OCHA DATA RESPONSIBILITY GUIDELINES

DECEMBER 2024

OCHA CENTRE FOR HUMANITARIAN DATA

OCHA

centre for humdata

TABLE OF CONTENTS

PREFACE

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

The OCHA Data Responsibility Guidelines ('the Guidelines') offer a set of principles, processes and tools that support data responsibility in OCHA's work.[1] The Guidelines were first agreed in October 2021 and were revised in October 2024 to align them with UN Secretariat policy and IASC guidance. The revision also takes account of the direct experience and feedback from OCHA offices in adopting the Guidelines over the past several years.

The audience for the Guidelines is OCHA staff involved in managing data across OCHA's core functions of coordination, advocacy, policy, humanitarian financing and information management, with a primary focus on the field. The Guidelines apply to all operational data managed directly by OCHA, managed on OCHA's behalf, or managed by humanitarian actors within activities coordinated by OCHA in different responses. This includes the following types of data:

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

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

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

Common operational data management activities for OCHA include situational analysis, needs assessments, 3W/4W, communicating with affected populations, access monitoring, and response monitoring and evaluation.

The Guidelines do not apply to OCHA's management of corporate data, such as human resources and financial data. OCHA's management of corporate data is regulated by applicable UN Secretariat rules. OCHA offices should consult the Data Protection and Privacy Policy for the Secretariat of the United Nations[2] ('the UN Secretariat Data Protection and Privacy Policy') and ensure their management of corporate data complies.

The Chief of the Information Management Branch and Lead for the Information Management Function is accountable for the adoption of the Guidelines across OCHA.

The Guidelines will be revised as needed.

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

[2] UN Secretariat, Secretary-General's bulletin on Data protection and privacy policy for the Secretariat of the United Nations, ST/SGB/2024/3 (2024).

RELATED GUIDANCE AND FRAMEWORKS

Promoting data responsibility is a priority for OCHA. OCHA's Strategic Plan 2023-2026 states that OCHA will "coordinate and facilitate system-wide standards for data responsibility to ensure the safe, ethical and effective management of data in humanitarian response." The Guidelines reflect the latest global guidance and policy instructions within the United Nations (UN) Secretariat and the broader humanitarian system, including:

- The Inter-Agency Standing Committee Operational Guidance on Data Responsibility[3]
- Data Protection and Privacy Policy for the Secretariat of the United Nations[4]
- The Secretary-General's Roadmap for Digital Cooperation[5]
- The Secretary-General's Data Strategy[6]

The Guidelines address how OCHA should implement the IASC Operational Guidance on Data Responsibility.[7] The Operational Guidance applies to both personal and non-personal data for operational response that is generated and/or used in humanitarian action, and is applicable to all humanitarian actors engaged in a response. It does not replace or supersede organizational policies and guidance, nor account for specific organizational mandates or relevant national or regional laws.

The Guidelines also address how OCHA's operational data management should align with the UN Secretariat Data Protection and Privacy Policy. This policy places mandatory obligations on OCHA and requires OCHA to report, through the USG, on its implementation. The policy applies to all OCHA's management of personal data and 'non-personal data in a sensitive context'.

[3] Inter-Agency Standing Committee, **Operational Guidance on Data Responsibility in Humanitarian Action** (2023).

[4] UN Secretariat, Secretary-General's bulletin on Data protection and privacy policy for the Secretariat of the United Nations, ST/SGB/2024/3 (2024).

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

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

[7] Inter-Agency Standing Committee, **Operational Guidance on Data Responsibility in Humanitarian Action** (2023).

STRUCTURE OF THE GUIDELINES

The Guidelines contain four sections and supporting Annexes.

Section 1: Introduction offers an overview of key concepts related to data responsibility in humanitarian action and explains OCHA's role in humanitarian data management.

Section 2: Actions for Data Responsibility in Humanitarian Response Contexts provides practical guidance on how OCHA should support actions for data responsibility at the system-wide level, working group level, and office level.

Section 3: Accountability outlines the key roles and responsibilities for ensuring the adoption of the Guidelines and explains how these relate to the governance and oversight functions established by the UN Secretariat Data Protection and Privacy Policy.

Section 4: Services to Support Adoption of the Guidelines provides an overview of the services available to OCHA staff implementing the Guidelines. These services are offered by the Information Management Branch through the Centre for Humanitarian Data and are available upon request.

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

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

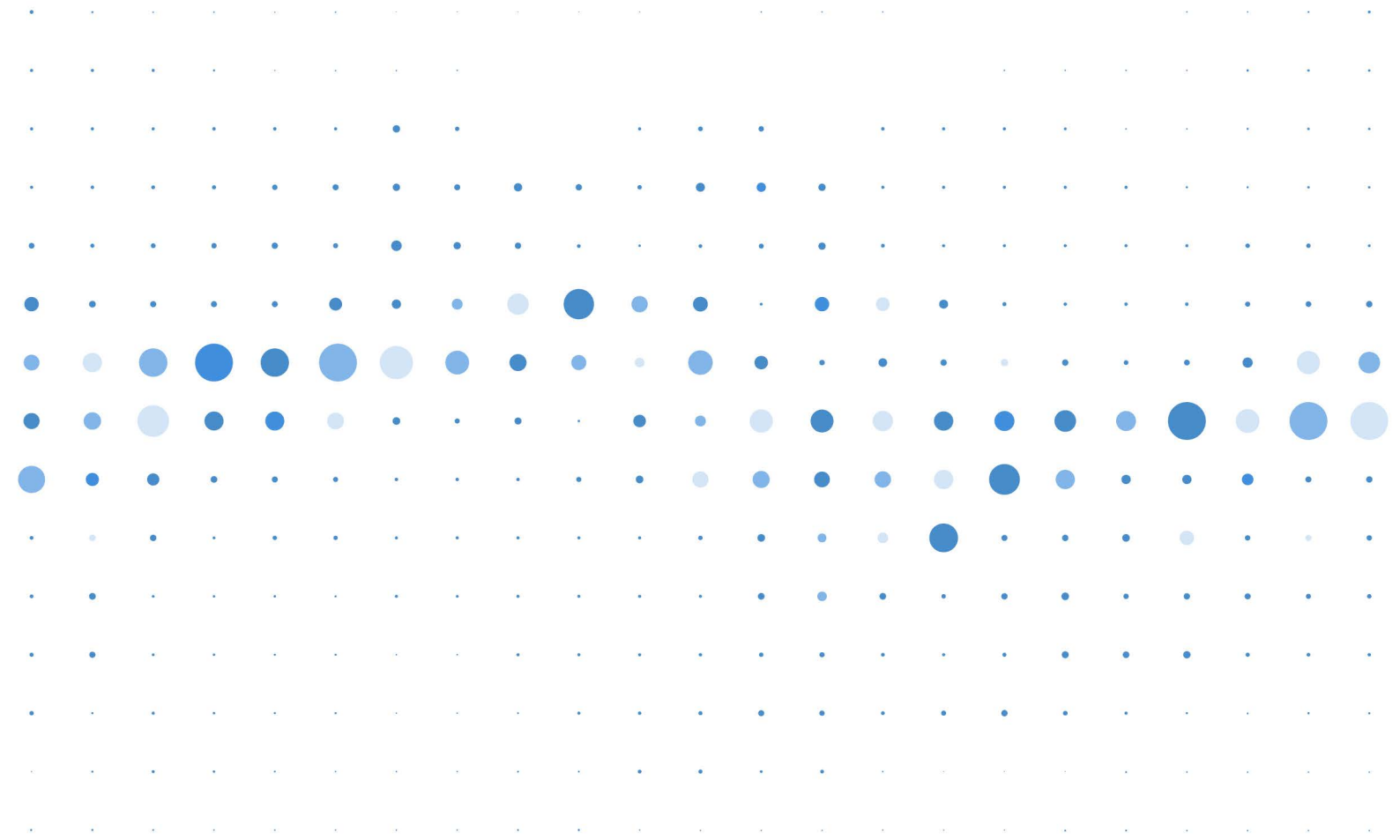
Annex C - Templates for Data Responsibility brings together the different templates referenced throughout the Guidelines. Editable versions of each template are available via links included in this Annex.

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

ACRONYMS

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

1. INTRODUCTION



1.1 DATA RESPONSIBILITY IN HUMANITARIAN ACTION

Data is a critical component of humanitarian response. The management of data relating to crisis contexts, affected people and humanitarian operations allows the humanitarian community to respond more effectively and efficiently. However, as organizations manage increasingly large volumes of data and make use of emerging technologies including artificial intelligence, they also face more complex challenges and risks. OCHA staff must be careful when handling data to avoid placing already vulnerable individuals and communities at further risk and to safeguard trust between affected populations and humanitarian organizations.

In recent years, the sector has seen the development of principles, policies and strategies for data responsibility in humanitarian action. These include system-wide guidance, such as the IASC Operational Guidance on Data Responsibility in Humanitarian Action, as well as global strategies and policies to guide data management within the UN system. OCHA's 2023-2026 Strategic Plan recognizes data responsibility as a key part of delivering on the organization's transformational priorities, and aims to position OCHA as a leader on this issue in the sector.

Despite considerable progress, the implementation of data responsibility in practice is often inconsistent within and across humanitarian response contexts. The OCHA Data Responsibility Guidelines are designed to help bridge these gaps by supporting OCHA staff to apply global frameworks for data responsibility in their day-to-day work.

DEFINING DATA RESPONSIBILITY AND RELATED TERMS

A full list of terms and definitions is available in Annex A. All definitions are aligned with the UN Data protection and privacy policy and the IASC Operational Guidance.

Data responsibility in humanitarian action is the **safe, ethical and effective management of personal and non-personal data for operational response**, in accordance with established frameworks for personal data protection.[8]

- **Safe** | Data management activities ensure the security of data at all times, respect and uphold human rights and other legal obligations, and do not cause harm.
- **Ethical** | Data management activities are aligned with the established frameworks and standards for humanitarian ethics[9] and data ethics.[10]
- **Effective** | Data management activities are well coordinated and achieve the purpose(s) for which they were carried out.

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

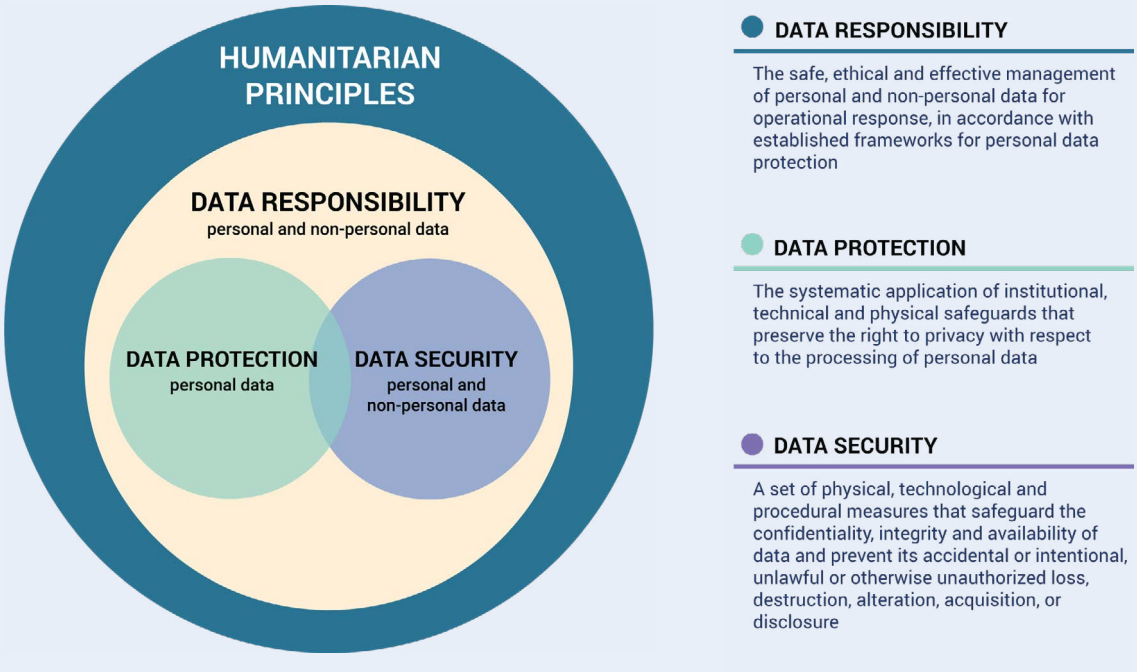
[8] This includes the Secretary-General's Bulletin on Data Protection and Privacy Policy for the Secretariat of the United Nations, ST/SGB/2024/3 (2024) and other administrative instructions from the UN Secretariat.

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

[10] The UN OCHA Centre for Humanitarian Data **Guidance Note on Humanitarian Data Ethics** (2019) provides further background information on the relation between humanitarian ethics and data ethics.

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

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



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

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

The term 'data processing' is used to refer to any operation or set of operations that is performed on personal data or 'non-personal data in a sensitive context', as per the UN Secretariat Data Protection and Privacy Policy.

Personal data: Information, in any form, that relates to an identified or identifiable natural person ('data subject').

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

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

- harm (such as sanctions, discrimination) to any person, including the source of the information or other identifiable persons or groups, or;
- a negative impact on an organization's capacity to carry out its activities or on public perceptions of that organization.[11]

Sensitive data includes personal data as well as 'non-personal data in a sensitive context'. Non-personal data in a sensitive context is information, in any form, that, while not relating to an identified or identifiable natural person, may, by reason of its sensitive context, put certain individuals and groups at risk of harm, including vulnerable or marginalized individuals and groups of individuals, such as children. The same types of data may have different levels of sensitivity in different contexts and sensitivity may change over time.

[11] Based on the definition in the ICRC-led Advisory Group on "Professional Standards", **Professional Standards for Protection Work, 3rd edition** (2018), Chapter 6: Managing Data and Information for Protection Outcomes.

1.2 OCHA'S ROLE IN HUMANITARIAN DATA MANAGEMENT

OCHA plays an important and unique role in humanitarian data management. Whereas other humanitarian organizations process data primarily for their own use, OCHA's data management is mainly focused on aggregation and analysis for the wider humanitarian community.

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

OCHA also plays a critical role in coordinating data and information management activities across a diverse group of stakeholders. OCHA's role is to connect partners to one another through the provision of services such as common standards and cloud-based infrastructure for storing and transferring data responsibly. In the age of digital data, OCHA must take into account the risk of hosting or acting as a passthrough for sensitive data. OCHA must also assess risks from the use of new and emerging technologies in its work. The Guidelines are designed to support this role.

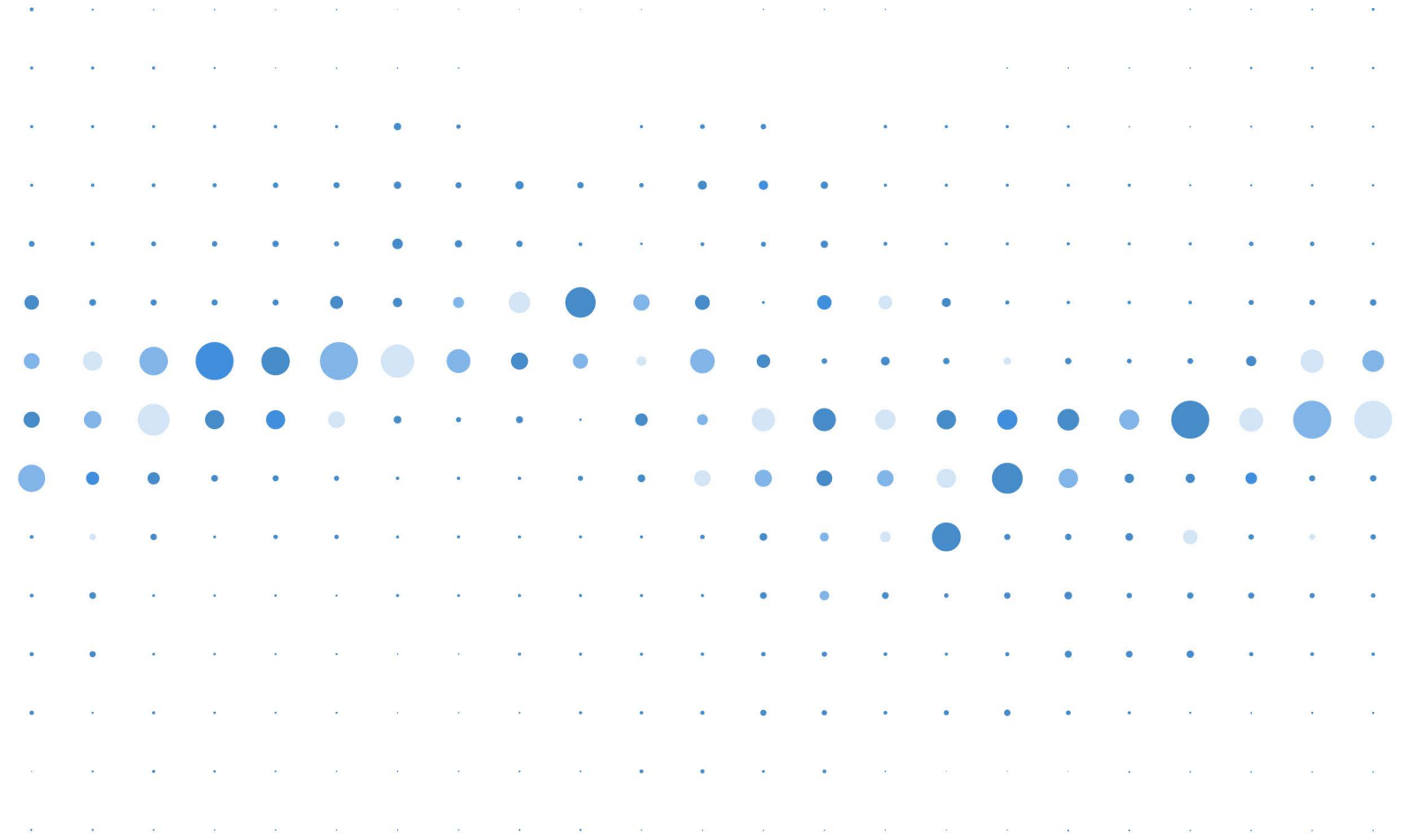
PRINCIPLED DATA MANAGEMENT

OCHA's data management is guided by two sets of principles. The IASC Operational Guidance contains principles that reflect the collective commitment of humanitarian actors to data responsibility at the system-wide, cluster/sector and working group, and organization levels. They were agreed through an inter-agency process, and are based on a review of existing principles for data management across the humanitarian and development sectors.[12]

In most situations the sets of principles from the IASC Operational Guidance and the UN Secretariat Data Protection and Privacy Policy complement and reinforce one another. Reach out to the Centre for Humanitarian Data for support on how to implement these principles in practice.

[12] A complete list of the documents compiled and analyzed by the IASC Sub-Group on Data Responsibility in 2020 to inform the drafting of the Principles is available in Annex D to the IASC Operational Guidance on Data Responsibility in Humanitarian Action.

2. ACTIONS FOR DATA RESPONSIBILITY IN HUMANITARIAN RESPONSE CONTEXTS



2 ACTIONS FOR DATA RESPONSIBILITY IN HUMANITARIAN RESPONSE CONTEXTS

The actions included in the IASC Operational Guidance on Data Responsibility in Humanitarian Action are designed for implementation at **three levels in a response**:

SYSTEM-WIDE LEVEL

CLUSTER/SECTOR AND WORKING GROUP LEVEL

ORGANIZATION LEVEL

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

The system-wide level refers to the highest-level coordination structures in a given response, e.g., the Humanitarian Country Team (HCT) and the Inter-Cluster/Inter-Sector Coordination Group (ICCG/ISCG).

As the convener of the ICCG/ISCG and the IMWG, OCHA has an important role to play in supporting actions for data responsibility at the system-wide level. There are **five actions** that should be prioritized by OCHA staff at the system-wide level.

01 CONDUCT A SYSTEM-WIDE DATA RESPONSIBLITY DIAGNOSTIC

Purpose:

The system-wide data responsibility diagnostic provides an overview of inter-agency/inter-cluster/inter-sector actions for data responsibility. It supports joint decision-making on how to focus and prioritize collective action on data responsibility.

OCHA's Role:

OCHA is responsible for initiating and facilitating the development of the system-wide data responsibility diagnostic by the relevant interagency mechanism(s) (including both the ICCG/ISCG and the IMWG), and for presenting the diagnostic to the HCT for review once finalized.

Recommended Approach:

- ☐ Prepare a draft of the diagnostic based on information available using the IASC Data Responsibility Diagnostic Template. This will likely require inputs from both the coordination and information management teams in the office.
- ☐ Circulate the draft to ICCG/ISCG and IMWG members for inputs.
- ☐ Consolidate inputs and finalize the draft diagnostic for collective review and validation during a joint meeting of the ICCG/ISCG, the IMWG and other thematic or technical working groups as relevant.
- ☐ Share the final diagnostic with the HCT and offer to provide a briefing on the key findings and related recommendations for data responsibility in the response.
- ☐ Share the completed diagnostic with the broader response community through appropriate channels, and establish a process for tracking implementation of recommendations, to monitor progress on key issues related to data responsibility.

Relevant Tool or Template:

IASC Data Responsibility Diagnostic Template

02 GENERATE AND MAINTAIN A SYSTEM-WIDE DATA MANAGEMENT REGISTRY

Purpose:

The system-wide data management registry provides an overview of data management activities taking place in the response. The registry requires inputs from clusters/sectors and other inter-agency entities.

OCHA's Role:

OCHA is responsible for establishing the system-wide data management registry and for supporting the relevant interagency mechanism(s) in keeping the data management registry up-to-date. Upon completion, OCHA should present the data management registry to the HCT.

Recommended Approach:

- ☐ Establish the system-wide data management registry using the IASC Data Management Registry Template. This should be led by the IM team with input and feedback from the coordination team.
- ☐ Circulate the system-wide data management registry to IMWG members for inputs.
- ☐ Consolidate inputs and review the system-wide data management registry during a joint meeting of the ICCG/ISCG, the IMWG and other thematic or technical working groups as relevant.
- ☐ Present the system-wide data management registry to the HCT, with any recommendations that have come out of the process, to ensure the HCT has an overview of data management activities to support responsible data management.
- ☐ Ensure follow-on tracking of any recommendations related to the registry and its regular updating.

Relevant Tool or Template:

IASC Data Management Registry Template

03 DEVELOP AND MAINTAIN A SYSTEM-WIDE INFORMATION SHARING PROTOCOL

Purpose:

The system-wide Information Sharing Protocol (ISP) serves as the primary document of reference governing data and information sharing in the response. It includes a context-specific Data and Information Sensitivity Classification outlining the sensitivity of specific data and information, as well as a recommended approach for sharing different types of data in the response.

OCHA's Role:

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

Recommended Approach:

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

Relevant Tool or Template:

IASC Information Sharing Protocol Template

04 TRACK AND COMMUNICATE ABOUT DATA INCIDENTS

Purpose:

Tracking and communicating about data incidents fosters learning and supports coordinated approaches to data incident management.

OCHA's Role:

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

Recommended Approach:

- ☐ Create a registry that captures key details about the nature, severity and resolution of different incidents. Where appropriate, this may be linked with other system-wide incident monitoring processes and tools, e.g., security and access monitoring systems. Limit access to the registry to staff involved in addressing incidents, to prevent unnecessary disclosure of information about incidents.

- ☐ Introduce the registry to the ICCG/ISCG and the IMWG and ensure that all relevant stakeholders are aware of the process for providing inputs, including thematic or technical working groups as relevant.

- ☐ Encourage inputs by the clusters/sectors on behalf of their members. Individual organizations may also provide inputs based on their own incident management tracking where these inputs are not already c overed by contributions from the relevant cluster/sector.

- ☐ Prepare periodic reports to the HCT summarizing the nature, severity and resolution tactics that stakeholders are using. When reporting, uphold confidentiality and do not share sensitive data.

Relevant Tool or Template:

IASC SOP for Data Incident Management Template

05 SUPPORT COORDINATION AND DECISION-MAKING ON COLLECTIVE ACTION

Purpose:

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

OCHA's Role:

OCHA is responsible for providing regular updates on data responsibility to the HCT, building on actions 1 through 4. OCHA should also promote alignment across clusters/sectors and between actions at the system-wide and cluster/sector levels.

Recommended Approach:

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

2.2 OCHA'S ROLE IN CLUSTER/SECTOR AND WORKING GROUP LEVEL ACTIONS FOR DATA RESPONSIBILITY

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

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

OCHA does have a direct role in completing actions for data responsibility within thematic working groups. These include Access Working Groups (AWGs), Cash Working Groups (CWGs), Gender in Humanitarian Action (GiHA) and Accountability to Affected People Working Groups (AAPWGs). For working groups that OCHA leads or co-leads, there are five actions that should be prioritized by OCHA staff as relevant to the activities of the working group.

01 CONDUCT A WORKING GROUP LEVEL DATA RESPONSIBLITY DIAGNOSTIC

Purpose:

The working group level data responsibility diagnostic provides an overview of existing actions for data responsibility within a working group in a given response context. It can help identify gaps regarding data responsibility and help prioritize the implementation of additional actions for data responsibility.

OCHA's Role:

- ☐ OCHA is responsible for conducting the data responsibility diagnostic together with the working group (co-)lead and the working group members.

Recommended Approach:

- ☐ Prepare a draft of the diagnostic based on information available using the IASC Data Responsibility Diagnostic Template.
- ☐ Circulate the draft to working group Co-Leads and members for inputs.
- ☐ Consolidate inputs and finalize the draft diagnostic for collective review and validation during a joint meeting of the working group.
- ☐ Share the final diagnostic with the working group and offer to provide a briefing on the key findings and related recommendations for data responsibility.
- ☐ Ensure regular check-ins with the working group on implementation of recommendations and any changes to the diagnostic.

Relevant Tool or Template:

IASC Data Responsibility Diagnostic Template

02 GENERATE AND MAINTAIN A WORKING GROUP LEVEL DATA MANAGEMENT REGISTRY

Purpose:

The working group data management registry provides an overview of data management activities that the working group is leading or participating in.

OCHA's Role:

- ☐ OCHA is responsible for establishing the data management registry and for keeping the data management registry up-to-date.

Recommended Approach:

- ☐ Establish the data management registry using the IASC Data Management Registry Template.
- ☐ Circulate the data management registry to working group Co-Leads and members for inputs.
- ☐ Consolidate inputs and review the data management registry before finalizing.

Relevant Tool or Template:

IASC Data Management Registry Template

03 DEVELOP AND MAINTAIN A WORKING GROUP SPECIFIC INFORMATION SHARING PROTOCOL

Purpose:

The system-wide Information Sharing Protocol (ISP) serves as the primary document of reference governing data and information sharing in the response. If no system-wide ISP is available in the response context, working groups can choose to develop their own ISP.

OCHA's Role:

OCHA should lead the drafting of an ISP for the working group if required in the response context.

Recommended Approach:

- ☐ Verify whether there is a system-wide ISP in place. If so, ensure that the data managed and shared by the working group is included and correctly classified in the ISP. If not, reach out to the IMWG to request an amendment of the ISP.
- ☐ If no system-wide ISP exists, approach the IMWG and introduce the concept of developing a system-wide ISP, and agree on an approach and timeline for the process with members.
- ☐ Alternatively, develop a working group-specific ISP if no system-wide ISP exists or if it does not cover the level of detail required for the working group.
- ☐ Develop an initial draft using the IASC Information Sharing Protocol template and circulate with the Co-Lead and members.
- ☐ Present the ISP to the working group members for review and endorsement.
- ☐ All stakeholders involved in data management should be made aware of the ISP and their respective obligations. Depending on the response, OCHA should make the endorsed ISP publicly available on ReliefWeb or a response-specific site.
- ☐ Ensure the working group regularly reviews the ISP for any necessary changes, particularly if there is a change in the security context.

Relevant Tool or Template:

IASC Information Sharing Protocol Template

04 OFFER TECHNICAL AND ADVISORY SUPPORT TO WORKING GROUP MEMBERS

Purpose:

Human, financial and technological resources are essential to strengthen data responsibility within the working group and across its members. This is particularly important when members undertake or participate in joint data management activities on behalf of or for the use of the working group.

OCHA's Role:

OCHA should provide advisory and technical support on data responsibility (e.g., how to conduct data impact assessments and securely transfer sensitive data), which should be incorporated into working group capacity development activities.

Recommended Approach:

- ☐ OCHA, together with the Co-Lead should advocate for the necessary resources for the working group and its members to be able to manage data responsibly and to promote related capacity development activities.

05 SUPPORT DESIGN FOR DATA RESPONSIBILITY

Purpose:

Including data responsibility considerations in the design, implementation, monitoring and evaluation of data management activities led by the working group helps minimize risks and maximize benefits.

OCHA's Role:

OCHA and the Co-Leads should ensure that data management activities led by the working group are designed for data responsibility, including by developing relevant standard operating procedures (SOPs).

Recommended Approach:

☐ Working groups should incorporate data responsibility, including data protection and privacy, into data management by design when planning any data management activity.

☐ Designing for data responsibility includes, for example, the following steps and considerations:

- Establish clear and replicable SOPs for data management activities. The IASC Operational Guidance includes a template SOP. SOPs should include information regarding applicable data subject rights where personal data is processed, and should specify the channels for requests regarding these rights.
- When selecting tools for data management, foster complementarity, interoperability (where appropriate, including with governmental and other local systems), and harmonization (including on terminology, typologies and data structure).
- Ensure the working group has assessed risks associated with any use of use of emerging technologies, including artificial intelligence, blockchain or other similar tools to process data or produce analysis.
- Offer training to working group members and partners on responsible data management, including on guidance developed by the working group for its data management activities.
- Support measures for the safe management of data (e.g., for data anonymization, provision of secure storage and data transfer solutions, etc.).
- Adhere to relevant guidance and protocols on data responsibility and related processes and procedures, including ISPs. This includes ensuring all data that needs to be shared for defined purposes is made available through appropriate channels in a responsible manner, with the necessary safeguards for personal data and in compliance with applicable data protection frameworks.

2.3 DATA RESPONSIBILITY WITHIN OCHA OFFICES

The actions for data responsibility at this level are primarily meant for OCHA country offices. Some actions at this level, such as the development of a standard operating procedure for data incident management, will also be relevant to OCHA headquarters sections in their operational data management.

The instructions under 'policy requirement' reflect mandatory requirements under the UN Secretariat Data Protection and Privacy Policy. The policy also establishes the role of data protection focal point,[13] tasked with supporting the implementation of the policy. Requirements to share data or information with the data protection focal point are flagged specifically in the actions below.

DATA SUBJECT RIGHTS

A data subject is any person to whom personal data relates, including beneficiaries of assistance.[14] Under the UN Secretariat Data Protection and Privacy Policy, data subjects have a number of rights relating to the processing / management of their personal data. These rights include:

1. The right to request information as to:
   a. The legal basis and specified purpose of processing of personal data
   b. The safeguards applicable to such data processing;
   c. The types of data being processed;
   d. The source(s) of data;
   e. The applicable retention period;
   f. Whether data processing involves automated decision-making that would result in decisions significantly affecting them;
   g. Whether data are being transferred outside the United Nations and, if data are being transferred, the recipient of the transfer and the purpose therefor.
2. The right to request access to a copy of personal data relating to them.
3. The right to request rectification or completion of inaccurate or incomplete personal data.
4. The right to request the deletion of personal data relating to them.
5. The right to request that the Secretariat cease or restrict the processing of personal data relating to them.

[13] Based on sections 6 and 7 in the UN Secretariat Data Protection and Privacy Policy, the Data Protection Focal Point is responsible for establishing procedures, conducting data impact assessments, and other duties set out in section 6.

[14] The data subject is any identified or identifiable natural person to whom personal data that are being processed by or on behalf of the Secretariat relate, including but not limited to a staff member, individual contractor or consultant, other United Nations personnel, an attendee at an official meeting or a beneficiary of assistance.

OCHA must fulfill its responsibilities towards data subjects. OCHA's data steward (the USG) should ensure information about data processing is available to data subjects, including on the procedures for making requests concerning the processing of their personal data. Such information should preferably be provided at the time of the collection of personal data or the transfer of such data outside the United Nations, including through individual or publicly available notices and through consent forms.[15] When designing for data responsibility, OCHA staff should include information on data subject rights in relevant documentation (such as SOPs). In line with the UN Secretariat Data Protection and Privacy Policy, OCHA's data steward will set up a centralized reporting mechanism to receive and disseminate requests by data subjects. OCHA's data steward is responsible for determining and taking actions on data subject requests. Additionally, OCHA's data steward is responsible for notifying data subjects of data breaches. This should be reflected in the SOPs for data incident management.

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

01 CONDUCT A DATA RESPONSIBLITY DIAGNOSTIC FOR THE OFFICE

Purpose:

The data responsibility diagnostic provides an overview of existing actions for data responsibility within an office. It can help identify gaps regarding data responsibility and helps offices prioritize the implementation of additional actions for data responsibility.

An annual data responsibility diagnostic at the office level is the means of verification for the adoption of actions for data responsibility to track progress on KPI D.1.2 in the OCHA results framework.

Recommended Approach:

- ☐ The annual data responsibility diagnostic should be conducted jointly by the OCHA office and the Centre for Humanitarian Data, with an Information Management Officer (IMO) and/or Humanitarian Affairs Officer (HAO).
- ☐ The data responsibility diagnostic should be conducted using **OCHA Data Responsibility Diagnostic Template**.

Relevant Tool or Template:

OCHA Data Responsibility Diagnostic Template

[15] See section 13 in the UN Secretariat Data Protection and Privacy Policy for instructions on the provision of information to data subjects.

02 CREATE AND MAINTAIN A DATA MANAGEMENT REGISTRY FOR THE OFFICE

Purpose:

OCHA offices should establish a data management registry to track all data management activities they are leading or contributing to. Some data management activities may already be included in tools such as a survey of surveys or an assessment registry. OCHA personnel should consult the registry and any similar tools before undertaking any new data collection in order to avoid duplication.

Policy Requirement:

- ☐ While the tracking of all data management activities is recommended, OCHA offices must record activities involving the management of personal data and 'non-personal data in a sensitive context'. The record of such activities must specify the purposes and means of the processing, the content and use of the data being processed, and any mitigation measures in place.
- ☐ The registry capturing these details must be shared with the data protection focal point to support the 'data mapping' mandated by the UN Secretariat Data Protection and Privacy Policy.

Recommended Approach:

- ☐ The IM unit in the OCHA office is responsible for developing a data management registry for all data management activities by the office. All staff involved in data management should be aware of the registry and know how to update it.
- ☐ The data management registry must at a minimum include the name, type, timeframe and actors involved in the data management activity, as well as the tools and infrastructure used, applicable guidance such as SOPs and ToRs for the activity, requirements for onward data sharing, and data retention and destruction timelines in line with applicable instructions from the data protection focal point.[16]
- ☐ The IM unit should share the data management registry with the data protection focal point.

Relevant Tool or Template:

IASC Data Management Registry Template

[16] According to the UN Secretariat Data Protection and Privacy policy, data stewards will establish internal processes in their respective entities for the periodic deletion of personal data and non-personal data in a sensitive context that is no longer needed for any purpose that is consistent with a legal basis for data processing.

03 CONDUCT A DATA IMPACT ASSESSMENT

Purpose:

A data impact assessment (DIA) helps identify and assess the potential risks, harms and benefits linked to the management of data and helps identify appropriate measures to prevent or mitigate any risks or harms identified. It should inform the design and implementation of a data management activity in order to maximize its benefits and minimize the risks.

Policy Requirement:

☐ While conducting a DIA is recommended for any data management activity to improve data responsibility, a DIA must always be conducted in the following circumstances:

(a) The processing of sensitive personal data;

(b) The processing of non-personal data in a sensitive context;

(c) The processing of large amounts of personal data;

(d) The processing of data involving significant merging, matching and manipulation of multiple data sets;

(e) Automated decision-making that would result in decisions significantly affecting data subjects;

(f) The use of artificial intelligence, blockchain or other similar emerging technologies to process data;

(g) The processing of data otherwise presents serious risks of harm to one or more individuals or groups of individuals.

☐ In the circumstances listed under (a) to (g) above, the DIA must be conducted in consultation with the data protection focal point.

Recommended Approach:

☐ The IMO or HAO responsible for the data management activity should prepare a draft Data Impact Assessment by filling out the Data Impact Assessment template using the information available to the OCHA Office.

☐ The draft should be shared with other actors involved in the data management activity for their input. DIAs should be conducted in an inclusive manner, involving affected populations where feasible.

☐ Address negative impacts identified in the Data Impact Assessment through appropriate, feasible, and robust prevention and mitigation measures.

☐ The data management activity should be redesigned or canceled if its foreseeable risks and harms outweigh its intended benefits, despite prevention and mitigation measures.

☐ Share the results of the DIA with the other actors involved in the data management activity and, where appropriate, with counterparts planning a similar activity in the context. This supports consistency in the assessment, monitoring, and mitigation of data-related risks over time.

☐ Share the results of the DIA with the data protection focal point.

Relevant Tool or Template:

Data Impact Assessment Template

04 DESIGN DATA MANAGEMENT ACTIVITIES FOR DATA RESPONSIBILITY

Purpose:

Including data responsibility considerations in the design, implementation, monitoring and evaluation of data management activities helps minimize risks and maximize benefits.

For OCHA, common data management activities include but are not limited to situational analysis, coordinated needs assessments, 3W/4W, communicating with affected populations, access monitoring, and response monitoring and evaluation (including through third parties). These activities typically consist of the following nine steps: planning, collecting, receiving and storing, assuring quality, sharing, analyzing, presenting, retaining and destroying, and evaluating.[17]

Policy Requirement:

☐ OCHA offices must adopt technical and organizational safeguards to promote data protection and privacy by design throughout the life cycle of data processing, in-line with section 10 of the UN Secretariat Data Protection and Privacy Policy.

Recommended Approach:

☐ Offices should incorporate data responsibility into data management by design when planning any data management activity. Designing for data responsibility includes, for example, the following steps and considerations:

- Establish clear and replicable standard operating procedures for data management activities. The IASC Operational Guidance includes a **Standard Operating Procedure for a Data Management Activity**. In addition, such SOPs should include information regarding applicable data subject rights where personal data is processed, and the channels for requests regarding these rights. The SOP should also include data retention and destruction timelines in line with applicable instructions from the data protection focal point.
- When selecting tools for data management, foster complementarity, interoperability (where appropriate, including with governmental and other local systems), and harmonization (including on terminology, typologies and data structure).
- Offer training to OCHA staff and partners on responsible data management, including on data security, the ISP and other guidance for the response, and on the SOPs for a given data management activity.
- Support measures for the safe management of data (e.g., for data anonymization, provision of secure storage and data transfer solutions, etc.).
- Adhere to relevant guidance and protocols on data responsibility and related processes and procedures, including ISPs. This includes ensuring all data that needs to be shared for defined purposes is made available through appropriate channels in a responsible manner, with the necessary safeguards for personal data and in compliance with applicable data protection frameworks.

Relevant Tool or Template:

Template for Designing for Data Responsibility

Standard Operating Procedure for a Data Management Activity

[17] There are a variety of data cycles and processes used in documentation across OCHA's different functions. The Guidelines present this cycle set of steps t to offer a frame for tips and outputs that support data responsibility within a given data management activity.

05 ESTABLISH DATA SHARING AGREEMENTS TO GOVERN THE TRANSFER OF PERSONAL DATA AND/OR NON-PERSONAL DATA IN A SENSITIVE CONTEXT

Purpose:

A data sharing agreement establishes the terms and conditions that govern the sharing of personal data or non-personal data in a sensitive context between two or more parties. Many data protection frameworks require a DSA as a necessary safeguard for sharing personal data. This type of agreement is essential to upholding legal, policy and normative requirements related to the sharing of personal data and non-personal data in a sensitive context.

Policy Requirement:

☐ Data sharing outside of the United Nations system must follow section 12 of the UN Secretariat Data Protection and Privacy Policy.

Recommended Approach:

☐ Always consult OCHA's Executive Office when developing data sharing agreements.

☐ Establish data sharing agreements whenever sharing personal data or sensitive non-personal data with other organizations.

☐ Data sharing agreements should be developed jointly by an HAO and IMO and negotiated with the data sharing partner.

☐ DSAs should always include instructions for data retention and destruction, as well as information regarding data subject rights (where personal data is shared).

Relevant Tool or Template:

Data Sharing Agreement Template

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

Purpose:

Data incident management enables actors to address data incidents and supports the development of a knowledge base to help prevent and better address future incidents. Communicating about data incidents fosters more coordinated approaches to incident management over time and creates awareness across the sector.

Policy Requirement:

☐ Where the data incident involves personal data or non-personal data in a sensitive context, OCHA must adhere to the obligations established in section 15 of the UN Secretariat Data Protection and Privacy Policy.

Recommended Approach:

☐ The SOP for Data Incident Management should be prepared jointly by an HAO and IMO and be approved by OCHA's data protection focal point and the Head of Office. It should be aligned with other incident management procedures (e.g., applicable UNDSS guidance).

☐ The SOP should include a process for notification, classification, treatment and closure of the incident. It should also specify appropriate channels for rectification and redress for individuals impacted by data incidents.

☐ Establish a data incident registry to capture key details about the nature, severity and resolution of each incident, as well as any mitigation measures taken to prevent future incidents.

☐ Share the data incident registry with the data protection focal point.

☐ OCHA offices should share their experience in managing and mitigating data incidents with other actors, i.e., at the cluster/sector and system-wide levels to foster more coordinated approaches to incident management.

Relevant Tool or Template:

OCHA SOP for Data Incident Management Template

OCHA Data Incident Registry Template

[21] Including forthcoming administrative issuances on data protection and privacy from the United Nations Secretariat.

07 ENSURE THE AVAILABILITY OF APPROPRIATE TOOLS FOR DATA MANAGEMENT WITHIN THE OFFICE[18]

Purpose:

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

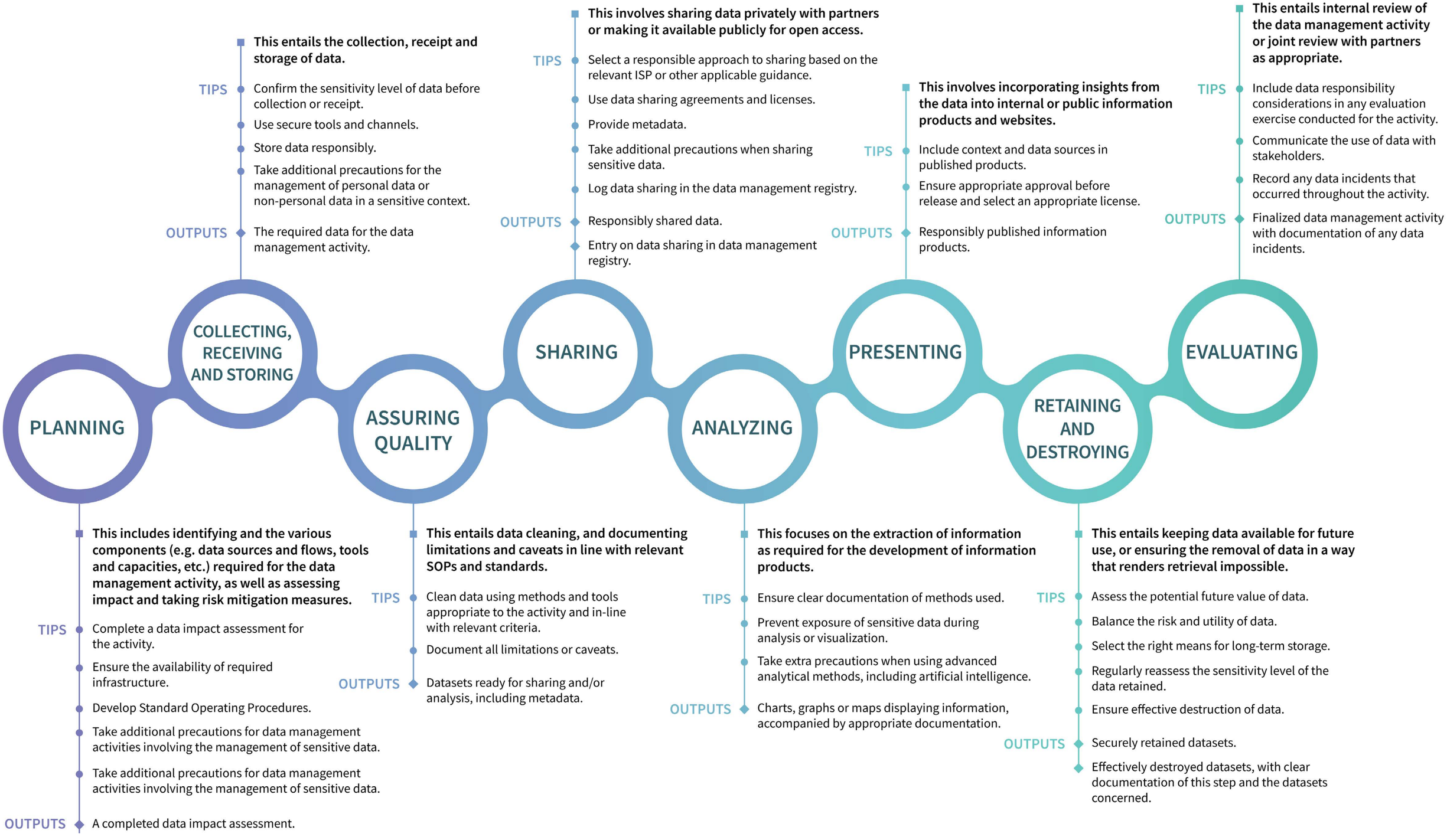
Recommended Approach:

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

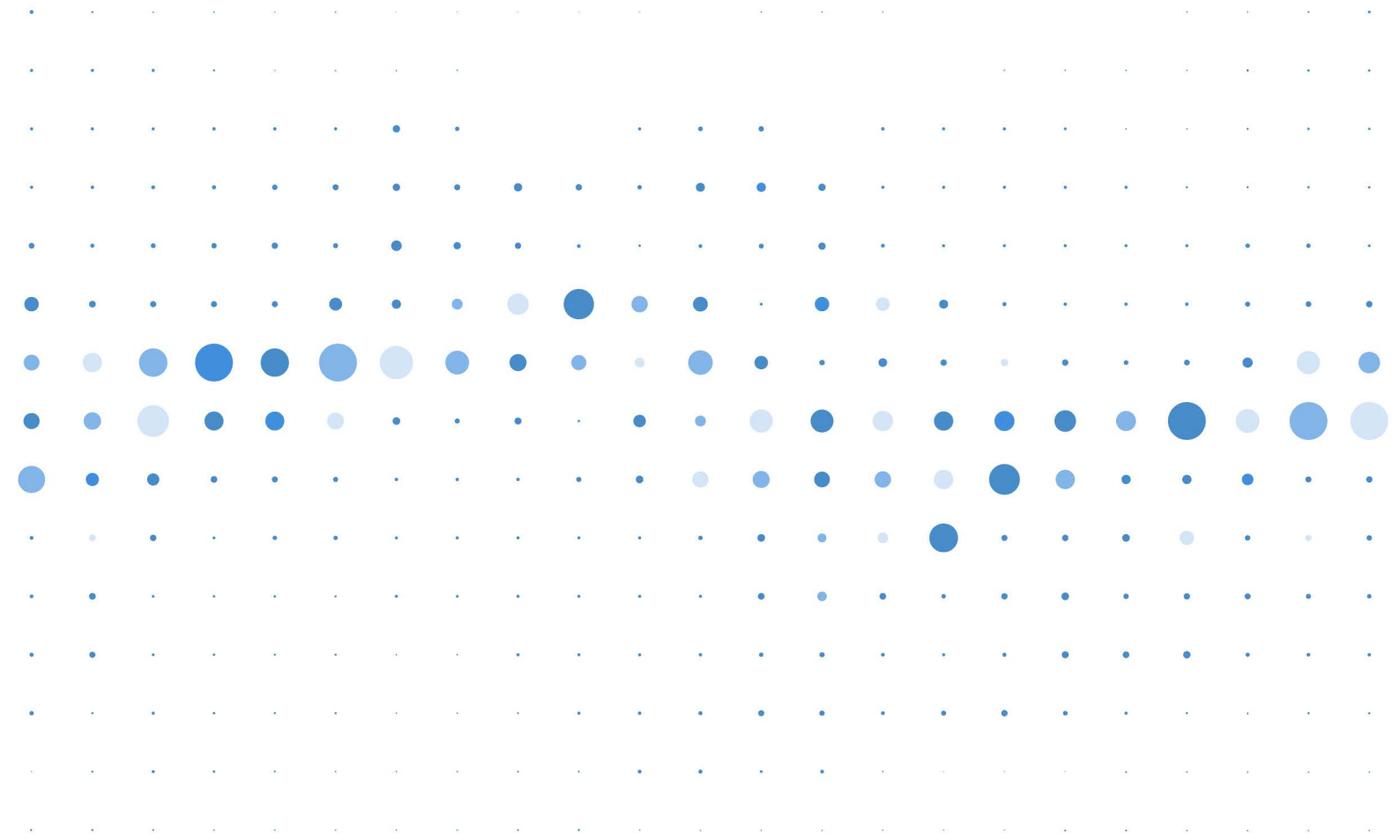
Relevant Tool or Template:

OCHA IMB SharePoint page on Technology Standards

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


PLANNING
This includes identifying and the various components (e.g. data sources and flows, tools and capacities, etc.) required for the data management activity, as well as assessing impact and taking risk mitigation measures.
TIPS
Complete a data impact assessment for the activity.
Ensure the availability of required infrastructure.
Develop Standard Operating Procedures.
Take additional precautions for data management activities involving the management of sensitive data.
Take additional precautions for data management activities involving the management of sensitive data.
OUTPUTS
A completed data impact assessment.
COLLECTING, RECEIVING AND STORING
This entails the collection, receipt and storage of data.
TIPS
Confirm the sensitivity level of data before collection or receipt.
Use secure tools and channels.
Store data responsibly.
Take additional precautions for the management of personal data or non-personal data in a sensitive context.
OUTPUTS
The required data for the data management activity.
ASSURING QUALITY
This entails data cleaning, and documenting limitations and caveats in line with relevant SOPs and standards.
TIPS
Clean data using methods and tools appropriate to the activity and in-line with relevant criteria.
Document all limitations or caveats.
OUTPUTS
Datasets ready for sharing and/or analysis, including metadata.
SHARING
This involves sharing data privately with partners or making it available publicly for open access.
TIPS
Select a responsible approach to sharing based on the relevant ISP or other applicable guidance.
Use data sharing agreements and licenses.
Provide metadata.
Take additional precautions when sharing sensitive data.
Log data sharing in the data management registry.
OUTPUTS
Responsibly shared data.
Entry on data sharing in data management registry.
ANALYZING
This focuses on the extraction of information as required for the development of information products.
TIPS
Ensure clear documentation of methods used.
Prevent exposure of sensitive data during analysis or visualization.
Take extra precautions when using advanced analytical methods, including artificial intelligence.
OUTPUTS
Charts, graphs or maps displaying information, accompanied by appropriate documentation.
PRESENTING
This involves incorporating insights from the data into internal or public information products and websites.
TIPS
Include context and data sources in published products.
Ensure appropriate approval before release and select an appropriate license.
OUTPUTS
Responsibly published information products.
RETAINING AND DESTROYING
This entails keeping data available for future use, or ensuring the removal of data in a way that renders retrieval impossible.
TIPS
Assess the potential future value of data.
Balance the risk and utility of data.
Select the right means for long-term storage.
Regularly reassess the sensitivity level of the data retained.
Ensure effective destruction of data.
OUTPUTS
Securely retained datasets.
Effectively destroyed datasets, with clear documentation of this step and the datasets concerned.
EVALUATING
This entails internal review of the data management activity or joint review with partners as appropriate.
TIPS
Include data responsibility considerations in any evaluation exercise conducted for the activity.
Communicate the use of data with stakeholders.
Record any data incidents that occurred throughout the activity.
OUTPUTS
Finalized data management activity with documentation of any data incidents.

3. ACCOUNTABILITY



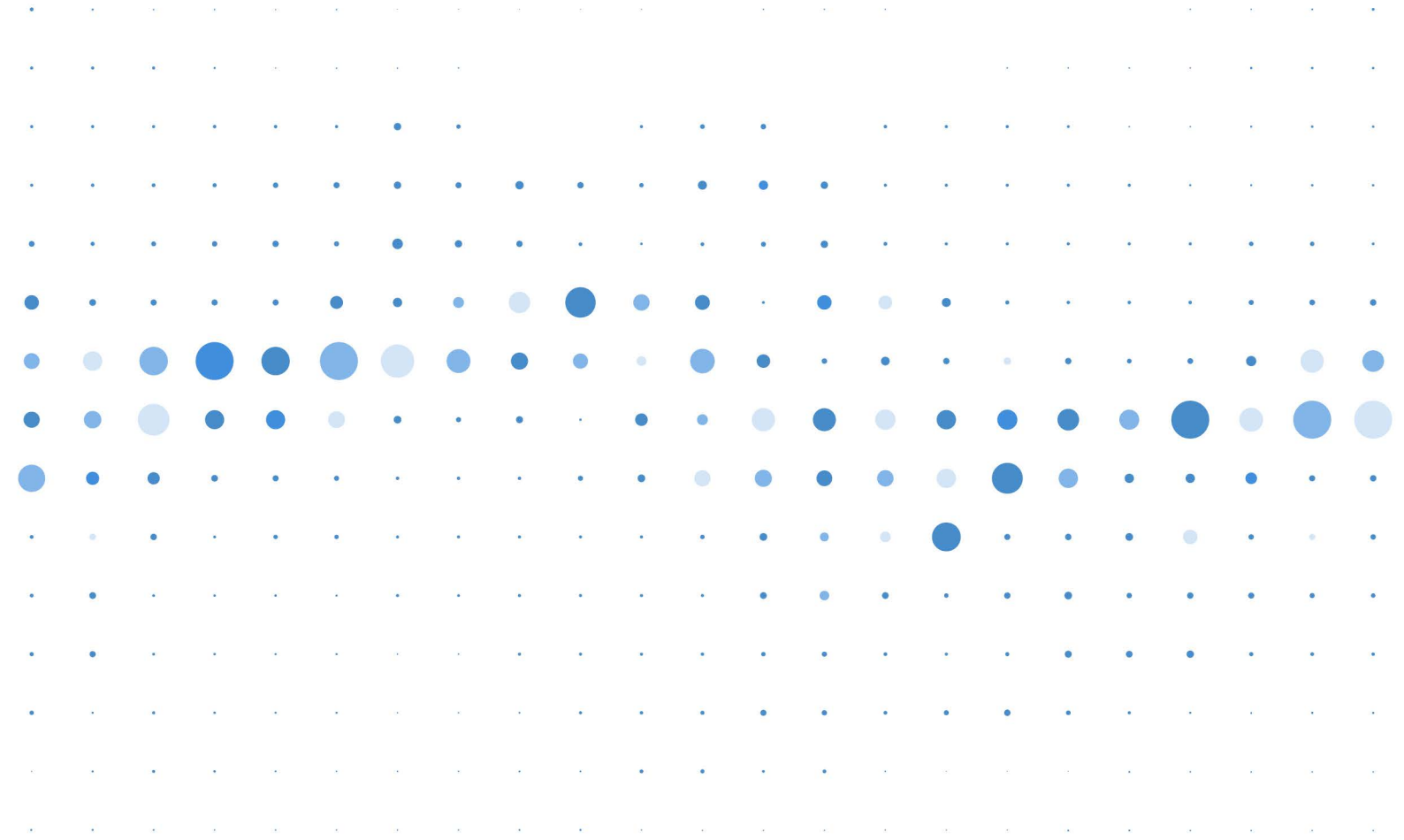
3 ACCOUNTABILITY

All OCHA staff and supporting personnel (e.g., contractors, stand-by partners, and secondments) who are authorized to manage data and related resources across OCHA should follow the Guidelines. Although effective adoption of the Guidelines requires action from all OCHA staff, accountability for adherence to the Guidelines rests with senior managers at headquarters and office level. The table below summarizes key responsibilities of different roles, groups and units in supporting adoption of the Guidelines and the UN Secretariat Data Protection and Privacy Policy.

ACCOUNTABILITIES RELATED TO THE ADOPTION OF THE OCHA DATA RESPONSIBILITY GUIDELINES

Group / Unit	Responsibilities
Under Secretary-General	• Fulfills the role of data steward as outlined in the UN Secretariat Data Protection and Privacy Policy.
Chief of IMB and head of IM Function	• Provides an annual report on adoption of the Data Responsibility Guidelines to the OCHA Data Steward.
Functional Leads, Directors and Branch Chiefs	• Promote staff awareness of and familiarity with the Guidelines. • Take corrective action and make related resources available for the management of data incidents.
Heads of Office and Section Chiefs	• Promote awareness and consultation of the Guidelines in day-to-day data management. • Ensure the availability of the required skills and resources for data responsibility. • Promote data responsibility beyond OCHA when engaging with partners.
Unit Heads	• Ensure appropriate application of the Guidelines in day-to-day data management work. • Promote data responsibility beyond OCHA when engaging with partners in the data ecosystem. • Support the HoO or Section Chief in the systematic reporting of any data incidents. • Systematically report any data incidents via the appropriate channel for tracking and support.
OCHA Data Protection Focal Points	• The responsibilities of the Data Protection Focal Point are outlined in sections 6 and 7 of the UN Secretariat Data Protection and Privacy Policy.
Humanitarian Affairs Officers and Information Management Officers	• Implement the actions for data responsibility at the relevant level(s) and in the context of their respective areas of focus • Report any data incidents via the appropriate channel.
Centre for Humanitarian Data	• Advise on best approaches to implement the Guidelines across OCHA. • Advocate for the use of the Guidelines. • Advise on data incident management. • Advise on priority areas for training and capacity development related to data responsibility.

4. RESOURCES AND SERVICES TO SUPPORT ADOPTION OF THE GUIDELINES



4 RESOURCES AND SERVICES TO SUPPORT ADOPTION OF THE GUIDELINES

There are a number of available resources that can help staff adopt the Guidelines. In addition, the Information Management Branch through the Centre for Humanitarian Data is committed to supporting offices and sections across OCHA in adopting the Guidelines. The Centre offers the following services upon request.

- **Introductory briefing**
  The Centre is available to provide briefings on data responsibility to offices or sections upon request. These briefings are designed to help staff gain a broad understanding of the Guidelines and address questions on how to initiate their implementation.

- **Diagnostic**
  The Centre will jointly conduct a Data Responsibility Diagnostic with all OCHA offices on an annual basis.

- **Ad-hoc advisory services**
  Offices or sections can contact the Centre with specific questions regarding the interpretation or application of the Guidelines.

- **Support missions**
  For contexts in which more in-depth support is required, the Centre is available to organize missions to support the adoption of the Guidelines and to facilitate conversations between OCHA staff and partners on issues related to data responsibility.

- **Templates**
  Templates are linked throughout the Guidelines. Reach out to learn more.

- **Training**
  The Centre offers tailored training on data responsibility for offices upon request and delivers sessions withinOCHA-wide training programmes.

- **Development of thematic guidance on data responsibility**
  The Centre works with different teams within OCHA to develop specific guidance[19] on adoption of data responsibility in different thematic areas.

[19] More information on the UN OCHA Centre for Humanitarian Data's work on data responsibility is available **here**. The Centre has developed a series of guidance notes on data responsibility, available **here**.

ANNEXES

ANNEX A

DEFINITIONS

Data: Re-interpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.[20]

Data impact assessment: A data impact assessment is a generic term to refer to a variety of tools that are used to determine the positive and negative consequences of a data management activity. These include commonly used – and sometimes legally required – tools such as Data Protection Impact Assessments and Privacy Impact Assessments.[21]

Data incidents: Event involving data management, such as the loss, destruction, alteration, acquisition, or disclosure of data and information, caused by accidental or intentional, unlawful or otherwise unauthorized purposes that have caused harm or have the potential to cause harm.[22]

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

Data management registry: A data management registry provides a summary of the key datasets being generated and managed by different actors in a context.[23]

Data processing: Any operation or set of operations that is performed on data or on sets of data, irrespective of the technology and processes used, including by automated means, by or on behalf of the Secretariat, including but not limited to collecting, registering, recording, structuring, storing, adapting, altering, cleaning, filing, retrieving, consulting, using, disseminating, disclosing, transferring, sharing, copying, making available, erasing and destroying.[24]

Data protection: The systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the processing of personal data.[25]

Data responsibility: The safe, ethical and effective management of personal and non-personal data for operational response, in accordance with established frameworks for personal data protection.

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.[26]

Data sensitivity: Classification of data based on the likelihood and severity of potential harm that may materialize as a result of its exposure in a particular context.[27]

Data sharing agreement: Agreement that establishes the terms and conditions that govern the sharing of personal data or sensitive non-personal data. It is primarily used for data sharing between two parties and typically established at the country level.[28]

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

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

[22] UN OCHA Centre for Humanitarian Data, **Guidance Note: Data Incident Management** (2019).

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

[24] UN Secretariat, **Secretary-General's bulletin on Data protection and privacy policy for the Secretariat of the United Nations**, ST/SGB/2024/3 (2024).

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

[26] UN OCHA Centre for Humanitarian Data, **Glossary**.

[27] UN OCHA Centre for Humanitarian Data, **Glossary**.

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

Data steward: The head of each entity, unless otherwise determined by the Secretary-General.[29]

Data subject: The data subject is any identified or identifiable natural person to whom personal data that are being processed by or on behalf of the Secretariat relate, including but not limited to a staff member, individual contractor or consultant, other United Nations personnel, an attendee at an official meeting or a beneficiary of assistance.[30]

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 management activity 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.

Identifiable natural person: An identifiable natural person is a natural person who can be directly or indirectly identified by means likely to be used, such as reasonably available expertise, resources and time, as well as data already available.[31]

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

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

Non-personal data: Any information which does not relate to a data subject. Non-personal data can be categorized in terms of origin, namely: data that has never related to a data subject, such as data about the context in which a response is taking place and data about humanitarian response actors and their activities; or data that was initially personal data but later made anonymous, such as data about the people affected by the humanitarian situation and their needs, the threats and vulnerabilities they face, and their capacities. Non-personal data includes Demographically Identifiable Information (DII) i.e., data that enables the identification of groups of individuals by demographically defining factors, such as ethnicity, gender, age, occupation, religion, or location.[32]

Non-personal data in a sensitive context: Information, in any form, that, while not relating to an identified or identifiable natural person, may, by reason of its sensitive context, put certain individuals and groups at risk of harm, including vulnerable or marginalized individuals and groups of individuals, such as children.[33]

Operational data management: The design of data management activities and subsequent collection or receipt, storage, processing, analysis, sharing, use, and retention and destruction of data and information by humanitarian actors. Such activities occur as part of humanitarian action throughout the planning and response cycle across clusters/sectors and include, but are not limited to, situational analysis, needs assessments, population data management, registration and enrollment, case management, communicating with affected populations, protection monitoring, and response monitoring and evaluation.[34]

Personal data: Information, in any form, that relates to an identified or identifiable natural person ('data subject').[35]

[29] UN Secretariat, **Secretary-General's bulletin on Data protection and privacy policy for the Secretariat of the United Nations**, ST/SGB/2024/3 (2024).

[30] UN Secretariat, **Secretary-General's bulletin on Data protection and privacy policy for the Secretariat of the United Nations**, ST/SGB/2024/3 (2024).

[31] UN Secretariat, **Secretary-General's bulletin on Data protection and privacy policy for the Secretariat of the United Nations**, ST/SGB/2024/3 (2024).

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

[33] Based on UN Secretariat, **Secretary-General's bulletin on Data protection and privacy policy for the Secretariat of the United Nations**, ST/SGB/2024/3 (2024).

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

[35] Based on UN Secretariat, **Secretary-General's bulletin on Data protection and privacy policy for the Secretariat of the United Nations**, ST/SGB/2024/3 (2024).

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

- harm (such as sanctions, discrimination) to any person, including the source of the information or other identifiable persons or groups, or;

- a negative impact on an organization's capacity to carry out its activities or on public perceptions of that organization.

Sensitive data includes personal data as well as 'non-personal data in a sensitive context'. Non-personal data in a sensitive context is information, in any form, that, while not relating to an identified or identifiable natural person, may, by reason of its sensitive context, put certain individuals and groups at risk of harm, including vulnerable or marginalized individuals and groups of individuals, such as children. The same types of data may have different levels of sensitivity in different contexts and sensitivity may change over time.

ANNEX B

DATA RESPONSIBILITY IN OCHA'S DATA MANAGEMENT CYCLE

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

TIPS AND OUTPUTS FOR DATA RESPONSIBILITY ACROSS THE DATA MANAGEMENT CYCLE

STEPS IN THE DATA MANAGEMENT CYCLE	TIPS AND OUTPUTS FOR DATA RESPONSIBILITY
1. PLANNING This includes identifying the various components (e.g. data sources and flows, tools and capacities) required for the data management activity, as well as assessing impact and taking risk mitigation measures.	**TIPS** ☐ Complete a data impact assessment for the activity. ☐ Ensure the availability of required infrastructure. ☐ Develop standard operating procedures. ☐ Take additional precautions for data management activities involving the management of sensitive data. ☐ Add the data management activity in the data management registry if available for the office. **OUTPUTS** ☐ A completed data impact assessment. ☐ A data sharing agreement, standard operating procedure and/or Terms of Reference, including a Data Retention and Destruction Schedule. ☐ Updated data management registry.
2. COLLECTING, RECEIVING AND STORING This entails the collection, receipt and storage of data.	**TIPS** ☐ Confirm the sensitivity level of data before collection or receipt. ☐ Use secure tools and channels. ☐ Store data responsibly. ☐ Take additional precautions for the management of personal data or non-personal data in a sensitive context. **OUTPUTS** ☐ The required data for the data management activity.
3. ASSURING QUALITY This entails data cleaning, and documenting limitations and caveats in line with relevant SOPs and standards.	**TIPS** ☐ Clean data using methods and tools appropriate to the activity and in-line with relevant criteria. ☐ Document all limitations or caveats. **OUTPUTS** ☐ Datasets ready for sharing and/or analysis, including metadata.

4. SHARING

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

TIPS

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

OUTPUTS

- ☐ Responsibly shared data.
- ☐ Entry on data sharing in data management registry.

5. ANALYZING

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

TIPS

- ☐ Ensure clear documentation of methods used.
- ☐ Prevent exposure of sensitive data during analysis or visualization.
- ☐ Take extra precautions when using advanced analytical methods, including artificial intelligence.

OUTPUTS

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

6. PRESENTING

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

TIPS

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

OUTPUTS

- ☐ Responsibly published information products.

7. RETAINING AND DESTROYING

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

TIPS

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

OUTPUTS

- ☐ Securely retained datasets.
- ☐ Effectively destroyed datasets, with clear documentation of this step and the datasets concerned.
- ☐ Comply with internal processes established by the Data Steward related to data retention.

8. EVALUATING

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

TIPS

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

OUTPUTS

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

ANNEX C

TEMPLATES FOR DATA RESPONSIBILITY

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

Templates from the IASC Operational Guidance:

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

Templates specific to OCHA:

- Data Responsibility Diagnostic (Office Level)
- Data Sharing Agreement
- Standard Operating Procedure for Data Incident Management (Office Level)
- Data Incident Registry

ANNEX D

FOUNDATIONS FOR DATA RESPONSIBILITY AT OCHA

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

Legal framework

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

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

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

Guidance from the UN Secretariat

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

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

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

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

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

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

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

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

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

UN Secretariat, 2024. Secretary-General's Bulletin on Data Protection and Privacy Policy, ST/SGB/2024/3: https://www.undocs.org/Home/Mobile?FinalSymbol=ST%2FSGB%2F2024%2F3&Language=E&DeviceType=Desktop&LangRequested=False.

Inter-Agency Standing Committee guidance

Inter-Agency Standing Committee (IASC), 2023. Operational Guidance on Data Responsibility in Humanitarian Action: https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action.

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

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