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)

OPERATIONAL GUIDANCE

DATA RESPONSIBILITY IN HUMANITARIAN ACTION

Inter-Agency Standing Committee
Results Groups 1 on Operational Response

February 2021

Table of Contents

Foreword

Data responsibility is paramount as the humanitarian system collects and shares more data than ever before. Just as the COVID-19 pandemic has exacerbated existing humanitarian crises, it has also increased our reliance on digital technologies and timely data.

When we talk about data in humanitarian settings, we are talking about the world's most vulnerable people: a record 235 million people will need humanitarian assistance and protection in 2021. New technologies and data sources are helping us to make faster, more informed decisions and we are reaching more people with assistance every year. However, the ways in which data is collected, shared and used by individual organizations and across the humanitarian system can present challenges to the privacy and security of affected people. In order to protect the people, we seek to help, we must be able to navigate the technical and ethical issues involved with managing different types of data. Data can place already vulnerable people at greater risk of harm or exploitation, when not handled responsibly.

In recent years we have seen the development of principles, policies, and strategies for the responsible management of data in humanitarian action but gaps remain between global frameworks and their practical application in field operations.

The *Inter-Agency Standing Committee Operational Guidance on Data Responsibility in Humanitarian Action* is a welcome and timely step towards collectively addressing the challenges and opportunities in this area. It comes amid a growing global recognition of the importance of data responsibility.

This system-wide Operational Guidance, which is a first, will ensure concrete steps for data responsibility in all phases of humanitarian action. It is the result of an inclusive and consultative process, involving more than 250 stakeholders from the humanitarian sector. Partners across the system will implement these guidelines in accordance with their respective mandates and the decisions of their governing bodies.

I encourage the members of the IASC and the broader humanitarian community to support the responsible use of data through the implementation of this Operational Guidance.

Mark Lowcock
Under-Secretary-General for Humanitarian Affairs and Emergency Relief Coordinator,
United Nations

Executive Summary

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.

Ensuring we 'do no harm' while maximizing the benefits of data requires collective action that extends across all levels of the humanitarian system. Humanitarians must be careful when handling data to avoid placing already vulnerable individuals and communities at further risk. This is especially important in contexts where the urgency of humanitarian needs drives pressure for fast, sometimes untested, data solutions, and the politicization of data can have more extreme consequences for people. For example, disclosing the location or particular identity or affiliation of an individual or community could lead to targeted attacks, social exclusion and/or stigma, amongst other potential harms. In addition to avoiding harm, the safe, ethical and effective management of data has a number of benefits: it can lead to more informed and transparent decision-making, more efficient humanitarian response, and increased trust among humanitarian actors and with the people they seek to serve.

The implementation of data responsibility in practice is often inconsistent within and across humanitarian response contexts. This is true despite established principles, norms and professional standards regarding respect for the rights of affected populations; the range of resources on data responsibility available in the wider international data community; as well as significant efforts by many humanitarian organizations to develop and update their policies and guidance in this area. However, given that the humanitarian data ecosystem is inherently interconnected, no individual organization can tackle all these challenges alone. While each organization is responsible for its own data, humanitarians under the Inter-Agency Standing Committee (IASC) – which brings together United Nations (UN) entities, Non-Governmental Organization (NGO) consortia and the International Red Cross and Red Crescent Movement – need common normative, system-wide guidance to inform individual and collective action and to uphold a high standard for data responsibility in different operating environments.

In view of this, the IASC Results Group 1 established a Sub-Group[1] on Data Responsibility in January 2020 to develop this joint, system-wide **Operational Guidance on Data Responsibility in Humanitarian Action**.

The Operational Guidance is divided into four sections:

- The first section describes the **rationale and approach** for the Guidance, offers an **overview of data responsibility in humanitarian action**, and clarifies the **audience and scope** of the document.

[1] The Sub-Group was co-led by the International Organization for Migration (IOM), the OCHA Centre for Humanitarian Data, and the United Nations High Commissioner for Refugees (UNHCR) and comprised twenty member organizations representing different stakeholders within the humanitarian system. The Sub-Group included representatives from CARE, CRS, DRC, ICRC, IFRC, IRC, IOM, JIPS, Mercy Corps, MSF, NRC, OCHA, OHCHR, Oxfam, Save the Children, UNFPA, UNHCR, UNICEF, WFP and WHO. See Annex D for more information on the process the Sub-Group followed to develop this Operational Guidance.

- The second section presents a set of **Principles for Data Responsibility in Humanitarian Action**.
- The third section describes **key actions for data responsibility** to be taken at different levels of humanitarian response, including specific **roles and responsibilities** for realizing these actions.
- The fourth section is a set of **Annexes** that offer **key definitions**, examples of **templates and tools for data responsibility**, **resources and references**, and **background information on the development of the Operational Guidance**.

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

Defining Data Responsibility

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.[2]

- **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[3] 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 as defined below.

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

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

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.

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

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

[3] Humanitarian ethics has developed as a principle-based ethics grounded in the principles of humanity, impartiality, neutrality and independence that guide the provision of humanitarian assistance and protection. These principles and related rules are enshrined in various codes of conduct now widely recognized as the basis for ethical humanitarian practice, including: The Humanitarian Charter and Minimum Standards in Humanitarian Response, including the Core Standards and Protection Principles, the Core Humanitarian Standard on Quality and Accountability, and the Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief. For additional guidance on humanitarian data ethics see The Centre for Humanitarian Data, *Guidance Note: Humanitarian Data Ethics* (2019), available at: https://centre.humdata.org/guidance-note-humanitarian-data-ethics/.

of that natural person.

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.

Sensitive Data: Data classified as sensitive based on the likelihood and severity of potential harm that may materialize as a result of its exposure in a particular context. Both personal and non-personal data can be sensitive. Many organizations have specific classification systems regarding what constitutes sensitive data in order to facilitate data management practices.

NB: A full list of definitions is available in Annex A.

Background, Rationale, and Scope

This Operational Guidance is intended to help humanitarian staff, organizations, and their partners practice data responsibility in different response contexts. Data responsibility is defined as the safe, ethical and effective management of personal and non-personal data for operational response.

This Operational Guidance offers a set of principles and actions that system-wide entities, clusters and/or sectors, and organizations can implement for data responsibility in humanitarian action. It does not aim to replace or supersede official organizational policies and guidance,[4] nor does it account for specific organizational mandates or relevant national or regional laws.

Data Responsibility in Humanitarian Action

Data responsibility is a critical issue for the humanitarian sector to address. Ensuring we minimize the risks while maximizing the benefits of data management in humanitarian settings requires a continued shift in practice and collective action that extends across and beyond humanitarian organizations.

The implementation of data responsibility in practice is often inconsistent within and across humanitarian response contexts. This is true despite established principles, norms, and professional standards regarding respect for the rights of affected populations and the range of available resources on data responsibility.

In recent years, many humanitarian organizations have developed or updated their policies, guidance, and practices to support different aspects of data responsibility. The sector has also seen an increasing number of collaborative efforts to improve data responsibility beyond individual organizations.

However, even in organizations with mature policy frameworks or where robust principles have been adopted, challenges in governance, capacity, and sustainable resourcing can lead to activities and practices that are inconsistent with data responsibility. Because the humanitarian data ecosystem is inherently interconnected, no individual organization can tackle all these challenges alone. While each organization is responsible for its own data, humanitarians under the IASC – which brings together UN entities, NGO consortia and the International Red Cross and Red Crescent Movement – need common normative, system-wide guidance to inform individual and collective action and uphold a high standard for data responsibility in different operating environments. This Operational Guidance complements and is informed by existing guidance[5] on data responsibility, both from development actors and within the broader humanitarian community.

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

[5] This includes, for example, the IASC Operational Guidance on Responsibilities of Cluster/Sector Leads, the Professional Standards for Protection Work, the Protection Information Management (PIM) Framework, the Responsible Data for Children

Challenges and Opportunities for Data Responsibility in Humanitarian Action
Experience in different humanitarian response settings has yielded a set of common challenges and opportunities that form the basis for collective action in the area of data responsibility.

Challenges:

- Lack of **common definitions** and related **inconsistencies in understanding and use of terminology** among humanitarian organizations about data responsibility.
- **Gaps in existing guidance and standards**, particularly regarding the responsible management of sensitive data, the assessment of risks associated with different types of data in different contexts, and the specific and complex challenges of data responsibility in humanitarian settings.
- Varied applicability of **different legal and regulatory frameworks** among International Organizations (IOs), NGOs and UN entities.
- **Uncertainty and lack of coordination** regarding the development of new technologies and humanitarian data management standards and practices, which often evolve faster than the policy instruments that govern their use.
- **Prioritization of organizations' own internal data protection practice** rather than investment in supporting this work within the sector more broadly.
- **Absence of shared and endorsed tools and processes** for implementing data responsibility in practice.
- **Lack of capacity** for responsible data management among many humanitarian organizations and their staff.
- **Underrepresentation** of local organizations, civil society organizations and community-based structures in data management activities.

Opportunities:

- **Increased investment by humanitarian and development organizations, donors, and host governments in data responsibility** as part of a strategy to advance the rights of affected populations and contribute to humanitarian outcomes and broader development goals.
- **Improved institutional capacity** regarding issues related to responsible data management (especially the protection of personal data).
- **Expanded opportunities for collaboration on data management, with the resulting efficiencies**, including through coordinated assessments, joint delivery of assistance, and other similar activities.
- **Increased interest in and support for building a practical evidence base** of 'what works' and 'what does not work' for data responsibility.
- **Increased transparency and accountability** of humanitarian organizations in how they manage data in support of different response activities.
- **Economies of scale** through joint efforts to produce guidance on and tools for the implementation of specific measures for data responsibility.

initiative, and the Signal Code: A Human Rights Approach to Information During Crisis, among others (see Annex C for additional references).

Scope and Target Audience of the Operational Guidance

The Operational Guidance applies to different types of operational data (both personal and non-personal data) generated or used in humanitarian response settings, namely[6]:

- **Data about the context** in which a response is taking place (e.g., legal frameworks, political, social and economic conditions, infrastructure, etc.) and the humanitarian situation of focus (e.g., security incidents, protection risks, drivers and underlying causes/factors of the situation or crisis).
- **Data about the people affected by the situation** and their needs, the threats and vulnerabilities they face, and their capacities.
- **Data about humanitarian response actors and their activities** (e.g., as reported in 3W/4W/5W).

This Operational Guidance does not cover 'corporate' data, such as data related to internal financial management, human resources & personnel, supply chain management and logistics, and other administrative functions in humanitarian organizations.

The Operational Guidance is relevant to all forms of operational data management taking place in all humanitarian response contexts. *Operational data management* includes 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. Because humanitarian organizations have a variety of cycles and processes[7], this Operational Guidance does not present a single or harmonized set of steps for data management. Rather, the principles and actions in this Operational Guidance are relevant to all steps involved in operational data management for humanitarian action.

This Operational Guidance supports all humanitarian actors, including UN entities, other IOs, international and national NGOs, and other stakeholders engaged in humanitarian action.

It specifically targets the following coordination structures as forums for promoting and monitoring the implementation of data responsibility at different levels of a response: the Humanitarian Country Team (HCT); the Inter-Cluster Coordination Group (ICCG), the Inter-Cluster Coordination Mechanism (ICCM), the Inter-Sector Working Group (ISWG), and/or the Information Management Working Group (IMWG); and clusters, Areas of Responsibility (AoRs), Working Groups, and/or sectors.

[6] This may include new or non-traditional data types, such as Call Detail Records (CDRs), social media data, etc. Humanitarian organizations should apply the same standard for managing such data as for other forms of data.
[7] A literature review of 55 documents yielded 18 different processes and cycles, each varying in length and containing different steps. The list of reviewed documents is available in Annex C.

It also targets different roles and functions at the system-wide, cluster/sector, and organization levels. These include Resident Coordinators/Humanitarian Coordinators, Heads of Office/ Country Representatives, Program Managers and Officers,[8] cluster/sector Coordinators or Leads, cluster/sector Steering Committees (SC) and Strategic Advisory Groups (SAGs), and Technical Staff.[9]

Ultimately, data responsibility requires the buy-in and participation of all functions across each organization, cluster/sector, and the humanitarian system at large.

[8] This includes for example Program Officers, Sectoral/Technical Experts, Humanitarian Affairs Officers, and similar roles.
[9] This includes for example Data and Information Management Officers, Data Analysts and Scientists, Statisticians, Data Protection Officers/Focal Points, Information Technology Staff, Registration Officers, Community Feedback & Response Mechanism Operators, Monitoring & Evaluation Officers, Enumerators, and similar roles.

Principles for Data Responsibility in Humanitarian Action

The following Principles for Data Responsibility in Humanitarian Action (hereafter 'the Principles') are designed to inform safe, ethical and effective operational data management within organizations, clusters/sectors, and the broader humanitarian system in a given response context. They should serve as a normative guide for actors implementing the recommended actions for data responsibility outlined in this Operational Guidance. The Principles do not represent a compliance standard.

These Principles are based on a review of existing principles for data management (including data protection) across the humanitarian and development sectors.[10] The review revealed gaps in guidance for operational data management at the system-wide and cluster/sector level, as well as gaps in guidance for the management of non-personal data at all levels of humanitarian response. The Principles help to fill these gaps and to ensure safe, ethical and effective data management. In this way, they reinforce humanitarians' overarching commitment to **Do No Harm** while **maximizing the benefits** of data in humanitarian action.[11] The Principles also reaffirm the centrality of affected people and their rights and well-being in humanitarian action.

The management of **personal data** should be informed by the *Personal Data Protection Principle*,[12] while the management of **non-personal data** should be informed by the other Principles. The Principles are presented in alphabetical order, and no hierarchy is intended.

Wherever these Principles conflict with one another in their interpretation or application, they should be balanced against each other based on the particular dynamics of the response context.[13] In the event that the Principles conflict with either internal policies or applicable legal obligations, the latter take precedent.

[10] This includes the humanitarian principles and widely accepted standards articulated for example in Sphere, the Core Humanitarian Standard and the Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief, the United Nations Data Strategy, and the UN Personal Data Protection and Privacy Principles. In addition, it includes more topical or thematic guidance specific to different aspects of data management, including the Professional Standards for Protection Work, the Protection Information Management (PIM) Framework, and the ICRC Handbook on Data Protection in Humanitarian Action, among others. Finally, the Principles draw on existing IASC guidance, including IASC Operational Guidance on Responsibilities of Cluster/Sector Leads & OCHA In Information Management, and IASC Operational Guidance for Coordinated Assessments in Humanitarian Crises. A complete list of the documents analyzed by the Sub-Group on Data Responsibility is available in Annex C.

[11] Broadly acknowledged across the humanitarian sector, the concept of Do No Harm finds its roots in medical practice, from which it was developed into an axiom of humanitarian response in Mary B. Anderson, *Do No Harm: How Aid Can Support Peace - Or War*, (1999). For the purposes of this document the term is used as follows: 'Doing no harm' entails that data management in humanitarian response should not cause or exacerbate risk for affected people and communities, host communities, humanitarian personnel or other stakeholders, through actions or omissions. Harm is defined as '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.' 'Maximizing the benefits' of humanitarian data management entails that data is shared when a purpose requires it, in an appropriate and safe way, upholding the necessary data protection requirements. It also entails that data is managed in ways that increase the likelihood of positive impact for affected people.

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

[13] See Annex B for *Examples of Principles in Practice*.

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 develops, both for digital data and analogue data.

---

[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 (2020) and the IASC Policy on Protection in Humanitarian Action (2016) offer guidance on confidentiality. These standards should be interpreted in line with existing organizational policies and guidelines.

[16] For more information on the humanitarian principles, see OCHA on Message: Humanitarian Principles, available at: https://www.unocha.org/sites/dms/Documents/OOM-humanitarianprinciples_eng_June12.pdf.

Defined Purpose, Necessity and Proportionality

Humanitarian data management and its related activities should have a clearly defined purpose. The design of processes and systems for data management should contribute to improved humanitarian outcomes, be consistent with relevant mandates and relevant rights and freedoms, and carefully balance those where needed. In line with the concept of data minimization, the management of data in humanitarian response should be relevant, limited and proportionate – in terms of required investment as well as identified risk – to the specified purpose(s).

Fairness and Legitimacy

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

Human Rights-Based Approach

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

People-Centered and Inclusive

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

Personal Data Protection

Humanitarian organizations have an obligation to adhere to (i) applicable national and regional data protection laws, or (ii) if they enjoy privileges and immunities such that national and regional laws do not apply to them, to their own data protection policies.[17] These laws and policies contain the list of legitimate bases for the processing of personal data, including but not limited to

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

consent.[18] When designing data management systems, humanitarian organizations should meet the standards of privacy and data protection by design and by default. Humanitarian organizations should take personal data protection into consideration when developing open data frameworks. In line with their commitment to inclusivity and respect for human rights, they should ensure the rights of data subjects to be informed about the processing of their personal data, and to be able to access, correct, delete, or object to the processing of their personal data.

Quality

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

Retention and Destruction

Sensitive data should only be retained for as long as it is necessary to the specified purpose for which it is being managed or as required by applicable law or donor audit regulations. When its retention is required, safe and secure storage should be ensured to safeguard sensitive data from being misused or irresponsibly exposed. All other data may be retained indefinitely, provided that its level of sensitivity is reassessed at appropriate moments, that access rights can be established, and – for anonymized or aggregate data – that a re-identification assessment is conducted. Regardless of the sensitivity level, a retention schema should indicate when data should be destroyed and how to do so in a way that renders data retrieval impossible. Specific durations for retention should be defined where possible and, where this is not the case, specific periods for review of necessity should be set.

Transparency

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

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

Recommended Actions for Data Responsibility in Humanitarian Response Contexts

The following section presents recommended actions for data responsibility at the system-wide level (1), the cluster/sector level (2), and the organization level (3). These actions represent the greatest leverage points for collective and organizational impact vis-à-vis data responsibility. They also represent a core set of recommended actions for data responsibility in practice that the humanitarian community should seek to uphold.

These actions are applicable in all humanitarian response contexts. Because the adoption of data responsibility varies within and across response settings, these actions are meant to serve as a common reference for adaptation and implementation in context. Their implementation will vary across settings and require adaptation based on the nature of a particular crisis. While some of the actions may be new at the system, cluster/sector, and organization levels in different settings, all the actions are designed to build on and complement existing practice, processes and tools.

The actions are presented in a logical sequence at each level to serve as a roadmap for progressive action and improvement. Humanitarian actors and their partners will need to identify appropriate entry points for implementing these actions based on the state of data responsibility in their context.

The table below provides a **description of each action** and its **importance for data responsibility**. The subsequent sections for the system-wide, cluster/sector, and organizational levels describe **how the actions should be adapted and implemented at each level** and **who should be involved**. These sections also include references to sample templates and tools (available in Annex B) to support the implementation of the different actions.

Actions for Data Responsibility in Humanitarian Response Contexts		
Actions	**Description**	**Importance**
Data responsibility diagnostic	A data responsibility diagnostic entails the identification and review of existing laws, norms, policies, and standards in the context; processes & procedures; and technical tools for data management.	This diagnostic helps to identify common opportunities and challenges for responsible data management and informs the prioritization of actions for data responsibility at different levels in a response.
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	The ecosystem map and data asset registry help identify data gaps and possible duplications, support complementarity and convergence (including with longer term development-oriented processes),

	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 context.	facilitate collaboration, and enable prioritization and strategic decision-making on responsible data management.
Data impact assessment[19]	Conducting 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.	An assessment informs the design and implementation of data management activities in a way that maximizes benefits and minimizes risks.
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 (including at the design and planning step) and monitoring adherence to these Principles throughout the process.	Including data responsibility considerations in the design, implementation, monitoring and evaluation of data management activities helps minimize risks and maximize benefits.
Information Sharing Protocol and Data & Information Sensitivity Classification	An Information Sharing Protocol (ISP) should include a context-specific data and information sensitivity classification[20], articulate common actions for data responsibility, contain clauses on personal data protection, if applicable, and specify how to handle breaches to the protocol.	An ISP serves as the foundation for a collective approach to responsible data and information exchange. While typically established at the system-wide level, ISPs may also be established at the cluster/sector and organization levels as needed.
Data Sharing Agreement	A data sharing agreement 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. In accordance with data protection frameworks, signing a DSA is required for the sharing of personal data.	This type of agreement is essential to upholding legal, policy, and normative requirements related to the sharing of personal data and, in some cases, sensitive non-personal data.
Data incident management[21]	Managing, tracking, and communicating about data incidents requires standard operating procedures for incident management and a central registry or	Data incident management helps reduce the risk of incidents occurring, supports the development of a knowledge base, and fosters more

[19] 'Data impact assessment' is a generic term that refers to multiple types of assessments, as defined in Annex A. Note that a Data Protection Impact Assessment (DPIA) is the established tool and process in data protection law that should be used (specifically) to assess personal data protection risks.

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

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

	log that captures key details about the nature, severity, and resolution of each incident.	coordinated approaches to incident management over time.
Coordination and decision-making on collective action for data responsibility	Existing mechanisms can be used to coordinate and 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.	Coordination and collective action help the response community to monitor progress and challenges, and to identify opportunities for improving data responsibility. They also help foster accountability and joint investment in the implementation of the other actions in this Operational Guidance.

Level 1: System-Wide Level Actions for Data Responsibility

Supporting data responsibility at the system-wide level of a response requires collective action in a number of areas. The Resident Coordinator's/Humanitarian Coordinator's Office, the Humanitarian Country Team, OCHA or UNHCR[22], and various coordination structures such as the ICCM/ICCG/ISCG, the IMWG, and the NGO Forum have important roles to play in supporting these actions.

Because levels of data responsibility vary within and across response settings, these actions are meant to serve as a common reference for adaptation and implementation in context. While some of the actions may be new at the system-wide level in certain settings, all the actions are designed to build on and complement existing practice, processes and tools within the humanitarian system. Specific roles and responsibilities are defined for implementing each action in the table below.

Across these actions, humanitarian organizations should ensure meaningful engagement with national organizations and authorities as appropriate in the specific context.[23] This can strengthen the response capacity of national actors, build trust, and create space for productive collaboration and management of issues related to data.

System-Wide Level Actions for Data Responsibility		
Actions	**Recommended Approach**	**Roles and Responsibilities**
Conduct a system-wide data responsibility diagnostic. **[Annex B: 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. If there is no system-wide data ecosystem map, this will ideally be undertaken together.	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 in strengthening data responsibility.
Generate and maintain a system-wide data ecosystem map.	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-	The data ecosystem mapping exercise should be completed on an annual basis by the **relevant interagency mechanism(s)** (both the

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

[23] This engagement should align with the IASC *Operational Guidance For Cluster Lead Agencies on Working With National Authorities* (2011), available at: https://www.alnap.org/help-library/iasc-operational-guidance-for-cluster-lead-agencies-on-working-with-national, depending on the role that national authorities are taking in the response.

[Annex B: Data Ecosystem Map Template]	agency bodies, as well as individual organizations whose activities would not otherwise be covered via clusters/sector mapping.	**ICCM/ICCG/ISCG** and the **IMWG**) and presented to the **HCT** for reference.
Develop and maintain a system-wide Information Sharing Protocol. **[Annex B: 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-wide 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.

Level 2: Cluster/Sector Level Actions for Data Responsibility

Supporting data responsibility at the cluster/sector level requires collective action in a number of areas that will complement the actions articulated at the system-wide and organization levels. These actions should be implemented in-line with other existing global guidance from the IASC and individual clusters/sectors.

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

Cluster/Sector Lead and Co-Lead Agencies are responsible for ensuring the actions are undertaken within the scope of a given cluster/sector response (i.e., actions of the Lead or Co-Lead Agencies, and any one of their partner organizations acting on behalf of the cluster/sector overall). These include efforts to promote adherence to global and national data protection laws (where applicable), norms, policies, and standards.

Across these actions, clusters/sectors should ensure meaningful engagement[24] with national and local organizations and authorities, and other relevant stakeholders. Such engagement can strengthen the response capacity of national actors, build trust, and create space for productive collaboration and management of issues related to data.

Cluster/Sector-Level Actions for Data Responsibility		
Actions	**Recommended Approach**	**Roles and Responsibilities**
Conduct a cluster/ sector-level data responsibility diagnostic. **[Annex B: 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/updated 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	The cluster/sector data ecosystem map should capture all existing data	The cluster/sector data ecosystem mapping exercise and

[24] This engagement should align with the IASC *Operational Guidance for Cluster Lead Agencies on Working With National Authorities* (2011), available at: https://www.alnap.org/help-library/iasc-operational-guidance-for-cluster-lead-agencies-on-working-with-national, depending on the role that national authorities are taking in the response, and be carried out in coordination with relevant inter-cluster/inter-sector mechanisms.

cluster/sector data ecosystem map and data asset registry. **[Annex B: Template for Data Ecosystem Map]**	management activities relevant to key response interventions within the cluster/sector. The cluster/sector data asset registry should capture all related data assets linked to the activities identified in the mapping. Together, these two actions help avoid duplication of efforts and support data sharing within the cluster/sector and across the response more broadly. They also inform inputs by the cluster/sector to the system-wide data ecosystem mapping exercise.	data asset registry development 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. **[Annex B: 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-wide level ISP, as well as relevant applicable laws, norms, policies, and standards in the context. *Note: If cluster/sector members plan to share personal data with each other, they should establish data sharing agreements for this purpose (see more in Level 3: Organization Level Actions for Data Responsibility, below).*	The ISP should be developed through a collective exercise led by the **cluster/sector Lead and Co-Lead Agencies** 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.	Human and financial resources for data responsibility at the cluster/sector level are essential to strengthen data responsibility within the cluster/sector itself and across its members. This is particularly important when members undertake or participate in joint data management activities on behalf of or to the benefit of the cluster/sector overall. Content on data responsibility (e.g., how to conduct data impact assessments and securely transfer sensitive data) should be incorporated into cluster/sector-level capacity development activities.	The **cluster/sector Lead and Co-Lead Agencies** have a responsibility to advocate for the necessary resources and to 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 cluster/sector-led data management activities to foster a consistent approach amongst members.	The **cluster/sector Lead and Co-Lead Agencies** should aim to design cluster-led data management activities in-line with this Operational Guidance. This could be done for example by including data responsibility in cluster strategies.
Track and communicate about data incidents within the cluster/sector.	Tracking and communicating about incidents within the cluster/sector helps reduce the risk of incidents recurring. A cluster/sector should feed into system-wide level tracking of data incidents to share learnings and good practice for mitigating risks within the broader community. At the cluster/sector level, this may include a central registry that captures key details about the nature, severity, and resolution of incidents. Any such registry should ensure adequate measures for confidentiality and protection of sensitive data.	The **cluster/sector Lead and Co-Lead Agencies** have a responsibility to establish and maintain a registry of data incidents that occur within data management activities led by the cluster/sector. They also should ensure that these incidents and the related lessons learned are shared with relevant system-wide bodies and forums.

Level 3: Organization Level Actions for Data Responsibility

Upholding data responsibility at the organization level in a given response setting is critical to the success of the actions for data responsibility at both the system-wide and cluster/sector levels. The actions in the table below should be implemented in-line with relevant official organizational policies and guidelines. They do not in any way affect or replace the obligations contained in applicable organizational policies or legal and regulatory frameworks. The recommended actions are designed for implementation by organizational offices and/or teams in a given response environment (e.g., country or area offices and teams).

Because levels of data responsibility vary within and across response settings, these actions are meant to serve as a common reference for adaptation and implementation in context. While some of the actions may be new for organizations in a certain setting, all the actions are designed to build on and complement existing practice, processes and tools within the broader humanitarian system.

Given the varied functions and capacities across humanitarian organizations, this Operational Guidance does not assign specific roles and responsibilities for data responsibility at the organization level. Wherever possible, organizations should integrate the actions outlined below into the roles and responsibilities of existing teams and functions involved in operational data management in different response environments.

Organization-Level Actions for Data Responsibility	
Actions	**Recommended Approach**
Conduct an organization-level data responsibility diagnostic. **[Annex B: Data Responsibility Diagnostic Template]**	The organization-level data responsibility diagnostic provides an overview of existing data responsibility measures within an organization's office in a given humanitarian setting. 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, and situational analysis) 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, and before undertaking any new data collection.

	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. **[Annex B: Data Impact Assessment Template]**	Data impact assessments (DIAs) should be conducted before and during data management activities in order to inform project planning, design, implementation, and adjustments/revisions. DIAs should be conducted in an inclusive manner, involving 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. *Note: Many organizations have specific policies, requirements and guidelines for how DIAs should be conducted. For those which do not, the template can serve as a useful reference (see Annex B).*
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 data (e.g., application of Statistical Disclosure Control[25] 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 effective manner, with the necessary safeguards for personal data and in compliance with applicable data protection frameworks. - Organizations should establish and communicate clearly about how individuals can access, verify, rectify, and/or delete data on themselves.
Establish data sharing	Organizations should establish data sharing agreements whenever transferring personal data or sensitive non-personal data to other organizations, in-line with

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

agreements to govern the transfer of personal data and sensitive data. **[Annex B: Data Sharing Agreement Builder]**	relevant institutional, legal and regulatory requirements as well as the Principles for Data Responsibility in Humanitarian Action. Note: While the circumstances of data sharing differ too much to provide a single template for data sharing agreements, the Data Sharing Agreement Builder in Annex B offers a set of points to consider in developing such agreements, should templates and models not already exist (by practice or policy) in the organization.
Establish a Standard Operating Procedure for data incident management. **[Annex B: SOP for Data Incident Management]**	Organizations should develop and implement Standard Operating Procedures (SOPs) to manage data incidents. This should include a process for notification, classification, treatment, and closure of the incident. They should also include a logging of incidents into their organization's knowledge base (e.g., using a registry that captures key details about the nature, severity, and resolution of each incident). Appropriate channels for rectification and redress for individuals impacted by a data incident should also be included in the SOPs. Organizations should share their experience in managing and mitigating data incidents with other actors, i.e., at the cluster/sector and system-wide levels.

Annex A: Definitions

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

Anonymization: Process by which personal data is irreversibly altered, either by removing or modifying the identifying variables, in such a way that a data subject can no longer be identified directly or indirectly.[26]

Consent: Consent is the most frequently used and often the preferred legal basis for personal data processing. However, given the vulnerability of most beneficiaries and the nature of humanitarian emergencies, many humanitarian organizations will not be in a position to rely on consent for most of their personal data processing.[27]

Data: Re-interpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.[28]

Data asset: Data assets are a body of data or information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently.[29]

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

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

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.

Data incidents: Events involving data management, such as the loss, destruction, alteration, acquisition, or disclosure of data and information, caused by accidental or intentional, unlawful or otherwise unauthorized purposes that have caused harm or have the potential to cause harm.[30]

Data minimization: The objective of ensuring that only the minimum amount of data is processed to achieve the objective and purposes for which the data were collected.[31]

Data quality: A set of characteristics that make the data fit for the purpose for which it is processed. Data quality includes components such as accuracy, relevance, sufficiency, integrity, completeness, usability, validity, coherence, punctuality, accessibility, comparability, and timeliness.[32]

---

[26] UN OCHA Centre for Humanitarian Data, *Glossary*: https://centre.humdata.org/glossary/.
[27] UNHCR, *Guidance on the Protection of Personal Data of Persons of Concern to UNHCR* (2018), https://www.refworld.org/docid/5b360f4d4.html.
[28] UN, *Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020-22* (2020), https://www.un.org/en/content/datastrategy/index.shtml.
[29] Adapted from United Kingdom National Archives, *Information Asset Fact Sheet* (2017), https://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf.
[30] The Centre for Humanitarian Data, *Guidance Note: Data Incident Management* (2019), https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf.
[31] ICRC, *Handbook on Data Protection in Humanitarian Action* (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.
[32] UN OCHA, *OCHA Data Responsibility Guidelines (Working Draft)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

Data protection: The systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the processing of personal data.[33]

Data protection impact assessment: A tool and process for assessing the protection impacts on data subjects in processing their personal data and for identifying remedial actions as necessary in order to avoid or minimize such impacts.[34]

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

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.[36]

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.[37]

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. In accordance with data protection frameworks, signing a DSA is required for the sharing of personal data.

Data subject: A natural person (i.e., an individual) whose personal data is subject to processing, and who can be identified, either directly or indirectly, by reference to this data and reasonably likely measures. The nomination as a data subject is linked to a set of specific data subject rights to which this natural person is entitled with regards to his/her personal data, even when this data is gathered, collected or otherwise processed by others.[38]

Harm: Negative implications of a data processing initiative on the rights of a data subject, or a group of data subjects, including but not limited to physical and psychological harm, discrimination and denial of access to services.[39]

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

Microdata: Observation data on the characteristics of statistical units of a population, such as individuals, households, or establishments, gathered through exercises such as household surveys, needs assessment or monitoring activities.[40]

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

[33] Definition developed by the UN Privacy Policy Group (2017).
[34] UNHCR, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* (2015), https://www.refworld.org/pdfid/55643c1d4.pdf.
[35] UN OCHA, *OCHA Data Responsibility Guidelines (Working Draft)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.
[36] The Centre for Humanitarian Data. *Glossary*: https://centre.humdata.org/glossary/.
[37] The Centre for Humanitarian Data. *Glossary*: https://centre.humdata.org/glossary/.
[38] UN OCHA, *OCHA Data Responsibility Guidelines (Working Draft)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.
[39] ibid.
[40] The Centre for Humanitarian Data, *Guidance Note: Statistical Disclosure Control* (2019), https://centre.humdata.org/guidance-note-statistical-disclosure-control/.

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.

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.

Personal data: Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[41]

Primary data: Data that has been generated by the researcher himself/herself, surveys, interviews, experiments, specially designed for understanding and solving the research problem at hand.[42]

Privacy: No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.[43]

Re-identification: A process by which de-identified (anonymized) data can be traced back or linked to an individual(s) or group(s) of individuals through reasonably available means at the time of data re-identification.[44]

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

Sensitive data: Data classified as sensitive based on the likelihood and severity of potential harm that may materialize as a result of its exposure in a particular context. Both personal and non-personal data can be sensitive. Many organizations have specific classification systems regarding what constitutes sensitive data in order to facilitate data management practices.[45]

Statistical Disclosure Control: Technique used in statistics to assess and lower the risk of a person or organization being re-identified from the results of an analysis of survey or administrative data, or in the release of microdata.[46]

[41] UN OCHA, *OCHA Data Responsibility Guidelines (Working Draft)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.
[42] Public Health Research Guide, *Primary & Secondary Data Definitions:* https://researchguides.ben.edu/c.php?g=282050&p=4036581.
[43] UN General Assembly, *International Covenant on Civil and Political Rights* (1976), https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
[44] UN OCHA, *OCHA Data Responsibility Guidelines (Working Draft)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.
[45] The Centre for Humanitarian Data, *Glossary*, https://centre.humdata.org/glossary/.
[46] The Centre for Humanitarian Data, *Guidance Note on Statistical Disclosure Control* (2019), https://centre.humdata.org/guidance-note-statistical-disclosure-control/.

Annex B: Templates and Tools for Data Responsibility

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

These templates and tools are not mandatory. Rather, they are provided as examples to help organizations put into practice the actions presented in this Operational Guidance. They do not replace existing templates or tools when these already exist in an organization, either by practice or by policy.

These templates and tools will be updated based on feedback received and lessons learned on their use over time. Each template and tool includes an introductory section describing the purpose of the tool, its source(s) and use to-date (where relevant), and instructions for its adaptation and use.

- **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**

Annex C: Resources and References

The following documents were included in the literature review that informed the drafting of this Operational Guidance.

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

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

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

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

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

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

ELAN/Cash Learning Partnership, 2018. Data Starter Kit for Humanitarian Field Staff: https://elan.cashlearning.org/.

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

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

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

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

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

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

ICRC-led Advisory Group incl. DRC on "Professional Standards", 2018. Professional Standards for Protection Work; Chapter 6: Managing Data and Information for Protection Outcomes: https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights.

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

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

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

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

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

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

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

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

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

Médecins Sans Frontières, 2013. Data Sharing Policy: https://fieldresearch.msf.org/bitstream/handle/10144/306501/MSF+data+sharing+policy+final+061213.pdf;jsessionid=E85DF92F1427CE9A46DA5A06D8D6AED5?sequence=1.

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

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

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

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

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

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

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

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

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

Terre des Hommes and CartONG, 2017. Data Protection Starter Kit: https://www.mdc-toolkit.org/data-protection-starter-kit/.

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

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

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

UN Office for the Coordination of Humanitarian Affairs (UN OCHA), 2019. Working Draft Data Responsibility Guidelines: https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

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

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

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

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

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

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

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

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

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

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

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

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 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.

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

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

UN Secretariat, 2004. Secretary-General's Bulletin on the Use of Information and Communications Technology Resources and Data, ST/SGB/2004/15: https://popp.undp.org/UNDP_POPP_DOCUMENT_LIBRARY/Public/United%20Nations%20Secretary-Generals%20Bulletin%20on%20Use%20of%20ICT%20Resources%20and%20Data%20ST_SGB_2004_15%20%E2%80%93%20Amended.docx.

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

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, 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.

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

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

Annex D: Background on Development of the Operational Guidance

The Inter-Agency Standing Committee Results Group 1 established the Sub-Group on Data Responsibility in January 2020 to lead the development of joint, system-wide operational guidance on data responsibility in humanitarian action. The Sub-Group was co-led by the International Organization for Migration, the OCHA Centre for Humanitarian Data, and the United Nations High Commissioner for Refugees, and comprised twenty member organizations[47] representing different stakeholders within the humanitarian system.

The Sub-Group developed this Operational Guidance through a collaborative and consultative process with IASC members and the broader humanitarian community, NGOs, United Nations agencies, other international organizations, and donors at the global, regional and national levels. A number of activities informed the development of the Operational Guidance, including:

- A literature review[48]
- A public-facing survey[49]
- A series of targeted consultations with different stakeholders from across the humanitarian system, including organizations, clusters/sectors, and system-wide structures
- An open feedback period through which 250 colleagues from 30 different organizations provided inputs and feedback on the draft operational guidance, and
- Three rounds of structured, organizational review of the draft Operational Guidance at different stages of development.

This Operational Guidance complements and is informed by existing guidance on data responsibility, both from development actors and within the broader humanitarian community. It is designed to leverage existing expertise on data responsibility, reinforce efforts and initiatives, and help mainstream best practice. It is aligned with other key sector-wide guidance and initiatives on different topics related to responsible data management. A full list of resources reviewed as part of the drafting process for the Operational Guidance is included in Annex C.

Given the dynamic and evolving nature of the challenges and opportunities for data responsibility in humanitarian action, this Operational Guidance will be reviewed and updated[50] in a collaborative and consultative manner every two years.

[47] The Sub-Group included representatives from: CARE, CRS, DRC, ICRC, IFRC, IRC, IOM, JIPS, Mercy Corps, MSF, NRC, OCHA, OHCHR, Oxfam, Save the Children, UNFPA, UNHCR, UNICEF, WFP and WHO.
[48] The Sub-Group conducted the Literature Review of relevant existing guidance on data responsibility with support from the Technical University of Delft. The list of documents reviewed is available in Annex C.
[49] The public survey was conducted online from February 27 until March 18, 2020. Survey results are available here: https://centre.humdata.org/survey-results-on-priorities-for-data-responsibility-in-humanitarian-action/.
[50] OCHA will be responsible for initiating the review and updating process for this Operational Guidance.