Overview of Revision Process for IASC Operational Guidance on Data Responsibility

InterAction Consultation
18 November 2022

Data Responsibility Working Group

- The Data Responsibility Working Group (DRWG) is a global coordination body working to advance data responsibility across the humanitarian system.

- The primary aim of the DRWG is to coordinate, support, and monitor collective action on data responsibility, primarily through the lens of the IASC Operational Guidance on Data Responsibility in Humanitarian Action.

DRWG CO-CHAIRS AND MEMBERS AS OF NOVEMBER 2022

Co-Chairs

DRC DANISH REFUGEE COUNCIL

IOM UN MIGRATION

OCHA centre for humdata

UNHCR The UN Refugee Agency

Members

CAFOD Catholic Agency for Overseas Development

care

cartong

CRS CATHOLIC RELIEF SERVICES

CLEAR Global

HEALTH CLUSTER

HOT Humanitarian OpenStreetMap Team

IFRC

IMPACT Shaping practices Influencing policies Impacting lives

INTERNATIONAL RESCUE COMMITTEE

JIPS Joint IDP Profiling Service

MERCY CORPS

MEDECINS SANS FRONTIERES

NRC NORWEGIAN REFUGEE COUNCIL

OXFAM International

Save the Children

UNESCO unesco

UNFPA

unicef

UNOPS

WFP

World Health Organization

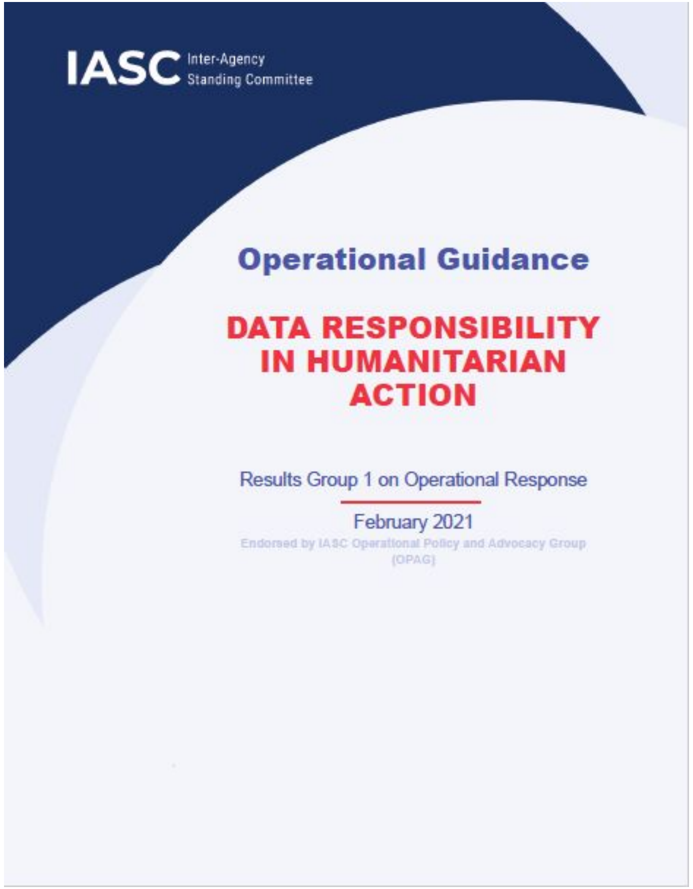
World Vision

Background on the IASC Operational Guidance

The **IASC Operational Guidance on Data Responsibility in Humanitarian Action** supports concrete steps for data responsibility in all phases of humanitarian action.

This Operational Guidance offers **a set of principles and actions** that support the implementation of data responsibility in humanitarian action.

It **complements and is informed by existing guidance** on data responsibility, both from development actors and within the broader humanitarian community.



IASC Inter-Agency Standing Committee

Operational Guidance

DATA RESPONSIBILITY IN HUMANITARIAN ACTION

Results Group 1 on Operational Response

February 2021

Endorsed by IASC Operational Policy and Advocacy Group (OPAG)

Endorsed February 2021

DEFINING DATA RESPONSIBILITY: SAFE, ETHICAL, AND EFFECTIVE DATA MANAGEMENT

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.

- **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.

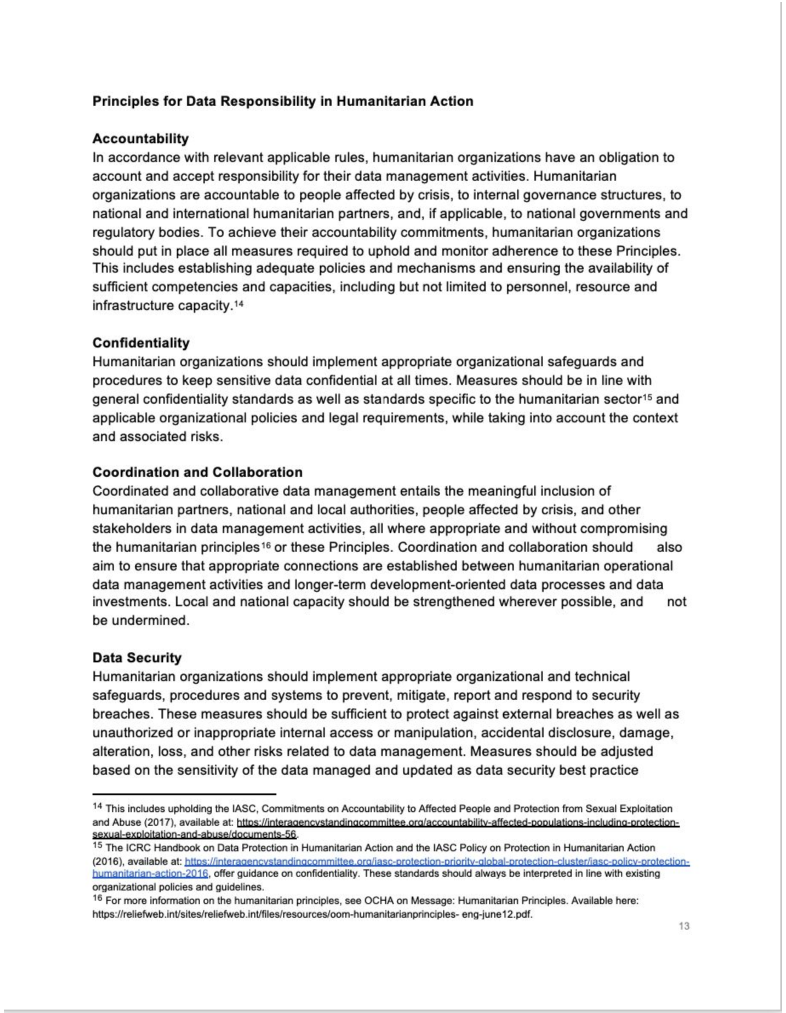
- **Ethical** | Data management activities are aligned with the established frameworks and standards for humanitarian ethics and data ethics.

- **Effective** | Data management activities achieve the purpose(s) for which they were carried out.

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

PRINCIPLES FOR DATA RESPONSIBILITY IN HUMANITARIAN ACTION

- ❖ Accountability
- ❖ Confidentiality
- ❖ Coordination and Collaboration
- ❖ Data Security
- ❖ Defined Purpose, Necessity and Proportionality
- ❖ Fairness and Legitimacy
- ❖ Human Rights-Based Approach
- ❖ People-Centred and Inclusive
- ❖ Personal Data Protection
- ❖ Quality
- ❖ Retention and Destruction
- ❖ Transparency



Principles for Data Responsibility in Humanitarian Action

Accountability
In accordance with relevant applicable rules, humanitarian organizations have an obligation to account and accept responsibility for their data management activities. Humanitarian organizations are accountable to people affected by crisis, to internal governance structures, to national and international humanitarian partners, and, if applicable, to national governments and regulatory bodies. To achieve their accountability commitments, humanitarian organizations should put in place all measures required to uphold and monitor adherence to these Principles. This includes establishing adequate policies and mechanisms and ensuring the availability of sufficient competencies and capacities, including but not limited to personnel, resource and infrastructure capacity.[14]

Confidentiality
Humanitarian organizations should implement appropriate organizational safeguards and procedures to keep sensitive data confidential at all times. Measures should be in line with general confidentiality standards as well as standards specific to the humanitarian sector[15] and applicable organizational policies and legal requirements, while taking into account the context and associated risks.

Coordination and Collaboration
Coordinated and collaborative data management entails the meaningful inclusion of humanitarian partners, national and local authorities, people affected by crisis, and other stakeholders in data management activities, all where appropriate and without compromising the humanitarian principles[16] or these Principles. Coordination and collaboration should also aim to ensure that appropriate connections are established between humanitarian operational data management activities and longer-term development-oriented data processes and data investments. Local and national capacity should be strengthened wherever possible, and not be undermined.

Data Security
Humanitarian organizations should implement appropriate organizational and technical safeguards, procedures and systems to prevent, mitigate, report and respond to security breaches. These measures should be sufficient to protect against external breaches as well as unauthorized or inappropriate internal access or manipulation, accidental disclosure, damage, alteration, loss, and other risks related to data management. Measures should be adjusted based on the sensitivity of the data managed and updated as data security best practice

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

[15] The ICRC Handbook on Data Protection in Humanitarian Action and the IASC Policy on Protection in Humanitarian Action (2016), available at: https://interagencystandingcommittee.org/iasc-protection-priority-global-protection-cluster/iasc-policy-protection-humanitarian-action-2016, offer guidance on confidentiality. These standards should always be interpreted in line with existing organizational policies and guidelines.

[16] For more information on the humanitarian principles, see OCHA on Message: Humanitarian Principles. Available here: https://reliefweb.int/sites/reliefweb.int/files/resources/oom-humanitarianprinciples- eng-june12.pdf.

AREAS OF ACTION FOR DATA RESPONSIBILITY

DATA RESPONSIBILITY DIAGNOSTIC

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

DATA ECOSYSTEM MAP AND DATA ASSET REGISTRY

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

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

DATA IMPACT ASSESSMENT[14]

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

DESIGNING FOR DATA RESPONSIBILITY

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

INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION

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

DATA SHARING AGREEMENT

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

DATA INCIDENT MANAGEMENT[16]

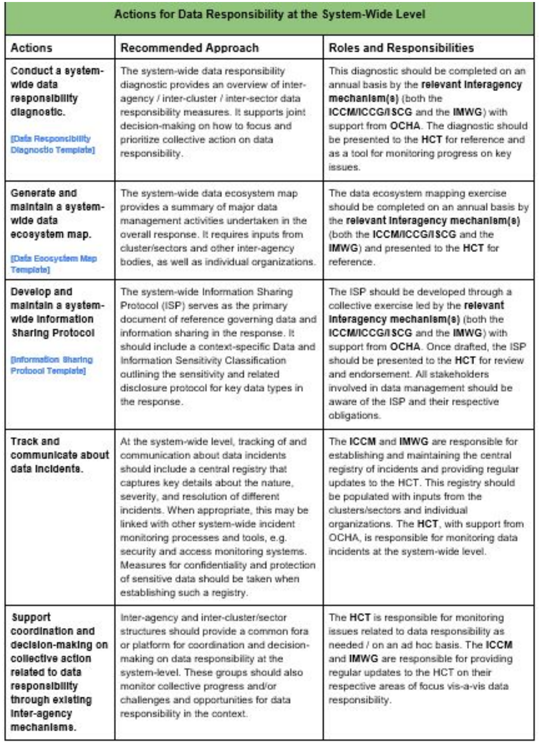
Managing, tracking, and communicating about data incidents requires standard operating procedures for incident management and a central registry or log that captures key details about the nature, severity, and resolution of each incident.

COORDINATION AND DECISION-MAKING ON COLLECTIVE ACTION FOR DATA RESPONSIBILITY

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

THREE LEVELS OF ACTIONS FOR DATA RESPONSIBILITY

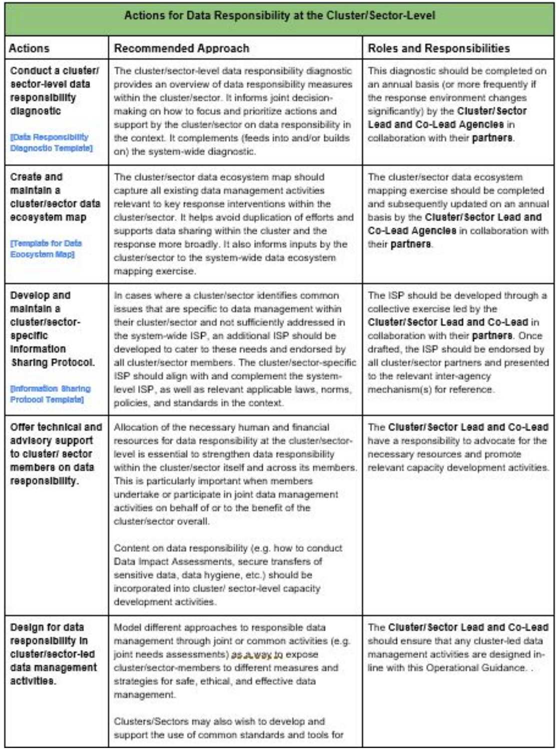
System-Wide



Actions for Data Responsibility at the System-Wide Level

Actions	Recommended Approach	Roles and Responsibilities
Conduct a system-wide data responsibility diagnostic. [Data Responsibility Diagnostic Template]	The system-wide data responsibility diagnostic provides an overview of inter-agency / inter-cluster / inter-sector data responsibility measures. It supports joint decision-making on how to focus and prioritize collective action on data responsibility.	This diagnostic should be completed on an annual basis by the **relevant interagency mechanism(s)** (both the **ICCM/ICCG/ISCG** and the **IMWG**) with support from **OCHA**. The diagnostic should be presented to the **HCT** for reference and as a tool for monitoring progress on key issues.
Generate and maintain a system-wide data ecosystem map. [Data Ecosystem Map Template]	The system-wide data ecosystem map provides a summary of major data management activities undertaken in the overall response. It requires inputs from cluster/sectors and other inter-agency bodies, as well as individual organizations.	The data ecosystem mapping exercise should be completed on an annual basis by the **relevant interagency mechanism(s)** (both the **ICCM/ICCG/ISCG** and the **IMWG**) and presented to the **HCT** for reference.
Develop and maintain a system-wide Information Sharing Protocol [Information Sharing Protocol Template]	The system-wide Information Sharing Protocol (ISP) serves as the primary document of reference governing data and information sharing in the response. It should include a context-specific Data and Information Sensitivity Classification outlining the sensitivity and related disclosure protocol for key data types in the response.	The ISP should be developed through a collective exercise led by the **relevant interagency mechanism(s)** (both the **ICCM/ICCG/ISCG** and the **IMWG**) with support from **OCHA**. Once drafted, the ISP should be presented to the **HCT** for review and endorsement. All stakeholders involved in data management should be aware of the ISP and their respective obligations.
Track and communicate about data incidents.	At the system-wide level, tracking of and communication about data incidents should include a central registry that captures key details about the nature, severity, and resolution of different incidents. When appropriate, this may be linked with other system-wide incident monitoring processes and tools, e.g. security and access monitoring systems. Measures for confidentiality and protection of sensitive data should be taken when establishing such a registry.	The **ICCM** and **IMWG** are responsible for establishing and maintaining the central registry of incidents and providing regular updates to the HCT. This registry should be populated with inputs from the clusters/sectors and individual organizations. The **HCT**, with support from OCHA, is responsible for monitoring data incidents at the system-wide level.
Support coordination and decision-making on collective action related to data responsibility through existing inter-agency mechanisms.	Inter-agency and inter-cluster/sector structures should provide a common fora or platform for coordination and decision-making on data responsibility at the system-level. These groups should also monitor collective progress and/or challenges and opportunities for data responsibility in the context.	The **HCT** is responsible for monitoring issues related to data responsibility as needed / on an ad hoc basis. The **ICCM** and **IMWG** are responsible for providing regular updates to the HCT on their respective areas of focus vis-a-vis data responsibility.

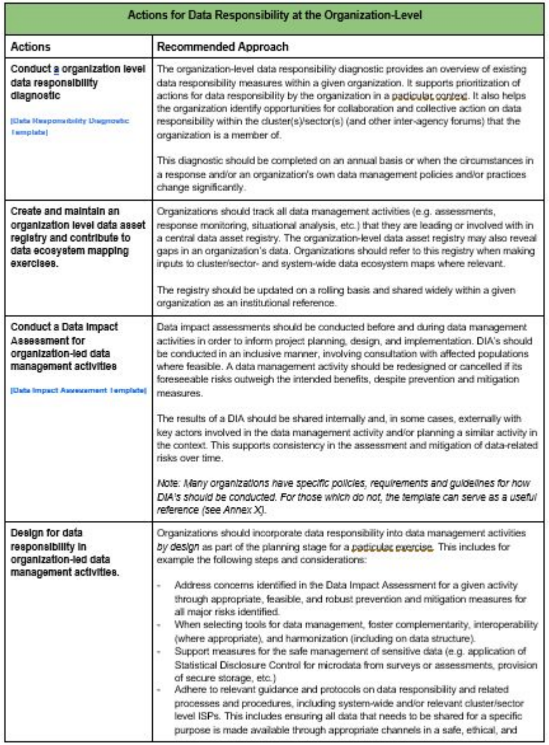
Cluster/Sector



Actions for Data Responsibility at the Cluster/Sector-Level

Actions	Recommended Approach	Roles and Responsibilities
Conduct a cluster/ sector-level data responsibility diagnostic [Data Responsibility Diagnostic Template]	The cluster/sector-level data responsibility diagnostic provides an overview of data responsibility measures within the cluster/sector. It informs joint decision-making on how to focus and prioritize actions and support by the cluster/sector on data responsibility in the context. It complements (feeds into and/or builds on) the system-wide diagnostic.	This diagnostic should be completed on an annual basis (or more frequently if the response environment changes significantly) by the **Cluster/ Sector Lead and Co-Lead Agencies** in collaboration with their **partners**.
Create and maintain a cluster/sector data ecosystem map [Template for Data Ecosystem Map]	The cluster/sector data ecosystem map should capture all existing data management activities relevant to key response interventions within the cluster/sector. It helps avoid duplication of efforts and supports data sharing within the cluster and the response more broadly. It also informs inputs by the cluster/sector to the system-wide data ecosystem mapping exercise.	The cluster/sector data ecosystem mapping exercise should be completed and subsequently updated on an annual basis by the **Cluster/ Sector Lead and Co-Lead Agencies** in collaboration with their **partners**.
Develop and maintain a cluster/sector-specific Information Sharing Protocol. [Information Sharing Protocol Template]	In cases where a cluster/sector identifies common issues that are specific to data management within their cluster/sector and not sufficiently addressed in the system-wide ISP, an additional ISP should be developed to cater to these needs and endorsed by all cluster/sector members. The cluster/sector-specific ISP should align with and complement the system-level ISP, as well as relevant applicable laws, norms, policies, and standards in the context.	The ISP should be developed through a collective exercise led by the **Cluster/ Sector Lead and Co-Lead** in collaboration with their **partners**. Once drafted, the ISP should be endorsed by all cluster/sector partners and presented to the relevant inter-agency mechanism(s) for reference.
Offer technical and advisory support to cluster/ sector members on data responsibility.	Allocation of the necessary human and financial resources for data responsibility at the cluster/sector-level is essential to strengthen data responsibility within the cluster/sector itself and across its members. This is particularly important when members undertake or participate in joint data management activities on behalf of or to the benefit of the cluster/sector overall. Content on data responsibility (e.g. how to conduct Data Impact Assessments, secure transfers of sensitive data, data hygiene, etc.) should be incorporated into cluster/ sector-level capacity development activities.	The **Cluster/ Sector Lead and Co-Lead** have a responsibility to advocate for the necessary resources and promote relevant capacity development activities.
Design for data responsibility in cluster/sector-led data management activities.	Model different approaches to responsible data management through joint or common activities (e.g. joint needs assessments) as a way to expose cluster/sector-members to different measures and strategies for safe, ethical, and effective data management. Clusters/Sectors may also wish to develop and support the use of common standards and tools for	The **Cluster/ Sector Lead and Co-Lead** should ensure that any cluster-led data management activities are designed in-line with this Operational Guidance. .

Organization

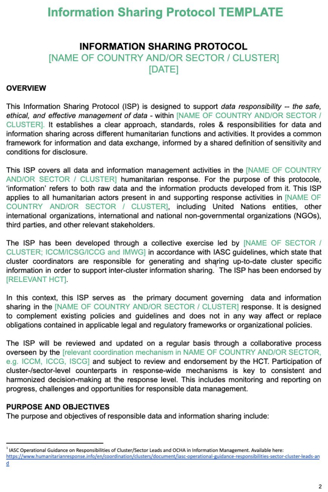


Actions for Data Responsibility at the Organization-Level

Actions	Recommended Approach
Conduct a organization level data responsibility diagnostic [Data Responsibility Diagnostic Template]	The organization-level data responsibility diagnostic provides an overview of existing data responsibility measures within a given organization. It supports prioritization of actions for data responsibility by the organization in a particular context. It also helps the organization identify opportunities for collaboration and collective action on data responsibility within the cluster(s)/sector(s) (and other inter-agency forums) that the organization is a member of. This diagnostic should be completed on an annual basis or when the circumstances in a response and/or an organization's own data management policies and/or practices change significantly.
Create and maintain an organization level data asset registry and contribute to data ecosystem mapping exercises.	Organizations should track all data management activities (e.g. assessments, response monitoring, situational analysis, etc.) that they are leading or involved with in a central data asset registry. The organization-level data asset registry may also reveal gaps in an organization's data. Organizations should refer to this registry when making inputs to cluster/sector- and system-wide data ecosystem maps where relevant. The registry should be updated on a rolling basis and shared widely within a given organization as an institutional reference.
Conduct a Data Impact Assessment for organization-led data management activities [Data Impact Assessment Template]	Data impact assessments should be conducted before and during data management activities in order to inform project planning, design, and implementation. DIA's should be conducted in an inclusive manner, involving consultation with affected populations where feasible. A data management activity should be redesigned or cancelled if its foreseeable risks outweigh the intended benefits, despite prevention and mitigation measures. The results of a DIA should be shared internally and, in some cases, externally with key actors involved in the data management activity and/or planning a similar activity in the context. This supports consistency in the assessment and mitigation of data-related risks over time. *Note: Many organizations have specific policies, requirements and guidelines for how DIA's should be conducted. For those which do not, the template can serve as a useful reference (see Annex X).*
Design for data responsibility in organization-led data management activities.	Organizations should incorporate data responsibility into data management activities *by design* as part of the planning stage for a particular exercise. This includes for example the following steps and considerations: - Address concerns identified in the Data Impact Assessment for a given activity through appropriate, feasible, and robust prevention and mitigation measures for all major risks identified. - When selecting tools for data management, foster complementarity, interoperability (where appropriate), and harmonization (including on data structure). - Support measures for the safe management of sensitive data (e.g. application of Statistical Disclosure Control for microdata from surveys or assessments, provision of secure storage, etc.) - Adhere to relevant guidance and protocols on data responsibility and related processes and procedures, including system-wide and/or relevant cluster/sector level ISPs. This includes ensuring all data that needs to be shared for a specific purpose is made available through appropriate channels in a safe, ethical, and

TOOLS AND TEMPLATES FOR DATA RESPONSIBILITY

❖ Examples of Principles in Practice
❖ Data Responsibility Diagnostic Tool
❖ Data Ecosystem Map and Asset Registry Template
❖ Information Sharing Protocol Template (including a Data Sensitivity Classification)
❖ Data Sharing Agreement Builder
❖ Data Impact Assessment Template
❖ Standard Operating Procedure for Data Incident Management



Information Sharing Protocol TEMPLATE

INFORMATION SHARING PROTOCOL
[NAME OF COUNTRY AND/OR SECTOR / CLUSTER]
[DATE]

OVERVIEW

This Information Sharing Protocol (ISP) is designed to support *data responsibility -- the safe, ethical, and effective management of data* - within [NAME OF COUNTRY AND/OR SECTOR / CLUSTER]. It establishes a clear approach, standards, roles & responsibilities for data and information sharing across different humanitarian functions and activities. It provides a common framework for information and data exchange, informed by a shared definition of sensitivity and conditions for disclosure.

This ISP covers all data and information management activities in the [NAME OF COUNTRY AND/OR SECTOR / CLUSTER] humanitarian response. For the purpose of this protocole, 'information' refers to both raw data and the information products developed from it. This ISP applies to all humanitarian actors present in and supporting response activities in [NAME OF COUNTRY AND/OR SECTOR / CLUSTER], including United Nations entities, other international organizations, international and national non-governmental organizations (NGOs), third parties, and other relevant stakeholders.

The ISP has been developed through a collective exercise led by [NAME OF SECTOR / CLUSTER; ICCM/ICSG/ICCG and IMWG] in accordance with IASC guidelines, which state that cluster coordinators are responsible for generating and sharing up-to-date cluster specific information in order to support inter-cluster information sharing. The ISP has been endorsed by [RELEVANT HCT].

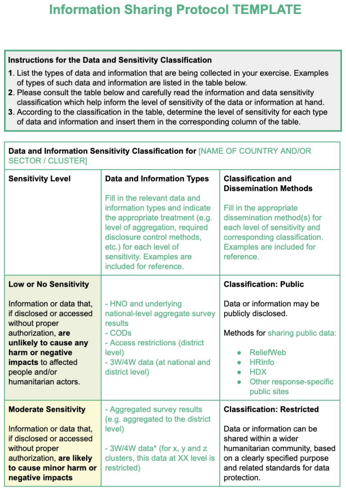
In this context, this ISP serves as the primary document governing data and information sharing in the [NAME OF COUNTRY AND/OR SECTOR / CLUSTER] response. It is designed to complement existing policies and guidelines and does not in any way affect or replace obligations contained in applicable legal and regulatory frameworks or organizational policies.

The ISP will be reviewed and updated on a regular basis through a collaborative process overseen by the [relevant coordination mechanism in NAME OF COUNTRY AND/OR SECTOR, e.g. ICCM, ICCG, ISCG] and subject to review and endorsement by the HCT. Participation of cluster-/sector-level counterparts in response-wide mechanisms is key to consistent and harmonized decision-making at the response level. This includes monitoring and reporting on progress, challenges and opportunities for responsible data management.

PURPOSE AND OBJECTIVES
The purpose and objectives of responsible data and information sharing include:

[1] IASC Operational Guidance on Responsibilities of Cluster/Sector Leads and OCHA in Information Management. Available here: https://www.humanitarianresponse.info/en/coordination/clusters/document/iasc-operational-guidance-responsibilities-sector-cluster-leads-and

2

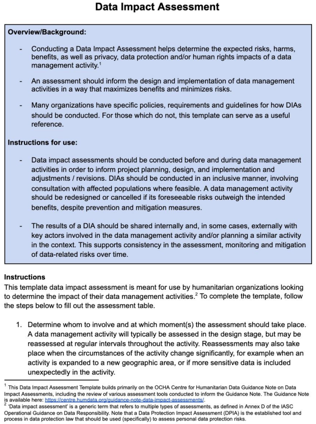


Information Sharing Protocol TEMPLATE

Instructions for the Data and Sensitivity Classification
1. List the types of data and information that are being collected in your exercise. Examples of types of such data and information are listed in the table below.
2. Please consult the table below and carefully read the information and data sensitivity classification which help inform the level of sensitivity of the data or information at hand.
3. According to the classification in the table, determine the level of sensitivity for each type of data and information and insert them in the corresponding column of the table.

Data and Information Sensitivity Classification for [NAME OF COUNTRY AND/OR SECTOR / CLUSTER]

Sensitivity Level	**Data and Information Types** Fill in the relevant data and information types and indicate the appropriate treatment (e.g. level of aggregation, required disclosure control methods, etc.) for each level of sensitivity. Examples are included for reference.	**Classification and Dissemination Methods** Fill in the appropriate dissemination method(s) for each level of sensitivity and corresponding classification. Examples are included for reference.
Low or No Sensitivity 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.	- HNO and underlying national-level aggregate survey results - CODs - Access restrictions (district level) - 3W/4W data (at national and district level)	**Classification: Public** Data or information may be publicly disclosed. Methods for sharing public data: ● ReliefWeb ● HRInfo ● HDX ● Other response-specific public sites
Moderate Sensitivity Information or data that, if disclosed or accessed without proper authorization, **are likely to cause minor harm or negative impacts**	- Aggregated survey results (e.g. aggregated to the district level) - 3W/4W data* (for x, y and z clusters, this data at XX level is restricted)	**Classification: Restricted** Data or information can be shared within a wider humanitarian community, based on a clearly specified purpose and related standards for data protection.



2

Data Impact Assessment

Overview/Background:

- Conducting a Data Impact Assessment helps determine the expected risks, harms, benefits, as well as privacy, data protection and/or human rights impacts of a data management activity.[1]
- An assessment should inform the design and implementation of data management activities in a way that maximizes benefits and minimizes risks.
- Many organizations have specific policies, requirements and guidelines for how DIAs should be conducted. For those which do not, this template can serve as a useful reference.

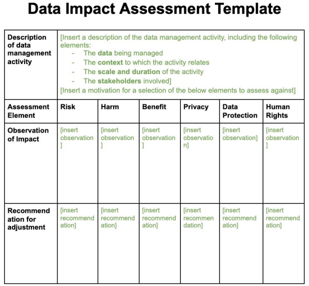
Instructions for use:

- Data impact assessments should be conducted before and during data management activities in order to inform project planning, design, and implementation and adjustments / revisions. DIAs should be conducted in an inclusive manner, involving consultation with affected populations where feasible. A data management activity should be redesigned or cancelled if its foreseeable risks outweigh the intended benefits, despite prevention and mitigation measures.
- The results of a DIA should be shared internally and, in some cases, externally with key actors involved in the data management activity and/or planning a similar activity in the context. This supports consistency in the assessment, monitoring and mitigation of data-related risks over time.

Instructions
This template data impact assessment is meant for use by humanitarian organizations looking to determine the impact of their data management activities.[2] To complete the template, follow the steps below to fill out the assessment table.

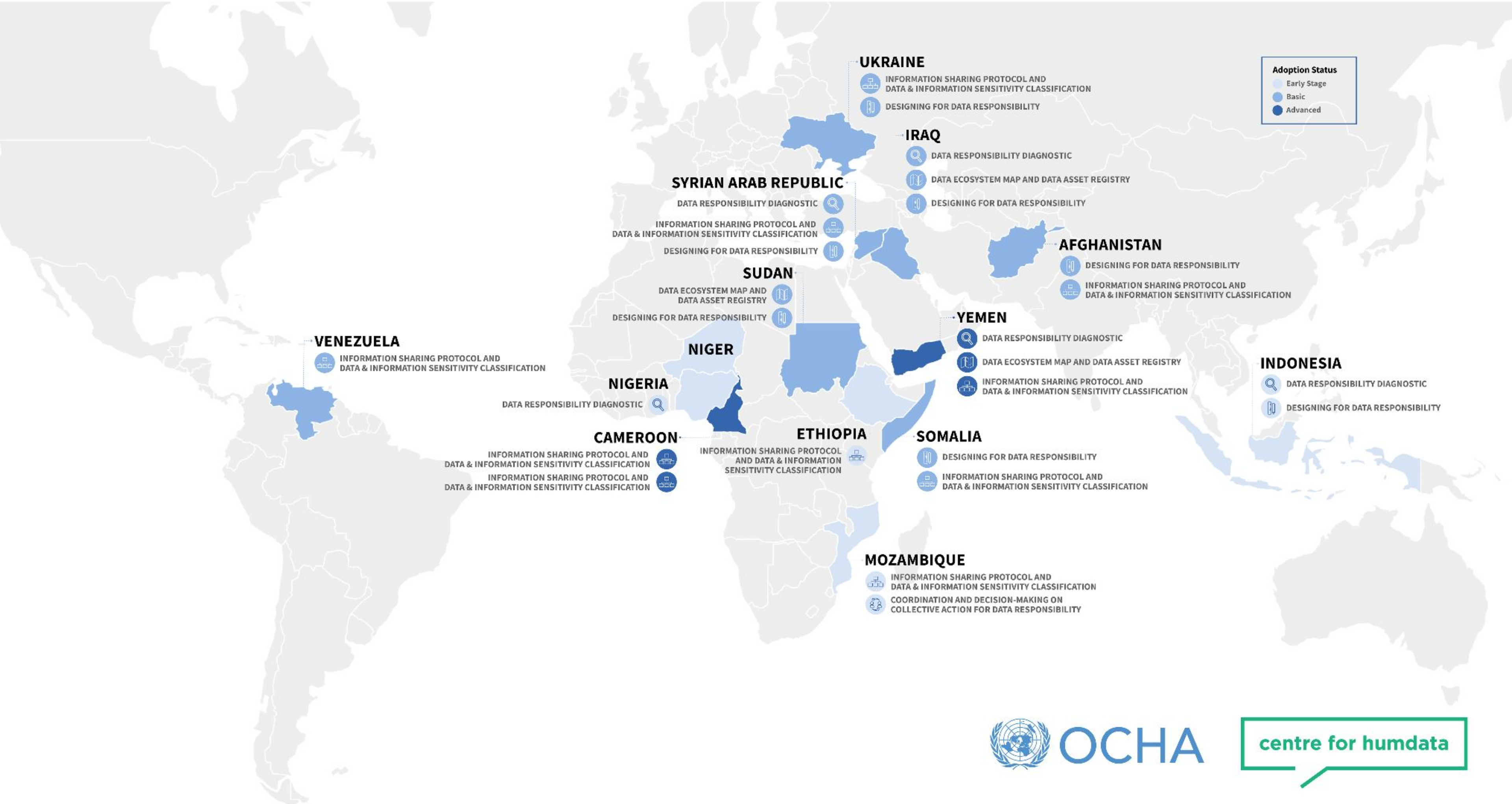
1. Determine whom to involve and at which moment(s) the assessment should take place. A data management activity will typically be assessed in the design stage, but may be reassessed at regular intervals throughout the activity. Reassessments may also take place when the circumstances of the activity change significantly, for example when an activity is expanded to a new geographic area, or if more sensitive data is included unexpectedly in the activity.

[1] This Data Impact Assessment Template builds primarily on the OCHA Centre for Humanitarian Data Guidance Note on Data Impact Assessments, including the review of various assessment tools conducted to inform the Guidance Note. The Guidance Note is available here: https://centre.humdata.org/guidance-note-data-impact-assessments/.
[2] 'Data impact assessment' is a generic term that refers to multiple types of assessments, as defined in Annex D of the IASC Operational Guidance on Data Responsibility. Note that a Data Protection Impact Assessment (DPIA) is the established tool and process in data protection law that should be used (specifically) to assess personal data protection risks.



Data Impact Assessment Template

Description of data management activity	[Insert a description of the data management activity, including the following elements: - The **data** being managed - The **context** to which the activity relates - The **scale and duration** of the activity - The **stakeholders** involved] [Insert a motivation for a selection of the below elements to assess against]					
Assessment Element	**Risk**	**Harm**	**Benefit**	**Privacy**	**Data Protection**	**Human Rights**
Observation of Impact	[insert observation]	[insert observation]	[insert observation]	[insert observation]	[insert observation]	[insert observation]
Recommendation for adjustment	[insert recommendation]	[insert recommendation]	[insert recommendation]	[insert recommendation]	[insert recommendation]	[insert recommendation]



Adoption Status

- ● Early Stage
- ● Basic
- ● Advanced

UKRAINE

- INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION
- DESIGNING FOR DATA RESPONSIBILITY

IRAQ

- DATA RESPONSIBILITY DIAGNOSTIC
- DATA ECOSYSTEM MAP AND DATA ASSET REGISTRY
- DESIGNING FOR DATA RESPONSIBILITY

SYRIAN ARAB REPUBLIC

- DATA RESPONSIBILITY DIAGNOSTIC
- INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION
- DESIGNING FOR DATA RESPONSIBILITY

AFGHANISTAN

- DESIGNING FOR DATA RESPONSIBILITY
- INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION

SUDAN

- DATA ECOSYSTEM MAP AND DATA ASSET REGISTRY
- DESIGNING FOR DATA RESPONSIBILITY

YEMEN

- DATA RESPONSIBILITY DIAGNOSTIC
- DATA ECOSYSTEM MAP AND DATA ASSET REGISTRY
- INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION

VENEZUELA

- INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION

NIGER

NIGERIA

- DATA RESPONSIBILITY DIAGNOSTIC

INDONESIA

- DATA RESPONSIBILITY DIAGNOSTIC
- DESIGNING FOR DATA RESPONSIBILITY

CAMEROON

- INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION
- INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION

ETHIOPIA

- INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION

SOMALIA

- DESIGNING FOR DATA RESPONSIBILITY
- INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION

MOZAMBIQUE

- INFORMATION SHARING PROTOCOL AND DATA & INFORMATION SENSITIVITY CLASSIFICATION
- COORDINATION AND DECISION-MAKING ON COLLECTIVE ACTION FOR DATA RESPONSIBILITY

OCHA

centre for humdata

Revision Process

REVISION PROCESS

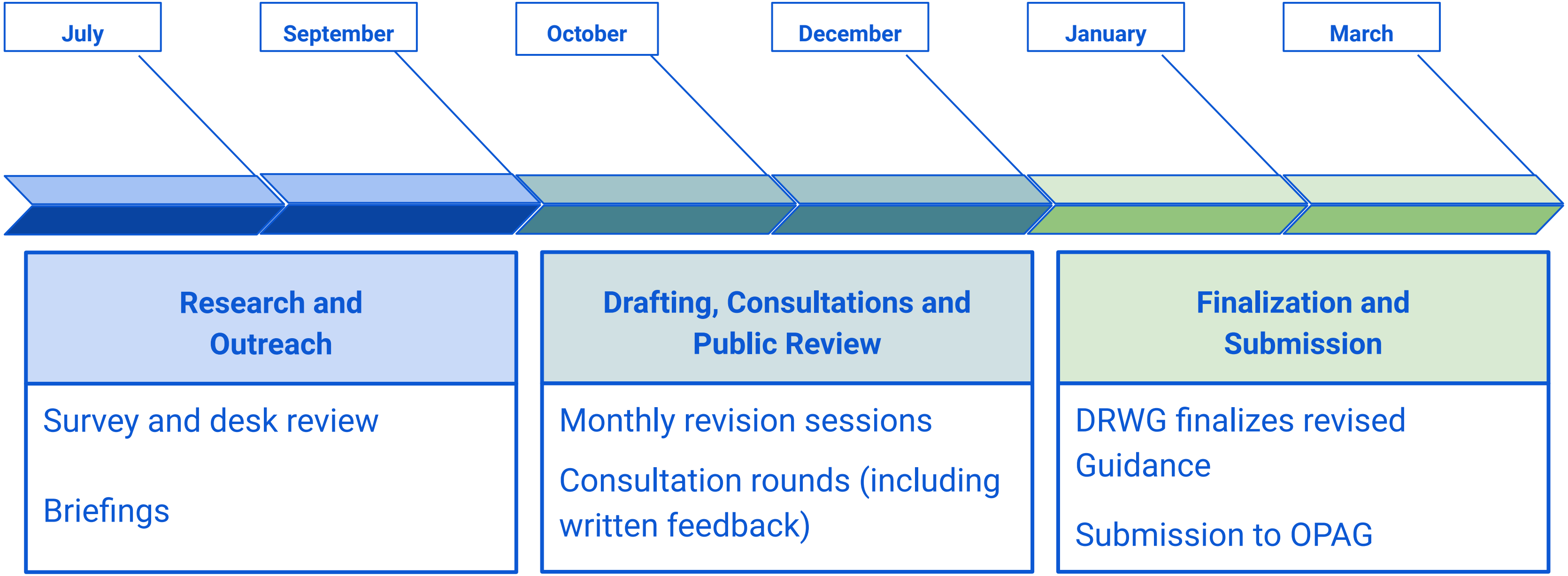
IASC OPAG Approval and Next Steps

➔ IASC committed to reviewing and updating the Operational Guidance through a collaborative and consultative process every two years

➔ On 15 June, IASC Operational Policy and Advocacy Group (OPAG) agreed to delegate authority for revision of OG to DRWG

→ ***27 Feb 2023***: Plan to submit final draft to OPAG for formal review and endorsement

REVISION PROCESS



July

September

October

December

January

March

Research and Outreach

Survey and desk review

Briefings

Drafting, Consultations and Public Review

Monthly revision sessions

Consultation rounds (including written feedback)

Finalization and Submission

DRWG finalizes revised Guidance

Submission to OPAG

Discussion

Questions?