OCHA centre for humdata

THE CENTRE FOR HUMANITARIAN DATA

GUIDANCE NOTE SERIES
DATA RESPONSIBILITY IN HUMANITARIAN ACTION

GUIDANCE NOTE: DATA RESPONSIBILITY AND ACCOUNTABILITY TO AFFECTED PEOPLE IN HUMANITARIAN ACTION

KEY TAKEAWAYS:

- Data responsibility is the safe, ethical and effective management of personal and non-personal data for operational response and is therefore central to the humanitarian system's Accountability to Affected People (AAP).
- Examples of data management related to AAP include communicating with communities, processing complaints and feedback, and tracking community perceptions.
- Collecting data from and about communities can lead to improved understanding of the priorities and preferences of affected people, as well as their increased participation in and ownership of humanitarian action.
- However, data management related to AAP might carry risks, including, among others, exposure of sensitive data that could lead to harm for affected people or humanitarian workers, and loss of trust between affected people, humanitarian organizations and stakeholders.
- Humanitarians should conduct data impact assessments, design for data responsibility, develop data management diagrams, maintain a data management registry, establish data sharing agreements, and introduce data incident management procedures.

INTRODUCTION

Accountability to Affected People (AAP) is a collective approach that ensures the needs and interests of people are at the center of humanitarian action. It is based on a commitment to take account of, give account to and be held to account by the people humanitarians seek to assist.[1] In their activities related to AAP, humanitarians collect and use increasing amounts of data. Responsible data management is critical to ensuring that these activities do not harm affected people, and is part of fulfilling the commitments related to AAP.

This Guidance Note explores data responsibility and AAP in humanitarian action. It identifies common data-related benefits and risks related to AAP, explains how humanitarians can implement actions from the IASC Operational Guidance on Data Responsibility in Humanitarian Action and offers examples of joint approaches to this work.

[1] For more on AAP in Humanitarian Action, and OCHA's role, see: **OCHA: Accountability to affected people**.

DATA MANAGEMENT RELATED TO AAP

Through AAP, humanitarians aim to ensure that humanitarian action protects and preserves the rights and dignity of people affected by crises, remains relevant and effective, leaves no one behind, and upholds humanitarian principles.[2] By recognizing that crisis-affected people experience aid differently, AAP enables humanitarians to work with affected people to ensure that their diverse needs, vulnerabilities and capacities are centered in decision-making and programme design.

Humanitarians do this primarily through the following activities:

- Systematically providing timely, relevant and actionable information about the humanitarian response, its actors and its activities to people and communities.
- Supporting the meaningful participation and leadership of affected people in decision-making, regardless of sex, age, disability status and other diversities.
- Ensuring community feedback mechanisms are in place to enable affected people to assess and comment on the performance of humanitarian action, and to make complaints about any issue, including sensitive topics such as protection, gender-based violence, sexual exploitation and abuse, fraud, corruption, racism and discrimination, environmental violations, and others.

Humanitarians increasingly use digital channels to engage with communities. As a result, large quantities of data can be collected and used, requiring appropriate management. Data responsibility — the safe, ethical and effective management of personal and non-personal data for operational response — is critical to these efforts.[3] Ensuring that data management activities[4] do not harm affected people is part of fulfilling the commitments related to AAP.

Common data management activities related to AAP include:

- Communicating with communities through the provision of timely and relevant information.
- Mechanisms for collecting, analyzing, referring and actioning complaints and feedback.
- Systems for tracking community perceptions, rumors, and misinformation, disinformation and hate speech (MDH).
- Information management activities to inform the delivery and coordination of assistance, including joint needs assessments and analysis, perception surveys, and mapping the presence and activities of partners in different locations.
- Information ecosystem analysis[5] to capture the relationship between information supply and information demand to and from communities.

Understanding how these activities relate to one another and how data moves between individuals, communities and organizations is part of a responsible and accountable approach to data management.[6]

[2] **Statement by Principals of the Inter-Agency Standing Committee (IASC) on Accountability to Affected People in Humanitarian Action**.

[3] **IASC Operational Guidance on Data Responsibility in Humanitarian Action (2023)**.

[4] A data management activity is any activity involving the management of data and information as part of humanitarian response. This includes the design of the activity, as well as the collection, receipt, storage, quality assurance, analysis, sharing, use, retention and destruction of data and information by humanitarian actors. **IASC Operational Guidance on Data Responsibility in Humanitarian Action (2023)**.

[5] Information Ecosystem Analysis seeks to capture all dimensions of the relationship between information supply and information demand. For more information, see: **Internews, Information Ecosystem Analysis - A Human-Centered Approach (2021)**.

[6] For more information, see the **Centre for Humanitarian Data's Tip Sheet on Understanding Data Ecosystems**.

BENEFITS AND RISKS OF DATA MANAGEMENT ACTIVITIES RELATED TO AAP

Understanding and balancing the benefits and risks of data management is a key component of data responsibility. Benefits and risks related to data managements activities related to AAP vary across contexts, and may include the following common benefits and risks:

Common benefits:

- Improved understanding of priorities and preferences of affected people, such as their preferred channels to receive and submit information.
- Increased participation in and ownership of humanitarian action by affected people.
- Gains in effectiveness of humanitarian action by responding to community feedback.
- Enhanced transparency and accountability.

Common risks:

- Accidental or intentional exposure of personal or non-personal sensitive data that could lead to re-identification, retaliation, stigmatization, violence or other forms of harm for affected people.
- Potential misuse of data for non-humanitarian purposes. For instance, this may occur when a commercial software vendor that provides a community communication channel uses the chat history to pursue their own business purposes.
- Biased analysis leading to poor decision-making. This can happen when non-representative data from perception surveys is used to draw response-level conclusions.
- Missed opportunities to use available data when efforts are not coordinated, which can lead to data collection fatigue by affected communities and individuals having to re-share the same difficult stories.
- Loss of trust between affected people, humanitarian organizations and other stakeholders when sensitive data is released or leaked.

RECOMMENDED ACTIONS FOR DATA RESPONSIBILITY IN AAP

Data responsibility requires the implementation of actions at different levels of a humanitarian response, in-line with the IASC Operational Guidance. The Centre for Humanitarian Data ('the Centre') recommends the following actions to support data responsibility as part of AAP:

- **Conduct a data impact assessment**
- **Design for data responsibility**
- **Develop data management diagrams**
- **Maintain a data management registry**
- **Establish data sharing agreements**
- **Introduce data incident management procedures**

[7] For more information, see this **Guidance Note on Data Impact Assessments**.

Conduct data impact assessments

A data impact assessment (DIA)[7] aims to determine the expected impacts of a data management activity and helps identify recommendations to mitigate the potential negative impacts. Many data management activities related to AAP involve the management of both personal and non-personal sensitive data or make use of new digital tools. As such, organizations should conduct a DIA before starting an activity to assess whether the activity can be implemented responsibly.

Design for data responsibility

Designing for data responsibility means identifying ways to make data management safe, ethical and effective. All measures for data responsibility should be outlined in a clear and replicable standard operating procedure (SOP). An SOP should include roles and responsibilities of stakeholders involved, tools and processes for data management, measures to prevent exposure of sensitive data, and clear terms for data retention and destruction. In addition, an SOP should specify the purpose of the given data management, as well as its legitimate basis, including but not limited to informed consent. The SOP should also specify measures to uphold data subjects' rights to be informed about how their data will be used, as well as to interact with it, or even request its full deletion. When developing an SOP, consult the data impact assessment for the activity to inform appropriate, feasible and robust risk mitigation measures.

Develop data management diagrams

A data management diagram offers a visual understanding of an activity and can help identify gaps in data sharing, legal provisions, infrastructure or guidance (e.g., this should be done when planning the information flows within a Community Feedback Mechanism).

Maintain a data management registry

A data management registry provides a summary of the key data management activities led by different actors in the response context, including the data managed in those activities. The registry should indicate the sensitivity level for each data type, and should align with existing data and information sensitivity classifications for the response context where available.[8] It should be updated on a rolling basis by the relevant interagency mechanism (e.g. the AAP Working Group).

Establish data sharing agreements

When sharing personal or highly sensitive data, organizations should establish a data sharing agreement (DSA). A DSA establishes the terms and conditions that govern the sharing of specific personal data and sensitive non-personal data between two or more parties. Check whether the data sharing is subject to a specific data protection framework (e.g. if one of the partners is subject to national legislation). In that case, the DSA needs to adhere to the requirements specified in the applicable data protection framework, including relevant data subject rights and requests. A DSA may not be required if dedicated clauses on data sharing are included in broader agreements, such as memorandums of understanding and service contracts.

Introduce data incident management procedures

Data incidents related to AAP include exposure of data ('data breach') that could lead to retaliation, stigmatization, violence or other forms of harm for affected people, and the misuse of affected people's data for non-humanitarian purposes. Data incident management refers to the processes and tools for identifying, resolving, tracking and communicating about data incidents.[9] It is a key component of transparent and accountable data management, and can help prevent future incidents. Organizations should establish a standard operating procedure for data incident management, and a registry or log to track data incidents and how they were handled. Where the data incident constitutes a personal data breach, organizations need to fulfill obligations established in the relevant data protection framework and in applicable data sharing agreements. This may include providing information about the breach to individuals whose personal data was exposed.

[8] A Data and Information Sensitivity Classification is part of an Information Sharing Protocol (ISP), which serves as the primary document of reference governing data and information sharing in the response. The Classification indicates the level of sensitivity of different types of data and information for a given context. This is a key component of an ISP and should be developed through a collective exercise in which different stakeholders agree on what constitutes sensitive data in their context.

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

Case Study from Afghanistan: Data Responsibility in AAP

Following the de facto authorities' decree in December 2022 banning Afghan women from working for NGOs, the IASC established minimum criteria for programming, including robust commitments around AAP. The AAP Working Group (AAP WG) launched the Afghanistan Community Voices and Accountability Platform to help humanitarians collect, analyze and respond to community feedback across the response in Afghanistan in a timely and secure manner.

Given the sensitivity of the data shared through the collective platform, the AAP WG took steps to ensure data responsibility by design. This included conducting a data impact assessment to identify and mitigate data-related risks, and establishing a standard operating procedure (SOP) for data management by all partners involved. The SOP specifies that no personal data should be stored within the platform. It also includes steps to ensure that data management within the platform does no harm, and promotes equality and non-discrimination. This is achieved through collective analysis of complaints and feedback received from affected communities, and the presentation of key insights in a neutral and impartial manner. The SOP is aligned with the system-wide Information Sharing Protocol for Afghanistan, which was endorsed by the Humanitarian Country Team in May 2023.

Case Study from Syria: Data Responsibility in Managing Community Feedback

The AAP WG developed data management diagrams to inform the expansion of the hotline. These diagrams visualized the flow of data and information between the different actors involved. This allowed the AAP WG to identify points for improvement in handling complaints and feedback data.

These improvements will be incorporated into an SOP for the joint hotline, which will build on the best practices of the existing PSEAH hotline. Measures for data responsibility will include restricting access to sensitive data, requiring the use of encrypted channels for transferring data, and defining a data retention and destruction schedule for sensitive data once it is no longer needed to fulfill the purpose of the hotline.

Organizations are encouraged to share their experience in promoting data responsibility in the design and delivery of AAP with the Centre via centrehumdata@un.org.

The Centre for Humanitarian Data ('the Centre'), together with key partners, is publishing a series of guidance notes and tip sheets on Data Responsibility in Humanitarian Action over the course of 2022 and 2023. The guidance note series continues work initiated in 2019 and 2020. It also complements the Inter-Agency Standing Committee Operational Guidance on Data Responsibility in Humanitarian Action (revised in April 2023) and the OCHA Data Responsibility Guidelines (October 2021). Through the series, the Centre aims to provide additional guidance on specific issues, processes and tools for data responsibility in practice. The guidance notes and tip sheets published in 2022-2023 have been made possible with the support of the Government of Switzerland.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA