ Ensure that methods and tools utilized in data cleaning meet the relevant criteria for the activity in the context ☐ Remove sensitive data if it is not required for the data management exercise ☐ Document all limitations or caveats **Outputs:** ○ Cleaned and standardized datasets ready for transfer and/or analysis, provided with limitations and caveats documentation
Transfer This step involves sharing data privately with partners or making it available publicly for open access.	**Actions:** ☐ Review and adhere to the relevant ISP for instructions on who the data can be shared with and at what level of disaggregation ☐ Conduct a due diligence assessment in cases where data is transferred to private sector partners or unknown entities. ☐ Ensure that data transfer agreements or licenses are in place and adhered to where required ☐ Select an appropriate method for transfer ☐ Provide metadata ☐ Take additional precautions when transferring sensitive humanitarian data **Outputs:** ○ Methods for secure and responsible data transfer established and in use by all relevant actors ○ Data transfer agreements (where needed)

Analysis This step focuses on statistical or spatial analysis of data that is presented using charts, graphs or maps.	**Actions:** ☐ Ensure clear documentation ☐ Don't expose sensitive data during analysis or visualization ☐ Take extra precautions when using advanced analytical methods ☐ Review the analysis methodology, outcome and documentation **Outputs:** ○ Charts, graphs or maps displaying information, accompanied by appropriate documentation
Communicating and Disseminating This step involves sharing the data through information products and websites.	**Actions:** ☐ Include context and data sources in published products ☐ Ensure appropriate approval before release and select an appropriate license ☐ Prevent further exposure **Outputs:** ○ Published information products
Feedback and Evaluation This step involves reflection of the overall data management process and solicitation of feedback from partners and audiences on what can be improved.	**Actions:** ☐ Complete an evaluation ☐ Communicate the use of data with stakeholders ☐ Record critical incidents **Outputs:** ○ Completed Data Responsibility Plan Evaluation Sheet
Retention and Destruction This step involves destroying or storing data, as appropriate.	**Actions:** ☐ Assess the potential future value of the data ☐ Select the right means for storage ☐ Regularly reassess the sensitivity level of the data retained ☐ Balance the risk and utility of data ☐ Ensure effective destruction of data **Outputs:** ○ Datasets selected for retention stored securely ○ Datasets selected for destruction effectively destroyed, with clear documentation of this step and the datasets concerned

KEY ACTIONS & OUTPUTS FOR DATA RESPONSIBILITY IN THE DATA MANAGEMENT PROCESS

Fundamentals

FUNDAMENTALS TO GET INTO PLACE:

- Data Ecosystem Map
- Information Sharing Protocol
- Tools for data management
- Required skills and training

STEPS IN THE DATA MANAGEMENT PROCESS

PLANNING

ACTIONS
- Complete a Data Responsibility Plan (DRP) for the exercise

OUTPUTS
- Data Responsibility Plan

COLLECTING AND RECEIVING

ACTIONS
- Ensure compliance with relevant data standards and protocols and comply with relevant data
- Determine whether the data needs to be received
- Receive sensitive data in a secure manner
- Determine the accuracy and integrity of the data received
- Manage microdata using Statistical Disclosure Control
- In cases where OCHA needs to conduct primary data collection, take measures to prevent duplication, enhance data quality, and ensure protection of sensitive humanitarian data
- When managing microdata (individual survey results), take measures such as running Statistical Disclosure Control (SDC) to mitigate risk

OUTPUTS
- Datasets that are compliant with all relevant standards and protocols

STORING

ACTIONS
- Confirm and monitor the level of data protection required
- Select the appropriate means for data storage
- Assign and monitor adherence to access conditions
- Store sensitive humanitarian data appropriately

OUTPUTS
- Storage infrastructure in place and ready for use, in compliance with requirements and access conditions

CLEANING

ACTIONS
- Ensure that methods and tools utilized in data cleaning meet the relevant criteria for the activity in the context
- Remove sensitive data if it is not required for the data management exercise
- Document all limitations or caveats

OUTPUTS
- Cleaned and standardized datasets ready for transfer and/or analysis, provided with limitations and caveats documentation

TRANSFER

ACTIONS
- Review and adhere to the relevant ISP for instructions on who the data can be shared with and at what level of disaggregation
- Conduct a due diligence assessment in cases where data is transferred to private sector partners or unknown entities.
- Ensure that data transfer agreements or licenses are in place and adhered to where required
- Select an appropriate method for transfer
- Provide metadata
- Take additional precautions when transferring sensitive humanitarian data

OUTPUTS
- Methods for secure and responsible data transfer established and in use by all relevant actors
- Data transfer agreements (where needed)

ANALYSIS

ACTIONS
- Ensure clear documentation
- Don't expose sensitive data during analysis or visualization
- Take extra precautions when using advanced analytical methods
- Review the analysis methodology, outcome and documentation

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

COMMUNICATING AND DISSEMINATING

ACTIONS
- Include context and data sources in published products
- Ensure appropriate approval before release and select an appropriate license
- Prevent further exposure

OUTPUTS
- Published information products

FEEDBACK AND EVALUATION

ACTIONS
- Complete an evaluation
- Communicate the use of data with stakeholders
- Record critical incidents

OUTPUTS
- Completed Data Responsibility Plan Evaluation Sheet

RETENTION AND DESTRUCTION

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

OUTPUTS
- Datasets selected for retention stored securely
- Datasets selected for destruction effectively destroyed, with clear documentation of this step and the datasets concerned

3.1 FUNDAMENTALS

Data responsibility begins with the selection or development of a set of fundamental assets ("Fundamentals"). These Fundamentals should ideally be established at the outset of a crisis response, and most OCHA offices already have many of these in place. In protracted crisis contexts, offices may wish to update and adapt these Fundamentals as the crisis evolves.

In addition to supporting data responsibility in OCHA's own data management activities, the Fundamentals contribute to OCHA's engagement with IASC members for inter-agency coordination. Specifically, they help clarify services that OCHA and partners commit to, potential joint-initiatives, and new data and information sharing agreements in a given context.

Data Ecosystem Map
This provides an overview of what data processing is taking place in the context concerned, by OCHA or by other actors. This will help speed up the development of plans for acquiring the data needed for different data management exercises, whether through primary collection or by receiving data from a partner organization. A template for a Data Ecosystem Map is available here.

Information Sharing Protocol
An Information Sharing Protocol (ISP) for the response establishes clear standards, approaches, and roles and responsibilities for information sharing across different functions and activities. Establishing this early in a crisis response can help socialize a responsible data approach in different clusters or sectors and with different partner organizations.

A strong ISP helps OCHA and its partners prepare for the exchange of data through pre-established procedures while preventing last-minute negotiations about transfers or, equally problematic, potentially irresponsible transfers without any type of agreement in place. It also provides clear guidelines for sensitivity assessment and classification of different types of data in the context. A template for a response-level ISP is available here.

An ISP specific to a data management activity, such as a needs assessment, may also be developed in cases where more detailed guidance is needed or new partners are involved. However, staff should prioritize the establishment of a response-level ISP covering all data management exercises in the context before developing more activity-specific protocols.

Tools for data management
OCHA uses a variety of tools and accompanying guidance to support effective and efficient data management for the execution of specific functions (e.g. the IM Toolbox). The call-out boxes about 'Tools' in each section below should serve as a quick reference for colleagues looking to identify and deploy technologies in support of responsible data practice, and are meant to complement the function-specific toolboxes wherever available.

3.2 PLANNING

The first step in any data management process should be planning, which includes identifying and documenting the various components (e.g. data sources and flows, tools and capacities, etc.) that make up the exercise. Data responsibility in the planning step involves identifying potential risks, devising risk mitigation measures, and identifying/scoping requirements for effective and safe data processing activities. The primary output of this step is a **Data Responsibility Plan template**, which can be filled out through the actions outlined below.

Describe the value
Describing the value of the data management exercise in concrete terms helps uphold the purpose specification principle. In turn, it helps staff identify the time and resources required for a particular activity, obtain management approval, and balance expected benefits against risks. The value of a data processing exercise can be determined by identifying the information gap that the project aims to fill and the decisions that the information will inform or influence. This relates directly to OCHA's efforts to adopt a more targeted and demand-driven approach to data management by clarifying the information needs of key clients, the problems they are trying to solve, and the questions they are trying to answer.

Articulate the scope and volume
Articulating the required scope and volume of humanitarian data to be collected or received helps determine associated risks. It also helps to review what data management exercises are required, especially when sensitive humanitarian data is involved. The description of the scope and volume should be as specific and detailed as possible. Make sure to cross-check the different data types against any established Sensitivity Classification that may be part of an Information Sharing Protocol established for the context, to determine where extra precautions may be required.

Map the flow of data
Mapping the flow of data is critical to establishing a common understanding of how different types of data will be processed throughout the course of the activity, as well as which individuals and/or organizations will be involved at the different stages. The flow map also helps identify the resources and technical capacities required. Finally, it allows for thorough Risk and Benefit Assessment (RBA), described in more detail below. A template for this mapping exercise is included in the Data Responsibility Plan.

Identify and define the risks
Risks in data processing may include potential harm to affected populations, safety or security risks for humanitarian workers, and infringements on rights, to name a few. This assessment should be based on context-specific input from relevant experts. Staff should refer to any established Sensitivity Classification that may be part of an Information Sharing Protocol established for their particular context to help define risks related to the different types of data in question.

Identify risk mitigation measures
Maintaining a clear list of risks and related mitigation measures is a critical action for ensuring data responsibility throughout an activity. Risk mitigation measures can be procedural or technical. Especially for technical risk mitigation and security, consultation with relevant experts may be required. In cases where no clear mitigation measures are available, consult with office management to determine whether the activity should still be reasonably carried-out.

Determine the capacities required
Different exercises will require a mix of technical, strategic, and analytical expertise. This may include, for example, assigning or bringing on a team member with a deep understanding of the risks related to needs assessment data. Resource and capacity constraints can create delays and even risks throughout the data management process. If an office does not have certain required resources to responsibly deliver an activity, staff should take steps to obtain these resources or adjust the project accordingly.

Use Standard Operating Procedures
It is common practice for OCHA offices to establish internal and external Standard Operating Procedures (SOPs) for different activities, from contact management to implementation of a multi-sector needs assessment (MSNA) to producing a 4W. Data responsibility requires that these SOPs not only articulate clear procedures, roles and responsibilities, but also align with existing guidance, including global guidelines and ISPs at the Response and Cluster level. SOPs should also include clear accountability mechanisms and escalation paths for cases where a data breach or other critical incident occurs. In cases where different stakeholders require validation, approval, or some other form of feedback or clearance before the release of data or a derivative information product, this should be clearly articulated in the SOP.

If primary data collection is required, take additional precautions
When collecting data directly from or about affected people and/or processing personal data, a separate set of specific risks need to be mitigated to ensure safe and effective data practice. Although OCHA does not typically engage in personal data processing, it does occur in certain contexts. In these cases, more rigorous measures including a Data Protection Impact Assessment (DPIA, which is a method to assess the impact of data processing on the protection of personal data and privacy) may be required. Staff should seek additional guidance beyond the Guidelines such as the ICRC & Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action. Additional resources are available here.

Recommended Tools for Data Responsibility in the Planning Step

Project management tools
Trello: https://trello.com
Atlassian: https://www.atlassian.com

Besides ease of use and personal preference of team members, data responsibility should be a key consideration when selecting the appropriate project management tool. Project plans will often contain attachments with, or link to, sensitive data and information. For online tools that allow public and restricted access, setting appropriate access permissions is critical.

Drafting tools
Google docs: https://www.google.com/docs/about/
Onedrive: https://support.office.com/en-gb/article/data-encryption-in-onedrive-for-business-and-sharepoint-online-6501b5ef-6bf7-43df-b60d-f65781847d6c

Because documents such as draft ISPs and SOPs and data ecosystem maps can contain sensitive information, it is important to use a trusted and secure tool and set appropriate access permissions when drafting them.

3.3 COLLECTING AND RECEIVING

This step outlines what primary and secondary data OCHA will collect or receive, and how that data will be assessed and received. OCHA frequently receives transfers of humanitarian data from a variety of different actors, including other International Organizations and Non-Governmental Organizations. Responsibly collecting and receiving data involves completing the actions outlined below.

Ensure compliance with relevant data standards and protocols
OCHA can support responsible practice internally and with its key counterparts by promoting a clear understanding of and compliance with relevant data standards and protocols by all actors.

Determine whether the data needs to be received
OCHA should only receive sensitive (including personal) humanitarian data if absolutely required for the fulfilment of its mission and in line with its mandate. If possible, receiving data at an aggregate level or receiving information derived from sensitive data is preferred to receiving raw sensitive data.

Receive sensitive data in a secure manner
Sensitive data should be transferred to OCHA in a manner that renders it accessible only to persons with the required access authorisation, in-line with the relevant ISP and SOP. Sensitive data should only be received through secure and encrypted file transfer services, for which requirements are defined in the 'Tools' box below. In cases where sensitive data is transferred to OCHA through insecure means, staff should notify the sender and reiterate the requirements for secure data transfers in the future.

Determine the accuracy and integrity of the data received
In line with the Principle on Data Accuracy, when receiving data, an appropriate metadata standard should be upheld to help determine the origin and other attributes of the data. Files should be inspected to determine that they have not been corrupted during the transfer and that no expected data is missing from the files.

Manage microdata using Statistical Disclosure Control
When receiving microdata (individual survey results), run a Statistical Disclosure Control (SDC) process to mitigate the risk of re-identification of respondents. One option for completing this process is sdcMicro,[11] a free and open source tool that allows users to assess the risk of re-identification of individual respondents, to decrease this risk by removing or altering values in a statistically correct manner and to measure the information loss caused by these edits. Reach out to the Centre for Humanitarian Data for support in determining the appropriate risk level for a given context, and to help strike the right balance between re-identification risk and information value.

11. sdcMicro and supporting documentation was developed by Statistics Austria, the Vienna University of Technology, the International Household Survey Network (IHSN) , PARIS21 (OECD), and the World Bank, provide instructions to conduct SDC.

Primary data collection
OCHA should only collect data directly from affected people if:

- The data collection effort is part of a coordinated needs assessment process,and;
- There is a significant need for this data to protect the life or vital interest of the affected people concerned, and;
- There is no other ongoing or scheduled effort to collect the data necessary to meet this need, and;
- OCHA has or can acquire the resources and capacity necessary for appropriate data collection under the circumstances of this specific case.

When OCHA does engage in primary data collection, or is in charge of overseeing a primary data collection exercise conducted by an implementing partner, staff should consult relevant sector guidance to ensure responsible practice. Some sectors, such as the Protection Sector, have clear and detailed guidance on the handling of sensitive information (e.g. *Professional Standards for Protection Work, Chapter 6*).[12] Beyond this, more general guidance, such as the ICRC and Brussels Privacy Hub *Handbook on Data Protection in Humanitarian Action*,[13] should serve as a key reference for OCHA staff in designing or managing primary data collection.

12. 'Professional Standards for Protection Work', Third Edition, ICRC (2018).

13. 'Handbook on Data Protection in Humanitarian Action' ICRC, Brussels Privacy Hub (2017).

Recommended Tools for Data Responsibility in the Collecting and Receiving Step

Secure Data Transfer
OneDrive: https://support.office.com/en-gb/article/data-encryption-in-onedrive-for-business-and-sharepoint-online-6501b5ef-6bf7-43df-b60d-f65781847d6c
Dropbox: https://www.dropbox.com/security
WeTransfer: https://wetransfer.zendesk.com/hc/en-us/categories/201270873-Security-Privacy

Statistical Disclosure Control
sdcMicro: http://surveys.worldbank.org/sdcmicro

Data Collection Tools that offer Encryption
KoBoToolbox: http://help.kobotoolbox.org/creating-forms/advanced/encrypting-forms
Open Data Kit: https://docs.opendatakit.org/security-privacy/
Guidance on selecting mobile data collection tools: https://digitalprinciples.org/resource/howto-choose-mobile-data-collection-plaform/

3.4 STORING

This step includes storage of data on OCHA's physical or cloud-based infrastructure. Responsible data storage requires appropriate storage facilities and accompanying technical resources. These requirements apply to physical and cloud-based storage of data within OCHA owned or managed infrastructure, including storage provided through third-party providers. Different data management activities require different types of storage and levels of security. Staff should ensure that the requirements for data storage identified in the Data Responsibility Plan are met and continue to be adhered to throughout the data management process.

Confirm and monitor the level of data protection required
The level of data protection required should be based on the sensitivity classification of the data that is being stored. The required infrastructure should be available and ready at the start of the data management process. When the context of the data management exercise changes, the sensitivity level of the data and the standards for appropriate storage may also change.

Select the appropriate means for data storage
Data may be stored in one of the following ways:

- Locally on an OCHA server, computer or laptop, or on an external storage device (e.g. hard-drive or flash-drive)
- Using commercially operated cloud storage such as Google Drive or iCloud
- On United Nations operated servers through OneDrive

In field locations, storing data on local infrastructure may risk loss or corruption of data. It is advised to store data on OCHA's OneDrive if possible, given the available connectivity and keeping in mind potential leaks of sensitive data. If use of OneDrive is not an option and data needs to be stored locally, follow the instructions for secure local storage provided below.

In cases where a project includes the development and/or ongoing management of a tool, platform or service by OCHA, additional considerations for hosting may apply. Consult the Digital Services Section for guidance on appropriate storage and access controls to such tools, platforms or services.

14. For specific guidance on setting up access controls, review Access Control for the United Nations Secretariat ICT Technical Procedure, OICT, November 2013.

Assign and monitor adherence to access conditions
Access to the data storage environment should be determined by the access conditions agreed by OCHA or humanitarian partners. This should ideally be specified in a Data Responsibility Plan.[14] This can also often mean that the data is made publicly available. In cases where OCHA is responsible for managing the data in question, access conditions should allow OCHA colleagues to delete or alter the data as required. This also means the data must be retrievable, for which good file and dataset management is critical. Instructions for good file and dataset management are available here: https://humanitarian.atlassian.net/wiki/spaces/imtoolbox/pages/61734950/File+and+Dataset+Management

Store sensitive humanitarian data appropriately
Humanitarian data that is classified as restricted, confidential or strictly confidential, must be stored in a manner that is compliant with relevant standards (including ST/SGB/2004/15 and ST/SGB/2007/06). Stored data should only be accessible to persons with the required access authorisation. Sensitive humanitarian data should not be stored using third party cloud storage services, unless:

- storage of the sensitive humanitarian data concerned is required in the interest of fulfilling OCHAs mission and mandate, and;
- time and resource constraints do not permit for storage of the data in the appropriate manner, and;
- the required urgency of data storage does not allow for the acquisition of additional resources to facilitate storage in the prescribed manner.

Recommended Tools for Data Responsibility in the Storing Step

For the storage of data files:

Commercially operated cloud storage
Google Drive: https://www.google.com/drive/
iCloud: https://www.icloud.com

Secure storage and hosting
OneDrive: https://onedrive.live.com/about/en-us/

Secure physical storage
Encrypted hard-drive: see for example https://www.cloudwards.net/how-to-encrypt-your-hard-drive/
File encryption: https://docs.microsoft.com/en-us/windows/desktop/fileio/file-encryption

3.5 CLEANING

Data cleaning entails such actions as correcting errors, adding missing values, and standardizing data. Protocols and standards for cleaning data may vary depending on the nature of the crisis and related sensitivity classification. If there is no established SOP and sensitivity classification to inform data cleaning exercises, OCHA should work with its counterparts to establish these instruments as a matter of urgency. In cases where no guidance is available, the content of this step should determine OCHA's default approach to this step of the data management process.

Ensure that methods and tools utilized in cleaning data meet the relevant criteria for the data processing activity in the context

Before cleaning data, staff should review the applicable guidance, including an SOP established in the Planning step outlined in the Guidelines and relevant global guidance, to ensure that they are aware of any restrictions to data cleaning.[15] It is important to ensure that risk mitigation measures are in place. This includes disaggregation of community-level data to an appropriate level. Methods for data cleaning may include the following:

- Downloading and using tools available in public Python or R libraries
- Applying Power Query or similar software to quickly correct errors
- Opening data in Microsoft Excel on a computer and checking manually
- Uploading data to cloud-based tools for cleaning (e.g. Google sheets; Tableau prep)
- Checking the values in the dataset against defined rules using an automated tool such as HDX Data Check

Remove sensitive data if it is not required for the data management exercise

In particular for data collected by OCHA, this is the step at which unnecessary sensitive data should be removed prior to transfer and/or analysis. There are various tools available to support the detection of sensitive (personal) data, such as Stealthbits and Spirion, included in the toolbox below.

For microdata (individual survey results), use a Statistical Disclosure Control (SDC) process to determine the risk of re-identification of respondents, and subsequently lower that risk to an acceptable level. The sdcMicro tool developed by the World Bank and accompanying guidance provide relevant information to conduct such a process.

Document all limitations or caveats

Staff responsible for data cleaning should record any gaps or flaws in the data, along with any other limitations or errors that occur during cleaning. This note should be attached to the data in a 'caveats' or 'limitations' section, either as metadata in the data file or as a written note in information products in which the data is used. Failure to note limitations or caveats may lead to erroneous conclusions being drawn from the data.

15. For example, the OCHA 'IM Toolbox' offers tutorials on CODs, Humanitarian ID, and GIS and Mapping data that include criteria for management and cleaning of these different datasets.

Recommended Tools for Data Responsibility in the Cleaning Step

Data cleaning
HDX Data Check: https://tools.humdata.org/wizard/datacheck/import

Local
Power Query: https://docs.microsoft.com/en-us/power-query/
Microsoft Excel: https://products.office.com/en/excel

Cloud-based
Google sheets: https://www.google.com/sheets/about/
Tableau prep: https://www.tableau.com/products/prep

Sensitive data detection tools
Stealthbits: https://www.stealthbits.com/sensitive-data-discovery-and-data-classification-software
Spirion: https://www.spirion.com/sensitive-data-discovery/
sdcMicro: http://surveys.worldbank.org/sdcmicro

3.6 TRANSFER

This step involves sharing data privately with partners or making it available publicly for open access. Data transfers occur frequently in a response. For example, an OCHA IMO in a Country Office transfers data when sharing a USB stick containing needs assessment data with a counterpart. Publishing data on HDX is another example of a data transfer.

Review and adhere to the relevant ISP for instructions on who the data can be shared with and at what level of disaggregation
If an ISP is in place for the response in which data is transferred, it will inform the appropriate method for transferring or publishing data. The ISP will also indicate the sensitivity of data on individuals or groups at different levels of aggregation and clarify when such data can be shared with specific audiences. In cases where there are no established ISPs, consult colleagues in the Information Management Working Group (IMWG) and relevant cluster or sector counterparts.

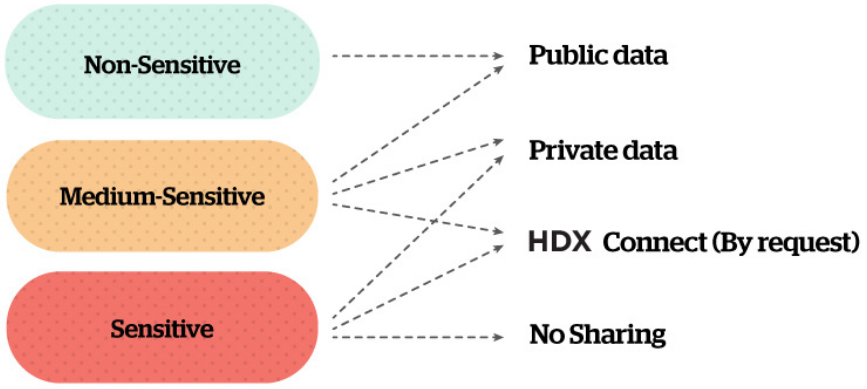
Data transfer agreements and licenses
Data transfer agreements are typically established in cases involving sensitive (e.g. personal data on affected populations) or proprietary data (e.g. commercial satellite imagery). These agreements should clearly specify the roles and responsibilities of the different parties involved and stipulate additional restrictions or protective measures on how the data is processed and shared. Different types of data transfer agreements will be needed depending on the type of data, the applicability of regional and national laws, and the actors involved. Reach out to the Centre for Humanitarian Data for support in developing such an agreement.

When transferring data, staff should observe any restrictions specified in the relevant license(s). Any licenses added to datasets or information products should remain attached to such resources throughout the data management process. For more information on commonly used data licenses, refer to the Data Licenses page on HDX.

Select an appropriate method for transfer
Select the method that suits the needs for the data transfer in question, keeping in mind the context and sensitivity of the data. With the exception of clearly-identified sensitive datasets, OCHA will share humanitarian data on the Humanitarian Data Exchange (HDX), either as the source of the data or as a contributor of the data on behalf of the source. In some cases, the relevant ISP and transfer or processing agreements may offer various methods for data transfer.

One example of different methods for transfer based on a sensitivity classification is seen in the categorization used on the Humanitarian Data Exchange, pictured below.

For more information, see a blogpost on the different ways to share data on HDX: https://centre.humdata.org/three-ways-to-share-data-on-hdx/



Provide metadata
Metadata allows the recipient of the data to assess the data, which helps prevent misinterpretation and drawing false conclusions. The original source of the data should be appropriately credited when data is shared onwards. For more guidance on appropriate metadata, refer to the HDX Guide to Metadata.

Take additional precautions when transferring sensitive humanitarian data
OCHA should only transfer sensitive humanitarian data if absolutely required for the fulfilment of its mandate. If possible, receiving data on an aggregate level or receiving information derived from sensitive data is preferred to receiving raw sensitive data. In most cases, staff are working with non-sensitive data which can be shared openly and without any transfer agreement in place.

Sensitive humanitarian data classified as restricted, confidential or strictly confidential should only be shared with partner organizations or individuals if these have been assessed to uphold data responsibility standards similar or equal to those provided in the Guidelines. A data transfer or data processing agreement should always be in place in such cases. In cases where the urgency of data transfer is too high to conduct an assessment of the counterpart's data responsibility standards, a benefit-risk assessment should determine whether the data should be shared.

Sensitive humanitarian data should be shared in a manner that renders it accessible only to those with the required access authorisation. This includes the use of secure transfer mechanisms, such as encrypted email, or features like HDX Connect, through which organizations can publish metadata without sharing the underlying data, and subsequently manage access to the underlying data by request.

Recommended Tools for Data Responsibility in the Transfer Step

Data publication
Humanitarian Data Exchange: https://data.humdata.org/

Secure file transfer method
OneDrive: https://support.office.com/en-gb/article/data-encryption-in-onedrive-for-business-and-sharepoint-online-6501b5ef-6bf7-43df-b60d-f65781847d6c
Dropbox: https://www.dropbox.com/security
WeTransfer: https://wetransfer.zendesk.com/hc/en-us/categories/201270873-

Security-Privacy
Encrypted email: https://www.cloudwards.net/how-to-encrypt-your-emails/

3.7 ANALYSIS

This step focuses on statistical or spatial analysis of data that is presented using charts, graphs or maps. Data responsibility in the analysis step involves securing necessary technical and analytical expertise, defining and adhering to consistent analytical methods, and identifying and openly acknowledging any limitations in the analysis.

Ensure clear documentation
The result of an analysis and/or visualisation project will depend to a great extent on choosing the right method and tool to reach the intended outcome. Documentation should include the origin of the data used, the processes and tools used for analysis, and gaps or flaws in the data. This is critical for future reproducibility and to determine the reliability of results.

Don't expose sensitive data during analysis or visualization
Preventing the exposure of sensitive humanitarian data or information during or after analysis and/or visualisation is critical. This includes conducting analysis of sensitive humanitarian data within a secure environment and only by individuals authorized to access the data. Be sure to review interactive visualizations to ensure the insights do not reveal sensitive data, e.g. by a specific survey question having less than e.g. by showing a low number of respondents for a survey question in a specific location.

Take extra precautions when using advanced analytical methods
When employing advanced data science, artificial intelligence, machine learning or similar techniques, staff should consult relevant technical experts and materials to identify extra precautions for responsible data processing. Reach out to the Centre for Humanitarian Data for further guidance.

Review the analysis methodology, outcome and documentation
After the analysis has been completed, it is useful to reflect on the methodology used and the outcome it produced, and to document these results for the 'Feedback and Evaluation' step. A template to record these results is provided in Annex A of the Guidelines.

Recommended Tools for Data Responsibility in the Analysis Step

Secure cloud analytics
Tableau: https://onlinehelp.tableau.com/current/server/en-us/security_net.htm
ESRI ArcGIS: https://support.esri.com/en/technical-article/000017037
Power BI: https://powerbi.microsoft.com/en-us/

Data visualisation
For non-sensitive data, use HDX Quick Charts: https://tools.humdata.org/wizard/

3.8 COMMUNICATING AND DISSEMINATING

This step involves sharing data through information products and websites. Dissemination of sensitive data to the wrong audience can create risk to affected people and other stakeholders. For this step, data responsibility involves upholding standards for accurate and appropriate representation of data and taking specific measures to prevent exposure of sensitive data.

Include context and data sources in published products
Results from humanitarian data processing presented in OCHA information products should be accompanied by adequate contextual information to mitigate risk of misinterpretation of data. The original source of data should always be appropriately referenced. Information products should not violate any use licenses under which data was originally shared by the source.

Ensure appropriate approval before release and select an appropriate license
Prior to publication, ensure all data within the information product is suitable and approved for public dissemination. This may entail sharing a finished information product with data providers for approval before release, or communicating with relevant national authorities for validation of key figures before publication of a report. Accountabilities and requirements for approval of information products should be understood at the outset of a data management exercise. See "Planning" above for more information on this subject.

If there is no license already attached to the data, select a license from available Creative Commons licenses or elsewhere, or create a new license. More guidance on licenses is available here: **https://data.humdata.org/about/license**

Prevent further exposure
In cases where highly sensitive data has been processed to generate a particular information product, ensure that the release of the product does not pose any new or additional risks to the population of concern or to humanitarian actors themselves.

Recommended Tools for Data Responsibility in the Communicating and Disseminating Step

Data and Information Sharing Platforms
HDX: https://data.humdata.org/
HDX Connect: https://centre.humdata.org/a-new-call-to-action-sharing-the-existence-of-data/
Reliefweb: https://reliefweb.int
HumanitarianResponse: https://www.humanitarianresponse.info
Humanitarian InSight: https://www.hpc.tools
HNO websites such as https://hno-syria.org

See the 'Transfer' step for guidance on tools for sharing sensitive data.

Public Websites
In cases where public websites are used to communicate and disseminate final information products, refer to OICT guidance for Minimum Security Requirements for Public Websites of the United Nations ICT Technical Procedure.

3.9 FEEDBACK AND EVALUATION

This step involves reflection of the overall data management process and solicitation of feedback from partners and audiences on what can be improved.

Complete an evaluation
Staff can use the evaluation sheet in the Data Responsibility Plan to reflect on the data management process. This includes evaluation of the capacities and resources used, the scope and volume of the data that was processed, and whether any risk mitigation measures were taken. This exercise helps support individual and organizational learning. Incorporate good practice into existing or new ISP(s) and SOP(s) for improved data management in the future.

Communicate the use of data with stakeholders
Wherever feasible, the use of data and the final information product(s) should be communicated back to the original data source or data contributor. This process helps data providers to adjust their collection efforts to better align with the different uses of the data and gives data providers an opportunity to ask questions about the way in which their data was processed, analyzed, and communicated.

Record critical incidents
Critical incidents should be recorded as they happen during the data management process. At the end of the data management process, review all critical incidents have been thoroughly documented.

Recommended Tools for Data Responsibility in the Feedback and Evaluation Step
Feedback and evaluation record keeping OneDrive: https://onedrive.live.com/about/en-us/

3.10 RETENTION AND DESTRUCTION

This step involves storing or destroying humanitarian data, in-line with the data retention specifications agreed for a specific activity. Following the retention principle, humanitarian data should be retained as long as its foreseeable potential value outweighs risks associated with retention. Sensitive data should only be retained for the time that is necessary for the specified purpose.

Assess the potential future value of the data
Non-sensitive humanitarian data that is reasonably likely to be of future value to OCHA or partners should be retained by OCHA and be kept accessible for as long as reasonably possible. At a minimum, non-sensitive humanitarian data should be retained as long as needed for monitoring and evaluation of processing, and for donor reporting and other accountability purposes.

Select the right means for storage
Even when stored digitally, data risks degradation. Ensure that the means of storage protect the current state of the data, and do not endanger future integrity or accessibility. This may mean investing additional resources to obtain adequate storage facilities.

Regularly reassess the sensitivity level of the data retained
The sensitivity of non-sensitive data can evolve as new complementary data sources and new analytical tools emerge. To ensure that data is retained or destroyed as appropriate, the Sensitivity Classification in an ISP applicabe in the context concerned should be reapplied regularly to retained data. In addition, the Sensitivity Classification may also need to be updated over time, e.g. in cases where the operational context significantly changes or in cases where a response operation is completed or closed and overall responsibility for certain data assets is transferred from one organization to another.

Balance the risk and utility of data
Determine the balance between sensitivity, potential future value of the data and value loss that would be created if the data is destroyed, by applying the Risk and Benefit Assessment tool. Before deciding to destroy sensitive data, it should be clear how valuable and how sensitive the data is. Also, it should be clear how hard it would be to regain the value lost by destruction. Based on these variables, the appropriate decision to (securely) retain or destroy the data should be made.

Data that is considered sensitive based on a Sensitivity Classification applicable to the context should only be kept for as long as needed to serve the purpose(s) for which it was collected or received. If sensitive humanitarian data is expected to be needed for other compatible purposes after completion of the project, make sure that the data is rendered less sensitive by removing unnecessary information.

Ensure effective destruction of data
Simply deleting files and emptying the trash may not be enough to appropriately destroy data from devices. Make sure to use a ‘disk sanitization’ or ‘disk wipe’ tool to completely destroy the data. Suggestions for tools are provided in the tools box below.

Recommended Tools for Data Responsibility in the Retention and Destruction Step

Data destruction tools
DBAN: https://sourceforge.net/projects/dban/
CBL Data Shredder: http://www.cbldatarecovery.com/data-shredder/
MHDD: http://hddguru.com/software/2005.10.02-MHDD/
Further information on 'Media Sanitization' can be found here: https://iseek-external.un.org/system/files/oict_guideline_for_information_media_sanitization.pdf

4. ACCOUNTABILITY

The Guidelines are to be followed by all OCHA staff and supporting personnel (e.g. contractors, stand-by partners, and secondments), who are authorized to manage humanitarian data and related resources across the organization. Although effective implementation of the Guidelines requires action from all OCHA staff, accountability for adherence to the Guidelines rests with senior managers at Headquarters and Field Office level.

The **Chief of the Information Management Branch (IMB) and Lead for the IM Function is accountable for the adoption of the Guidelines and their implementation across the organization**.

The Centre for Humanitarian Data will convene a cross-functional **Data Responsibility Advisory Group (DRAG)** to track and support the implementation of the Guidelines and monitor critical incidents. The DRAG will bring together representatives from OCHA's branches and functions on a regular basis to monitor and examine practices around implementation, challenges, breaches and related concerns. The Centre will serve as the Secretariat for the DRAG. The Terms of Reference for the DRAG are included in Annex B of this document.

Every six months, the **Chief of IMB will submit a report to the Assistant Secretary-General (ASG)** on progress in the implementation of the Guidelines as well as any critical incidents related to data management.

At the global level, all **Function Leads, and Branch or Section Chiefs** whose teams manage humanitarian data, are responsible for ensuring implementation of the Guidelines. For example, the Lead for the Centre for Humanitarian Data is responsible for ensuring data responsibility in all aspects of the Humanitarian Data Exchange, e.g. preventing sensitive data from being shared on the platform.

At the field-level, **Heads of Office (HoO)** are responsible for ensuring adherence within their office. This means that, for example, the HoO for a Country Office that processes sensitive data should make sure that the required infrastructure for secure processing is in place.

Unit Heads are responsible for ensuring the appropriate application of the Guidelines in OCHA's day-to-day data management work. For example, when a new data management process is started, the Head of the Unit managing the data should be aware of the ensure that a Data Responsibility Plan is prepared before the process begins.

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

Group / Unit	Responsibilities
Chief of IMB and head of IM Function	• Provide semi-annual report on implementation of the Data Responsibility Guidelines to the ASG
Functional Leads, Directors and Branch Chiefs	• Promote staff awareness of and familiarity with the Guidelines. • Conduct an assessment of the effectiveness of the implementation of the Guidelines after two years. • Take corrective action and making related resources available for the management of critical 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 in the data ecosystem. • Systematically report any critical incidents to the Data Responsibility Advisory Group for tracking and support.
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 critical incidents to the Data Responsibility Advisory Group
Centre for Humanitarian Data	• Chair the Data Responsibility Advisory Group • Provide ongoing support for adoption of the Guidelines

Please see the section below on **Services to Support Implementation** for support provided to fulfil this set of responsibilities.

5. SERVICES TO SUPPORT IMPLEMENTATION OF THE GUIDELINES

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

Introductory briefing
The Centre will provide introductory webinars to offices or staff 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 (see Section 3) as they manage data. 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, facilitating conversations and workshops with OCHA staff and partners on issues related to data responsibility. The mission scan 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 will develop a training curriculum on data responsibility skills for OCHA and partners. The format of trainings will vary based on the needs of the requesting office and availability of the Centre team.

EXAMPLES OF POTENTIAL SUPPORT FROM THE CENTRE ACROSS THE DATA MANAGEMENT PROCESS		
Stage	**Scenario**	**Potential Support from the Centre**
Planning	An OCHA country team is working to develop a Data Responsibility Plan for the Multi-Sector Needs Assessment and the HNO and HRP. Given the large number of stakeholders involved, the office is looking for guidance on how best to develop this plan and ensure that it responds to the needs and requirements of the different stakeholders, while also upholding the OCHA Data Responsibility Guidelines.	The Centre could potentially (a) review the draft plan and provide remote feedback; (b) remotely participate in a Q&A session with the IMWG and Sector / Cluster Leads on the draft plan; or (c) conduct an in-country support mission to facilitate a workshop for OCHA and its counterparts in order to draft and finalize the Data Responsibility Plan and other related templates for this exercise.
Collecting and Receiving	OCHA is preparing to receive needs assessment data from a variety of sources, without the ability to determine the sensitivity level of the data in advance. The Head of Office is concerned that although the office is prepared to receive public data as required for the project, the available infrastructure may expose sensitive data to unauthorised access.	The Centre could (a) remotely help in developing communications with the counterparts assisting them in conducting a sensitivity assessment prior to transfer, or (b) advising on the technical requirements of additional infrastructure to appropriately handle sensitive data.
Storing	OCHA is asked to store sensitive humanitarian data on behalf of different cluster partners as part of a needs assessment exercise. While OCHA identified the related risks and proposed mitigation measures for this activity in its Data Responsibility Plan, it is uncertain as to whether the available storage infrastructure is sufficient to meet the data protection requirements.	The Centre could provide remote support and technical guidance to relevant OCHA colleagues in reviewing technical requirements, assessing the selected storage solution, and recommending additional safeguards (technical and operational) to ensure that the sensitive data is appropriately stored.

Cleaning	An OCHA IMO cleaning a dataset containing survey results is not sure whether any sensitive information is still contained in the dataset. Because the data pertains to a conflict setting, disclosure of the identity of survey respondents would lead to significant risk to affected people.	The Centre could provide support by (a) recommending a tool remotely, to assess the sensitivity of data or (b) conducting a data sensitivity assessment.
Transfer	A partner NGO has requested that OCHA share datasets, for which a data transfer agreement would be required. The Country Office handling the request worries that they do not possess the expertise or experience to establish such an agreement.	The Centre, in close consultation with the Office of Legal Affairs could support the development of a data transfer agreement with the NGO concerned by offering a template and modular clauses for the agreement to the office.
Analysis	An OCHA IMO is creating several data visualisations, and is worried that the software used to generate the visualisations may not be secure enough to process the data concerned.	The Centre can (a) provide remote advice to the IMO on the security requirements of the software given the sensitivity level of the data, and (b) point the IMO to software for which the security standards have been assessed and found appropriate for handling the data concerned.
Communica-ting and Disseminating	An OCHA Public Information Officer has prepared an internal document and receives a request for access from an NGO. The PIO is not familiar with the NGO and not sure whether the document should be shared, since it is based on sensitive data.	The Centre could provide case-specific advice to allow the communications officer to determine whether the document should be shared.

Feedback and Evaluation	The head of an IMU, who is tasked with evaluating a data management process, has encountered irresponsible use of data, not noticed during the project itself. Due to one organization's confusion over the sensitivity classification, sensitive data was shared with a broad audience and subsequently exposed to a malicious actor, that may have used it to plan an attack. The head of IMU is not sure whether and how to appropriately report this.	In this scenario, the Centre can support remotely by conducting a preliminary assessment of the breach and referring the head of IMU to the appropriate reporting channel. If the breach is considered significant, the Centre could deploy to provide further assistance on-the-ground if required. The Centre can also provide support to help prevent similar breaches from happening in the future.
Retention and Deletion	After the development of an HRP is completed, the responsible IMO is considering how to delete sensitive data that is no longer needed. Because the office has not processed sensitive data before, there is no standard process in place by which to destroy data.	When the Centre receives such a request, it could provide remote assistance by directing the IMO to a selection of tools that would be suitable for destroying the data concerned.

DEFINITIONS[16]

16. These definitions build primarily on the work of the UN Privacy Policy Group. In some cases, definitions were drawn from other relevant references, including regional legislation such as GDPR and selected OCHA and sector guidance documents.

Aggregate data: Accumulated data that is combined and organized into groupings or series at a broader level to that at which detailed observations are taken.

Biometrics: Techniques for measuring personal biological (anatomical or physiological) or behavioural characteristic which can be used to establish the identity of a natural person by comparing it with stored reference data. "Biometric identifiers" (BIs) are pieces of information that encode a representation of a person's unique human signatures (e.g. fingerprints, retinal scans or voice scans) which cannot be easily changed and can be electronically verified.

Community Identifiable Information: Data points that enable the identification, classification, and tracking of individuals, groups, or multiple groups of individuals by demographically defining factors. These may include ethnicity, gender, age, occupation, and religion. May also be referred to as Demographically Identifiable Information "DII."

Critical Incident: Any event in which a risk is caused to affected people, the organization and/or partners due to inappropriate management of humanitarian data.

Data: Facts and statistics collected together for reference or analysis.

Data analytics: The practice of examining data through qualitative and quantitative analysis and research to, for example, gain insights, identify behavioural patterns, draw conclusions, and/or improve decision making.

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 contributor: A person or organization that shares data with another party or platform.

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

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 processor: A person or organization that processes and adds value to raw data, e.g. by cleaning it, loading it into a searchable database, or combining it with data from other sources.

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. A DPIA would, for example, contain a general description of the envisaged system, project, policy or data transfer arrangement involving processing of personal data, an analysis of the risks to the rights of data subjects by virtue of the circumstances and the nature of the personal data processed, the safeguards, security and other measures in place or proposed to ensure the protection of the data.

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, including up to date nature of the data.

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.

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). Although data may also relate to organizations, rather than individuals, organizations would not be considered 'data subjects' under the recognized legal definition.

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.

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.

Humanitarian data ecosystem: A combined, dynamic overview of data processing activities, data flows and actors interacting with humanitarian data relating to a crisis or geographic area.

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

Microdata: Observation data on the characteristics of statistical units of a population, such as individuals, households, or establishments, collected by a census, survey, or registry.

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.

Re-identification: A process by which de-identified (anonymised) 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.

Risk Benefit Assessment: A process for identifying and balancing the benefits and risks related to the processing of data, as well as the likelihood, magnitude and severity of harms that can result from the identified risks in a particular context.

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.

Statistical Disclosure Control: Measures applied on data to eliminate (or reduce) the risk of disclosing information on the individual statistical units (respondents). These measures usually modify or restrict the amount of the data released.

Sensitive Data: Data with a high sensitivity level based on the magnitude and severity of potential harms and the likelihood of such harm materialising.

ANNEX A - TEMPLATES FOR DATA RESPONSIBILITY

This section brings together all templates referenced in the Guidelines.

- Data Ecosystem Map
- Information Sharing Protocol
- Data Responsibility Plan

DATA ECOSYSTEM MAP TEMPLATE

Click here to download an editable version of this template for use in your context. CLICK HERE

This Data Ecosystem Map template is designed for use by OCHA staff responsible for managing humanitarian data for a variety of different purposes. The template is meant to be adapted and tailored to specific contexts. If you want to receive support in drafting and/or reviewing your Data Ecosystem Map, contact the Centre for Humanitarian Data.

As the context evolves and new data sources and/or users emerge, refer back to this ecosystem map and update it to reflect these developments.

In order to create your Data Ecosystem Map, start by answering the following questions:

- What data assets are being managed in your context (e.g. Beneficiary lists, Needs Assessments, Humanitarian Access data, etc.)
- Who are the people/roles and organisations involved across the data management process for different activities (e.g. Information Management Officer, Content Expert, Data Provider, etc.)
- What are the relationships and roles that these actors have in the ecosystem (e.g. Regional Office as Facilitator, Humanitarian Coordinator as final sign-off, Data Sharing Partnerships with Implementing Partners, etc.)

Samples

Symbols	Entity or Object
	Infrastructure
	Data
	UN
	Other IO
N	NGO
	Civil Society
	Government
	Potential Transfer
	Data Transfer
	Vetted / Trusted / Secure

DATA ECOSYSTEM MAP TEMPLATE

Country / Context: _____ **Date Completed:** _____

INFORMATION SHARING PROTOCOL TEMPLATE

Click here to download an editable version of this template for use in your context. CLICK HERE

This Information Sharing Protocol (ISP) template is designed for use by OCHA staff and partners responsible for managing humanitarian data for a variety of different purposes. The template is meant to be adapted and tailored to specific contexts, and should be supplemented with additional directives and instructions as necessary (e.g. an additional section regarding data protection would be valuable in a Protection Sector ISP where highly sensitive personal data is being managed). If you want to receive support in drafting and/or reviewing your ISP, contact the Centre for Humanitarian Data.

INFORMATION SHARING PROTOCOL

[INSERT NAME OF COUNTRY AND/OR SECTOR / CLUSTER HERE]

[INSERT DATE HERE]

Background

This documents presents the information sharing protocol (ISP) for the [INSERT COUNTRY CONTEXT AND/OR NAME OF SECTOR / CLUSTER HERE]. It applies to all [SECTOR] actors, e.g.: [LIST ALL OF THE DIFFERENT TYPES OF ACTORS INVOLVED IN THE SECTOR + COORDINATION STRUCTURE].

The ISP is adapted from the ISP template provided in the OCHA Data Responsibility Guidelines.[1] It has been developed by [INSERT NAME OF COUNTRY AND/OR SECTOR / CLUSTER HERE] in accordance with IASC guidelines, which state that cluster/sub-cluster coordinators are responsible for generating up-to-date cluster specific information and sharing it with OCHA, in order to support inter-sector data sharing.[2] In this context, this ISP should be considered the primary document guiding data and information exchange for the purpose of humanitarian response.

1. [Insert link to public version of OCHA Data Responsibility Guidelines once released.]

2. IASC Operational Guidance on Responsibilities of Cluster/Sector Leads and OCHA in Information Management

The ISP is designed to establish a clear approach, standard, roles & responsibilities for information sharing across different functions and activities in the [COUNTRY NAME] response context.

Purpose of Information Sharing

[INSERT PURPOSE OF INFORMATION SHARING HERE]

The benefits of information sharing in this way include:

- [LIST BENEFITS OF SHARING INFORMATION IN THE PROPOSED WAY HERE. SUCH BENEFITS MAY INCLUDE THE FOLLOWING.]
- Better triangulation of information and corroboration of evidence
- Ability to provide regular, credible protection situation analysis, response monitoring, analysis and recommendations
- Improved inter-agency collaboration
- Strengthened operational coordination
- Improved protection and response to survivors and individuals at risk
- Conducting joint analysis

INFORMATION SHARING PROTOCOL TEMPLATE

Application and Scope
This ISP applies to [INSERT SECTOR/CLUSTER NAME] Coordinators, Information Management Officers, and other [INSERT SECTOR/CLUSTER NAME] Members involved in handling data and information at various stages of the humanitarian programme cycle.

The scope of the ISP is all humanitarian data and information generated and used in the response. For the purposes of this ISP, humanitarian data is defined as follows:

- Data and information about the context in which a humanitarian crisis is occurring (e.g., baseline/ development data, damage assessments, geo-spatial data);
- Data and information about the people affected by a crisis and their needs; and
- Data and information about the response by organizations and people seeking to help.

This ISP applies not only to finished information products but also to the underlying data used to generate such products.

Data Sensitivity
Data is considered sensitive based on the likelihood and severity of potential harm that may materialize as a result of its exposure in a given context. For example, the locations of medical facilities may be considered highly sensitive in an active conflict situation, whereas they should be actively and publicly shared in a typical natural disaster response.

Some types of data are categorically considered sensitive. These include:

- Personal data (e.g. name, phone number, national identity number, date of birth
- Disaggregated (household-level) assessment data
- Unprocessed Individual survey results (microdata)

Use the template below to formalize the criteria and parameters for a sensitivity assessment and classification in your context.

Information and Data Sensitivity in the [COUNTRY NAME] Context
Briefly describe considerations regarding information and data sensitivity specific to your context. Sample text is included below.

Data 'Sensitivity' Definitions
If there are already definitions of data and information sensitivity in your context, briefly describe these here. It is important to document the different definitions and understandings across sectors or clusters in your context to ensure that the overall definition of sensitive data and information is comprehensive and accurate to the operating environment.

Sensitive Data and Information
List the typical datasets and information products that are considered sensitive in your context. Sample text is provided below.

INFORMATION SHARING PROTOCOL TEMPLATE

For the purposes of this document, sensitive data and information are defined as data or information that, if disclosed or accessed without proper authorization, are likely to cause:

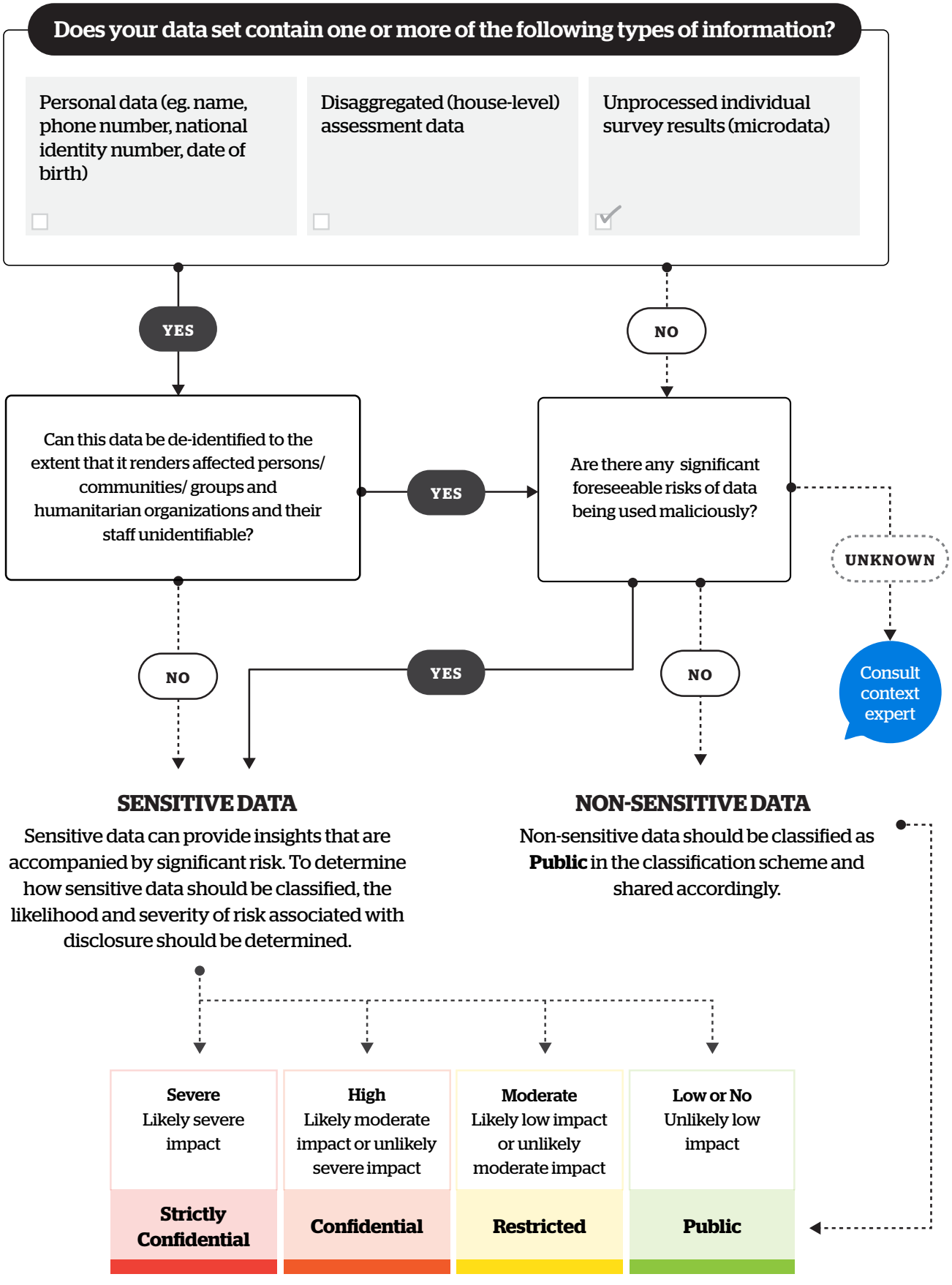
- harm (such as sanctions, discrimination, and security threats) to any person, including the source of the information or other identifiable persons or groups; or
- a negative impact on an organization's capacity to carry out its activities or on public perceptions of that organization.[3]

Given the highly context-specific nature of information sensitivity, It is not possible to propose a definitive list of the types of data or information that would be considered 'sensitive' across contexts. Nevertheless, there is a need to articulate and agree on the characteristics of different levels of sensitivity in order to then determine how information and data should be classified and subsequently shared. This means that there will always exist a certain degree of flexibility that the individual applying this classification mechanism will have to navigate based on their own experience and expertise. In case this flexibility provides an obstacle to decision-making, seeking advice from colleagues with complementary expertise and experience is recommended.

The first step in the application of this template instrument is determining the sensitivity level of the information or data concerned, based on the following decision tree. Sensitivity is determined as a factor of the likelihood and severity of harms and/or negative impacts resulting from data and information being disclosed or accessed without proper authorization.

3. International Committee of the Red Cross, "Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence," 2018. Available here: https://shop.icrc.org/professional-standards-for-protection-work-carried-out-by-humanitarian-and-human-rights-actors-in-armed-conflict-and-other-situations-of-violence-2512.html?__store=default

INFORMATION SHARING PROTOCOL TEMPLATE



INFORMATION SHARING PROTOCOL TEMPLATE

Data and Information Classification, Parameters for Disclosure, and Dissemination Methods
Under this ISP, data and information should be shared in-line with the parameters presented in the table below. As the sensitivity of data and information may change over time as the response context evolves, the [CLUSTER/SECTOR WORKING GROUP] will review and revise this table every [XX] months.

Information and Data Sensitivity Classification in the [Insert Context]

Sensitivity	Definition	Examples of potential harms or negative impacts	Information and Data Sensitivity Classification	Data and Information Types	Dissemination Methods
Low or No	Information or data that, if disclosed or accessed without proper authorization, are unlikely to cause any harm or negative impacts to affected people and/or humanitarian actors.	**Unlikely low impact**: When disclosing data aggregated at sub-district, district, governorate or national levels, there exists a minimal chance that affected people and/or humanitarian actors will be negatively affected.	**Public**	…… …… …… Examples may include: 3W/4W, HNO	…… …… …… ReliefWeb | HRInfo | HDX | other response-specific public sites etc.
Moderate	Information or data that, if disclosed or accessed without proper authorization, are likely to cause minor harm or negative impacts and/or be disadvantageous for affected people and/or humanitarian actors.	**Likely low impact:** Disclosure of the locations of boreholes could potentially lead to minor harm or negative impacts if shared publicly. **Unlikely moderate impact:** Disclosure of the number of and community-level locations of humanitarian partner staff could potentially lead to moderate harm or negative impacts if shared outside of humanitarian community.	**Restricted**	…… …… …… Aggregated survey results Examples may include: Mobility Tracking Figures, etc. NB: Depending on your context, additional data and information may be considered restricted. Be sure to reflect on and specify this when adapting the ISP.	…… …… …… HDX [via HDX Connect] | Hub-level mailing lists | intra-sector mailing lists etc.
High	Information or data that, if disclosed or accessed without proper authorization, are likely to cause serious harm or negative impacts to affected people and/or humanitarian actors and/or damage to a response.	**Likely moderate impact:** When a partner beneficiary list is disclosed, it is possible that affected people are stigmatized or discriminated against. **Unlikely severe impact:** If beneficiary lists containing personal information are disclosed, beneficiaries may be persecuted and imprisoned.	**Confidential**	…… …… …… Examples may include: Aid-Worker Contact Details / Lists, etc. NB: Depending on your context, additional data and information may be considered confidential. Be sure to reflect on and specify this when adapting the ISP.	…… …… …… HDX [via HDX Connect] | Internal intra-sector sharing only | Inter-sector sharing on case by case basis | etc.
Severe	Information or data that, if disclosed or accessed without proper authorization, are likely to cause severe harm or negative impacts and/or damage to affected people and/or humanitarian actors and/or impede the conduct of the work of a response.	**Likely severe impact:** If the precise names and locations of humanitarian workers were disclosed, this would very likely lead to physical harm, persecution, imprisonment or death of the staff members.	**Strictly Confidential**	…… …… …… Individual survey responses Personal data (i.e. beneficiary lists)[4], etc. NB: Depending on your context, additional data and information may be considered strictly confidential. Be sure to reflect on and specify this when adapting the ISP.	…… …… …… Bilateral disclosure between intra-sector partners

Agreed Principles and Commitments

- [LIST RELEVANT PRINCIPLES AND COMMITMENTS. SUCH PRINCIPLES AND COMMITMENTS MAY INCLUDE THE FOLLOWING.]
- Information and data should only be shared following the Principles for Data Responsibility in Humanitarian Response contained in the OCHA Data Responsibility Guidelines[5]
- Information should only be shared in accordance with the IASC guidelines on information management, sharing and confidentiality[6]
- Humanitarian information/data should be made accessible to all humanitarian actors at the required level of granularity, unless sharing the data threatens the humanitarian space and safety of the organization, its staff, partners and beneficiaries
- Information management and exchange should be based on collaboration, partnership and sharing with a high degree of trust, participation and joint ownership
- OCHA staff and partners will always utilize/share information in a manner that recognizes the sensitivities associated with this humanitarian operation and respects the need for confidentiality and anonymization
- When sharing sensitive information, the sending party is responsible for classifying the information shared to indicate whether it can be shared further and with whom (based on the data sensitivity classification) to ensure that the recipient(s) adopt suitable measures to prevent the information from being compromised or inappropriately disclosed.
- Recipients of sensitive information or data as classified using the sensitivity classification are responsible for storing such information or data by extracting and protecting information which cannot be shared, prior to sharing.

4. Personally identifiable data like beneficiary lists should be shared within bilateral agreements based on organizational policies framed in accordance with the minimum standards prescribed by the UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, as adopted by Resolution A/Res/45/95 of 14 December 1990, available at: http://www.refworld.org/docid/3ddcafaac.html and other international instruments concerning the protection of personal data and individuals' privacy.

5. OCHA Data Responsibility Guidelines, Centre for Humanitarian Data, 2019, p. 16.

6. IASC Operational Guidance on Responsibilities of Cluster/Sector Leads and OCHA in Information

Breaches to the Protocol and Dispute Resolution[7]

[INSERT ACTIONS TO BE TAKEN UPON BREACH OF PROTOCOL. THESE CAN BE STRUCTURED ALONG THE LINES OF THE BELOW]
Should there be a breach of this Protocol by any of participating members, a meeting will be called for all members within ten days to discuss the breach and develop a resolution. If a full meeting is not possible within ten days or if a resolution cannot be reached, the [NAME CLUSTER/SECTOR] lead hold a meeting to determine the course of action. If needed, an external interlocutor may be approached to facilitate the discussion and resolution.

[NAME CLUSTER/SECTOR] members may stop sharing data if the protocol is breached and will inform [NAME CLUSTER/SECTOR] lead in writing of their reasons for stopping the flow of data. While the matter is being resolved, and if the [NAME CLUSTER/SECTOR] lead is not involved in the breach, it is recommended that [NAME CLUSTER/SECTOR] members continue to share data to inform field level response. The consolidated information will not be shared externally until the breach is resolved.

The resolution of a breach or suspected breach must be agreed to by all members of the [NAME CLUSTER/SECTOR].

In case of differences in interpretation of this ISP or other disputes, the [NAME CLUSTER/SECTOR] lead will be responsible for finding an amenable resolution. If such a resolution cannot be found, the [NAME CLUSTER/SECTOR] lead will refer the dispute to [NAME INDEPENDENT THIRD].

7. Adapted from the GBVIMS Inter-Agency Information Sharing Protocol, http://www.gbvims.com/gbvims-tools/isp/

DATA RESPONSIBILITY PLAN TEMPLATE

Click here to download an editable version of this template for use in your context. CLICK HERE

This Data Responsibility Plan template is designed for use by OCHA staff responsible for managing humanitarian data for a variety of different purposes. The template is meant to be adapted and tailored to specific contexts. If you want to receive support in drafting and/or reviewing your Data Responsibility Plan, contact the Centre for Humanitarian Data.

OCHA Office

Insert name of OCHA office responsible for this exercise.

Exercise

Indicate the exercise (e.g. needs assessment, 3W/4W, Evaluation, etc.).

Project Lead(s)

Insert name, role/title, and contact details for the Project Lead.

Date of Plan

Insert the date on which this plan was developed.

Value Description

Describe the value of the data management exercise in concrete terms.

Scope and Volume

Articulate the required scope and volume of humanitarian data to be collected or received.

Tools for Receipt or Collection

Indicate which tool(s) will be used for the receipt and/or collection of data in this exercise.

Standard Operating Procedure and Information Sharing Protocol

Indicate which SOP(s) and ISP(s) apply to this data management exercise.

Capacities and Resources

Determine the capacities and resources required for responsible data management and indicate their availability (e.g. data visualization expertise; licenses for required tools/software; encrypted storage; funds for maintenance of data transfer or collection solution, etc.)

Additional Precautions

If primary data collection is required, indicate which additional precautions you will take to ensure protection (e.g. completion of a DPIA; consulting with context/local experts; running statistical disclosure control before sharing aggregate data, etc.)

DATA RESPONSIBILITY PLAN TEMPLATE

Risks and Mitigation Measures

Identify and define the risks associated with the data management exercise. For each risk, identify concrete mitigation measures.

Risks	Mitigation Measures
I.	I.
II.	II.
III.	III.
IV.	IV.
V.	V.

DATA RESPONSIBILITY PLAN TEMPLATE

Data Flow Map

Reproduce the portion of your Data Ecosystem Map that includes the stakeholders and data flows, relationships, and related actions that comprise the data management exercise in question. If there is no Data Ecosystem Map for your context, start here by simply mapping out the details for your exercise.

Symbols	Entity or Object
	Infrastructure
	Data
	UN
	Other IO
N	NGO
	Civil Society
	Government
	Potential Transfer
	Data Transfer
	Vetted / Trusted / Secure

⚙ DATA RESPONSIBILITY PLAN TEMPLATE

Evaluation of Data Responsibility

NB: This should be completed at the end of the data management exercise. For ongoing / recurring exercises (such as the 3W/4W or HNO/HRP), complete this evaluation step on an annual basis to help track improvements in data responsibility over time. Check the box for each action or output completed during the course of your data management exercise. Indicate the total number of checked boxes in the 'data responsibility score' box at the bottom of this sheet.

Fundamentals

- ☐ Data ecosystem map
- ☐ Information Sharing Protocol
- ☐ Tools for data management
- ☐ Required skills and training

Planning

- ☐ Data Responsibility Plan (DRP) completed

Collecting and Receiving

- ☐ No known cases of datasets that were not compliant with relevant standards and protocols
- ☐ No known cases of stakeholders failing to comply with relevant standards and protocols
- ☐ No known cases of sensitive data being transferred in an insecure manner
- ☐ In cases where OCHA conducted primary data collection, measures were taken to prevent duplication, enhance data quality, and ensure protection of sensitive humanitarian data
- ☐ In cases where OCHA managed microdata (individual survey results), measures such as running Statistical Disclosure Control (SDC) taken to mitigate risk

Storing

- ☐ Storage infrastructure was established and available for use throughout the exercise, in compliance with requirements and access conditions
- ☐ No known breaches of access conditions for data being stored

Cleaning

- ☐ Cleaned and standardized datasets were consistently made available, and included documentation of limitations and caveats
- ☐ Methods and tools utilized in data cleaning met the relevant criteria for the exercise in the context

Transfer

- ☐ No known deviations from or breaches of relevant ISP(s)
- ☐ When transferring data to private sector partners or unknown entities, due diligence assessment returned positive
- ☐ Methods for secure and responsible data transfer established and available for use throughout the exercise
- ☐ Data transfer agreements were in place and adhered to where required
- ☐ All necessary precautions were taken consistently when transferring sensitive humanitarian data

Analysis

- ☐ All charts, graphs or maps displaying information were accompanied by background, contextual and/or technical expertise and provided with limitations or caveats and methodology documentation
- ☐ Resources and capacities required for accurate, effective, and principled analysis and/or visualisation were available as needed
- ☐ Methods and tools for analysis and/or visualisation were clearly documented
- ☐ No known cases of data analysis conducted in a manner that did not follow to relevant Standard Operating Procedures (SOPs)
- ☐ A review of the analysis methodology, outcome and documentation has been conducted

DATA RESPONSIBILITY PLAN TEMPLATE

Evaluation of Data Responsibility

NB: This should be completed at the end of the data management exercise. For ongoing / recurring exercises (such as the 3W/4W or HNO/HRP), complete this evaluation step on an annual basis to help track improvements in data responsibility over time. Check the box for each action or output completed during the course of your data management exercise. Indicate the total number of checked boxes in the 'data responsibility score' box at the bottom of this sheet.

Communicating and Disseminating

- ☐ No known deviations from the appropriate format, channel and audience for the product based on the relevant ISPs and SOPs
- ☐ Contextual information was always included as part of published information products or datasets
- ☐ Staff ensured appropriate communication and follow-up with different stakeholder groups, including clearance before communicating final information products where required
- ☐ Sources and source licenses were always referenced in published information products or datasets

Feedback and Evaluation

- ☐ Use of data was communicated back to stakeholders and the original data source
- ☐ Successes and failures experienced throughout the data processing exercise(s) were recorded for the purposes of case-based learning
- ☐ Data Responsibility Evaluation has been completed

Retention and Destruction

- ☐ Datasets selected for retention were stored securely, using proper means for storage to ensure data integrity and accessibility
- ☐ Datasets selected for destruction were destroyed effectively, with clear documentation of this step and the datasets concerned
- ☐ Measures were taken to determine the balance between sensitivity, potential future value of the data and value loss that would be created if the data is destroyed

DATA RESPONSIBILITY SCORE

Step	Score
Fundamentals	_____ / 4
Planning	_____ / 1
Collecting and Receiving	_____ / 5
Storing	_____ / 2
Cleaning	_____ / 2
Transfer	_____ / 5
Analysis	_____ / 5
Communicating and Disseminating	_____ / 4
Feedback and Evaluation	_____ / 3
Retention and Destruction	_____ / 3
Total	_____ / 34

TERMS OF REFERENCE
Data Responsibility Advisory Group
March 2019

Background

The United Nations Office for the Coordination of Humanitarian Affairs (OCHA) has adopted Data Responsibility Guidelines to promote appropriate use of data across the organisation. Data is a critical component of humanitarian response. The management of digital data relating to crisis contexts, affected people and humanitarian response operations allows the humanitarian community to respond in a more effective and efficient manner. However, as organizations process increasingly large volumes of data, they also face more complex challenges and risks.

The need for **data responsibility** has now been recognized by a wide variety of organizations, both within and outside the humanitarian space. Data responsibility goes beyond the concepts of "data privacy" and "data protection". It **entails a set of principles, processes and tools that support the safe, ethical and effective management of data in humanitarian response**.[1] Whereas many humanitarian organizations have developed policies and guidelines focused on the management of personal data,[2] guidance has been lacking on how to ensure data responsibility in the management of other forms of humanitarian data such as survey results and datasets containing information that could be used to target individuals in conflict areas. The OCHA Data Responsibility Guidelines aim to fill this gap.

1. 'Building Data Responsibility into Humanitarian Action' OCHA Think Brief (2016).

2. 'Mapping and Comparing Responsible Data Approaches', NYU GovLab, Leiden University (2016).

A critical component of the Guidelines is the Data Responsibility Advisory Group (DRAG).

Purpose of the DRAG

The DRAG is a cross-functional group convened by the Centre for Humanitarian Data that will track the implementation of the Guidelines and support the monitoring of critical incidents related to data management. The DRAG will bring together working-level representatives from each of OCHA's functions and several field offices on a regular basis to monitor and examine practices around progress, challenges, breaches and other concerns related to data responsibility. The ultimate purpose of the DRAG is to support OCHA's Branch Chiefs and Function Leads in ensuring widespread adoption and implementation of the Data Responsibility Guidelines across the organisation.

Activities

In-line with the Guidelines, the DRAG will be responsible for the following:

- Providing input and feedback on the report to the ASG, to be sent out by the Chief of IMB every six months
- Advising on best approaches to deliver on the Guidelines across the organisation
- Advocating for the use of, and promoting awareness of the Guidelines
- Advising on critical incident management, to be lead by the office or section affected with support from the Centre for Humanitarian Data
- Advise on priority areas for training and capacity development related to data responsibility

This work will require roughly 2 hours of engagement and effort from members each month.

Composition and Chair
The DRAG will consist of ten members to be nominated by each Functional Lead (each Lead will nominate a focal point and a back-up). All five functions should be represented on the DRAG at all times. Field Office representation will also be critical, with both Regional Offices and Country Offices participating in the DRAG at all times. The DRAG will be chaired by a representative from the Centre for Humanitarian Data.

Membership
Members will serve on a voluntary basis for an initial twelve-month period with an option to extend for a further twelve months. The DRAG will meet virtually every two months to provide input and feedback for, and sign off on the draft report on Data Responsibility that will be sent to the ASG every six months. In case of an urgent request for support, the DRAG may convene ad hoc completely or partially. To the extent possible and based on the availability of funds, one face-to-face meeting will be held every year.

Secretariat
The Centre for Humanitarian Data will provide the Secretariat for the DRAG. The Secretariat will deliver the following support:

- Convene the DRAG call every two months
- Prepare the agenda and take the minutes for each DRAG call
- Draft the Data Responsibility report for the ASG

Confidentiality
One of the key barriers to progress in improving data management practices is the lack of organisational learning due to a hesitancy to share information about incidents. For this reason, conversations held during the DRAG calls will be kept confidential, to allow representatives to share their experiences freely. Detailed notes from the DRAG calls will not be shared beyond the DRAG and its Secretariat.