OCHA centre for humdata

THE CENTRE FOR HUMANITARIAN DATA

GUIDANCE NOTE SERIES
DATA RESPONSIBILITY IN HUMANITARIAN ACTION

NOTE #5: DATA IMPACT ASSESSMENTS

KEY TAKEAWAYS:

- Data impact assessments determine the potential benefits and risks associated with data management. They are a critical component of responsible data management, but are often overlooked.
- There are a wide variety of approaches to data impact assessments. Selecting the right assessment for a given data management activity can minimise the risk and maximise the benefit to affected people, humanitarians and other stakeholders.
- Applicable laws and regulations, internal policies, the context in which data management will take place and other factors determine which assessment(s) should be applied to a data management activity.
- Data impact assessments should be conducted before and during data management activities in order to inform project planning and design. Activities should be redesigned or cancelled if the foreseeable risks of data management outweigh the intended benefits.

DATA IMPACT ASSESSMENTS

Various sources of guidance on data responsibility[1] in humanitarian action contain tools for conducting data impact assessments in order to understand the positive and negative consequences of a data management activity. Such assessments are a key component of accountability mechanisms and can serve to demonstrate compliance with applicable law, regulations and/or internal policies.[2] Even when not obligatory, an assessment is advisable to help maximise benefits and minimise risks associated with any data management activity.[3]

A data management activity refers to a process by which data is collected, stored, analysed and/or disseminated. Common data management activities in the humanitarian sector include needs assessments, surveys, and beneficiary registration.

Assessment outcomes may require that an activity be redesigned or cancelled, if the foreseeable risks of data management outweigh the intended benefits.[4] Common risks associated with data management include privacy infringements to individuals and groups, affected people being exposed to physical harm

[1] Defined as the safe, ethical, and effective management of data. For more information, see the working draft OCHA Data Responsibility Guidelines, available here: **https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf**.

[2] A literature review of 55 publicly available guidance documents informing responsible data management across the humanitarian sector revealed 22 different approaches, included as tools or recommended in the guidance document.

[3] While positive implications of data management are usually referred to as 'benefits', negative implications include risks and harms -- with rights infringements often called out specifically. Risks are typically defined as the multiplication of likelihood and impact of harm. See the International Standardisation Organisation's definitions of 'risk' and other relevant terms here: **https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en**.

[4] When conducted at the outset of the development and/or use of a new tool or architecture, this contributes to data protection by design or privacy by Design. For more information, see for example Privacy By Design, The 7 Foundational Principles, available here: **http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf**.

and persecution, or the risk of misrepresentation and poorly informed decision-making. Common benefits of data management activities include better targeting of humanitarian assistance to those in need, preventing inefficiency or waste by improved tracking of aid delivery, and more detailed understanding of a crisis situation.

TYPOLOGY OF ASSESSMENTS

There are many different approaches to assessments. Some of the most common references include: Risk Assessments; Risks, Harms and Benefits Assessments; Human Rights Impact Assessments; and Data Protection or Privacy Impact Assessments.

Even assessments with similar names can cover different focus areas. For example, a risk assessment for one organisation may be broad and cover physical risk to individuals as well as potential rights infringements and even expected benefits of data management activities. Other risk assessments are focused only on the potential negative consequences of data management activities. The differences between these approaches can often be explained by the sector or field from which they have been developed.

ASSESSMENT FOCUS

Consider your focus as you select the right model or tool for undertaking the assessment.

- **Risk** is defined by the International Standardisation Organisation (ISO) as 'the effect of uncertainty on objectives', and is 'usually expressed in terms of risk sources, potential events, their consequences and their likelihood.'[5] For data management in the humanitarian sector, risk can be defined as the likelihood and impact of harm resulting from data management. Risk is included as a focus area in most assessments.

- **Harm** is the negative consequence of a risk materialising. Harms that are typically covered in assessments include physical harm to individuals, stigmatisation of groups, and the impairment of aid delivery. Such harm can impact one or more predefined stakeholders, such as affected people and aid workers, among others.

- **Benefit** is the potential positive impact of data management activities, often measured in the provision of humanitarian aid or resource efficiency gains.[6]

- **Privacy** involves determining whether individual (and sometimes group) privacy is respected in data management. This focus area often relates to applicable rules or legislation.

- **Data protection** comprises a broader set of laws and regulations regarding data management, including the protection of privacy. Like the privacy focus area, this often relates to applicable rules or legislation.[7]

- **Human rights** covers fundamental rights including the right to privacy, but also the right to life and other rights that are relevant in humanitarian response situations.[8]

[5] See the ISO 31000:2018 Risk Management Guidance, available here: **https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en**.

[6] See for example the United Nations Global Pulse Risks, Harms and Benefits Assessment tool which also appears on page 4 of this Guidance Note and is available here: **https://www.unglobalpulse.org/policy/risk-assessment/**.

[7] See the Handbook on Data Protection in Humanitarian Action (2nd ed.), Christopher Kuner and Massimo Marelli (May 2020), p. 299, available here: **https://www.icrc.org/en/data-protection-humanitarian-action-handbook**.

[8] See for example the OHCHR Guiding Principles on Business and Human Rights, available here: **https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf**, and for an example of a human rights centered approach, this report on the role of new technologies for the realisation of economic, social and cultural rights (in particular para. 46), available here: **https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf**.

Assessments can take into account one or two of these focus areas or be broader and even include all of them. Variations reflect the applicability of legal frameworks, organisational priorities, and other factors, and can mean that one assessment is better suited than others in a given context.

DECIDING TO DO AN ASSESSMENT

Determining whether an assessment is needed and if so, which areas to focus on, is the first step. Consider these questions:

1. **Is a specific assessment required by applicable laws and regulations?**

   Applicable laws and regulations will often prescribe that an assessment should be conducted, and will prescribe the focus areas that should be included in the assessment. Assessments may be supplemented by additional steps, either taken from existing templates or designed for the data management activity at hand.

2. **Do internal organisational policies require that a specific assessment be conducted?**

   Where internal guidance regarding the preparation for data management activities is available, always follow such guidance. Depending on the circumstances of the activity, additional steps may be added to mandatory assessments.[9]

3. **Does the foreseen data management activity entail the management of sensitive data?**

   Sensitive data is data that requires additional protection as its disclosure or unauthorised access is likely to cause harm to the source of the data or other identifiable persons or groups, or may have a negative impact on an organisation's reputation or capacity to carry out its activities.[10] If such data is likely to be managed in a given activity, an assessment should be conducted.

4. **Is data management taking place in a particularly sensitive response context?**

   For certain operations, humanitarian data management activities warrant additional caution. A context can be particularly sensitive due to specific vulnerabilities of affected people, the value of their data to parties that may wish to subject them to harm, or the legal obligations — lawful or unlawful — with which the actors involved must comply. Skewed power dynamics (situations in which one or more stakeholders have an advantage in resources or otherwise) warrant extra attention. Where private actors are involved, issues around access, governance and control should be considered.

5. **Will the data management activity be systematic or large-scale?**

   Systematic and/or large-scale data management activities, such as annual Multi-Cluster Location Assessments or the roll-out of a country-wide beneficiary registration system, warrant assessments that take into account a longer timeframe, with more attention to the way in which the assessment will be updated and repeated.

Even if the answer to each of these questions is 'no', a basic consideration of benefits and risks associated with the data management activity is still recommended. If any of these questions is answered with 'yes', an assessment should be conducted.

Always check to see if an assessment has been conducted previously for a linked or similar data management activity. This will help inform whether an assessment is still needed for the current activity or whether gaps between the two activities can instead be assessed. Any other relevant information regarding the similar data management activity — such as a past data breach — should be taken into account when conducting an assessment of the new activity.

[9] See for an example of a template Data Impact Assessment this Restoring Family Links template for National Red Cross and Red Crescent Societies, available here: **https://www.icrc.org/en/document/rfl-code-conduct**.

[10] Source: Centre for Humanitarian Data, Glossary of Data Terms, available here: **https://centre.humdata.org/glossary/**.

TOOLS FOR ASSESSMENTS

While there is no single approach to assessments across the humanitarian sector, there exist various publicly available tools and templates that can be adapted for use by humanitarians. Notable examples include the following:

- UN Global Pulse has developed a Risk, Harms and Benefits Assessment tool, which focuses on data protection, privacy and ethics. It is designed to assess data and artificial intelligence innovation projects. The tool is a combination of a human rights and data privacy impact assessment.[11]

- The International Committee of the Red Cross and the Brussels Privacy Hub promote the use of a Data Protection Impact Assessment. The template can be found in the second edition of their Handbook on Data Protection in Humanitarian Action.[12]

- The International Red Cross and Red Crescent Movement use a data impact assessment that is focused on data protection when restoring family links.[13]

Mapping structures in refugee settlements with satellite imagery
UN Global Pulse

UN Global Pulse used its Risk, Harms and Benefits Assessment in a project involving the use of satellite imagery assisted by neural networks to map structures in refugee settlements. The assessment was undertaken by a diverse team of experts, from legal and policy specialists to technical and programme staff.

The assessment highlighted that satellite imagery could be used to reveal the location of vulnerable groups of individuals in refugee camps. Malicious actors may be able to undertake harmful misuse of the analysis resulting in potential fundamental rights violations and harms. Knowing the location of individuals in a conflict setting could lead to persecution, discrimination, physical harm or even death. Possible algorithmic failure or bias could result in certain groups of individuals being left unaccounted for and without assistance.

As a result of the assessment, the team identified mitigation measures that included reviewing the security and retention measures of the data, algorithm training for personnel, and policy clarifications, such as placing limits on public release of results. The risks were regularly re-evaluated throughout the project as the technology and data sources evolved.

[11] The UN Global Pulse tool is grounded in the UN Principles on Personal Data Protection and Privacy and UNSDG Guidance Note on Data Privacy, Data Protection and Data Ethics as well as other relevant international instruments. The tool is available here: **https://www.unglobalpulse.org/policy/risk-assessment/**.

[12] See the Handbook on Data Protection in Humanitarian Action (2nd ed.), Christopher Kuner and Massimo Marelli (May 2020), p. 299, available here: **https://www.icrc.org/en/data-protection-humanitarian-action-handbook**.

[13] See the RFL template for National Red Cross and Red Crescent Societies, available here: **https://www.icrc.org/en/document/rfl-code-conduct**.

CONDUCTING THE ASSESSMENT

The following steps will help to ensure that a data impact assessment is successful:

1. **Involve the right internal and external stakeholders**

   The roles and expertise needed to design and apply the assessment will vary based on the type of assessment, as well as the type and scale of the activity that will be assessed. The skills needed include:

   - Legal and compliance expertise in data protection, privacy and human rights
   - Technical and data management knowledge of the data management activity
   - Knowledge of the context in which the data management activity is taking place

2. **Clarifying the consequences of assessment outcomes**

   Define the potential outcomes and their consequences ahead of the assessment itself. An assessment typically leads to any of the following outcomes:

   A. The negative consequences associated with data management are non-existent or negligible. In these cases, the data management activity can continue.

   B. The negative consequences are unacceptable. To continue, the design of the data management activity should be revisited. Once negative consequences are brought into balance with the expected benefits, the activity can continue.

   C. The negative consequences are unacceptable and cannot be mitigated. In such cases, the data management activity should be cancelled.

3. **Adapt the assessment to the context**

   The assessment may need to be adapted to a specific risk in the context of the data management activity.[14] This involves adding additional focus areas based on the concerns of vulnerable populations.[15]

4. **Determine when to reassess**

   Since data management and the context in which it takes place are not static, regular reassessments should be scheduled at the outset of an activity. The conditions under which a reassessment may be required — such as a drastic change in data management or the context in which it takes place — should also be determined.

5. **Make a distribution plan**

   Decide who should be able to read the assessment results and be clear about how they will be shared with difference audiences.

[14] See for example the United Nations Global Pulse Risks, Harms and Benefits Assessment tool which also appears on page 5 of this Guidance Note and is available here: **https://www.unglobalpulse.org/policy/risk-assessment/**.

[15] See the Privacy International and ICRC report 'The Humanitarian Metadata Problem: "Doing No Harm" In The Digital Era', October 2018, available from **https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era**.

RECOMMENDATIONS

The Centre for Humanitarian Data and the collaborators on this guidance note recommend that organisations focus on the following areas:

1. **Design standard data impact assessment tools**

   A standard assessment can draw on commonly used and established assessment tools. Taking a standardised approach and adjusting it for the given context reduces friction and saves time if the tool is already submitted for internal legal and management review.

2. **Develop the capacity to conduct assessments**

   Identifying, developing and updating the skills required for assessments helps prevent delays in conducting assessments, and reduces the chance of flawed or incomplete assessment outcomes.

3. **Share data impact assessment outcomes**

   Assessment results should be shared to the extent possible and as long as it does not compromise the confidentiality of operational activities.

Organisations are encouraged to share their experience in assessing risks, harms, and benefits of data with the Centre for Humanitarian Data via centrehumdata@un.org.

COLLABORATORS: **UN GLOBAL PULSE**; **THE INTERNATIONAL COMMITTEE OF THE RED CROSS**; **PRIVACY INTERNATIONAL**.

The **Centre for Humanitarian Data** ('the Center'), together with key partners, is publishing a series of eight guidance notes on Data Responsibility in Humanitarian Action over the course of 2019 and 2020. The Guidance Note series follows the publication of the **working draft OCHA Data Responsibility Guidelines** in March 2019. Through the series, the Centre aims to provide additional guidance on specific issues, processes and tools for data responsibility in practice. This series is made possible with the generous support of the Directorate-General for European Civil Protection and Humanitarian Aid Operations (DG ECHO).



This project is co-funded by the European Union

This document covers humanitarian aid activities implemented with the financial assistance of the European Union. The views expressed herein should not be taken, in any way, to reflect the official opinion of the European Union, and the European Commission is not responsible for any use that may be made of the information it contains.