OCHA centre for humdata

THE CENTRE FOR HUMANITARIAN DATA

SÉRIE DE NOTES D'ORIENTATION
LA RESPONSABILITÉ DES DONNÉES DANS L'ACTION HUMANITAIRE

DATA IMPACT ASSESSMENTS

KEY TAKEAWAYS:

- Data Impact Assessments (DIAs) 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 DIAs. Selecting the right assessment for a given data management activity can help minimize the risks and maximize the benefits 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

Guidance on data responsibility[1] in humanitarian action often contains tools for conducting Data Impact Assessments ('DIAs' or 'assessments'). The purpose of conducting a DIA is to understand the positive and negative consequences of a data management activity. DIAs are a key component of accountability mechanisms and can serve to demonstrate compliance with applicable law, regulations, internal policies and other guidance.[2] Even when not obligatory, a DIA is advisable to help maximize benefits and minimize risks associated with operational data management.[3]

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. Examples of common data management activities are registration exercises and protection monitoring.

DIA 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 or 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.

[1] Defined as the safe, ethical and effective management of data. For more information, see the working draft **OCHA Data Responsibility Guidelines**.

[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. The literature review is available from the Centre for Humanitarian Data ("The Centre") upon request.

[3] Positive implications of data management are usually referred to as 'benefits', while negative implications include risks and harms – with rights infringements often called out specifically.

[4] DIAs contribute to Data Protection by Design or Privacy by Design if they are conducted at the outset of the development or use of a new tool or architecture. For more information, see for example **Privacy By Design, The 7 Foundational Principles**.

TYPOLOGY OF ASSESSMENTS

There are many different approaches to DIAs. Some of the most common 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 organization 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 in which they were developed.

FOCUS AREAS

Organisations should consider the following focus areas when selecting a model or tool for undertaking the assessment:

- **Risk** is the likelihood and impact of harm resulting from operational data management.[5] Risk is included as a focus area in most DIAs.
- **Harm** consists of a negative consequence of a data management activity for an individual or group of individuals. DIAs typically cover harms such as physical harm to individuals, stigmatization of groups and the impairment of aid delivery. Such harm can impact different stakeholders, including affected people and aid workers.
- **Benefit** relates to the potential positive impact of data management, often measured in the provision of humanitarian aid or resource efficiency gains.[6] Operational data management can benefit various stakeholders, with an inherent focus on affected people.
- **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, the right to life and other rights that are relevant in humanitarian response situations.[8]

DIAs can take into account one or more of these focus areas. Variations reflect the applicability of legal frameworks, organizational priorities and other factors, and can mean that one assessment is better suited than others in a given context.

DECIDING TO DO AN ASSESSMENT

Answer the following questions to determine whether an assessment is needed and if so, which areas to focus on:

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 which focus areas should be included. Required DIAs may be supplemented by additional steps, either taken from existing templates or designed for the data management activity at hand.

[5] The International Standardization Organization (ISO) defines risk as 'the effect of uncertainty on objectives', which is 'usually expressed in terms of risk sources, potential events, their consequences and their likelihood.' See the **ISO 31000:2018 Risk Management Guidance**.

[6] See for example the **United Nations Global Pulse Risks, Harms and Benefits Assessment tool**.

[7] For an example of a Data Protection Impact Assessment template, see Brussels Privacy Hub (VUB) and International Committee of the Red Cross (ICRC) **Handbook on Data Protection in Humanitarian Action (2nd edition)**, 2020, p. 299.

[8] See for example the **OHCHR Guiding Principles on Business and Human Rights**, and for an example of a human rights centered approach, this **report on the role of new technologies for the realization of economic, social and cultural rights** (in particular para. 46).

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 activity entail the management of sensitive data?**
   Data is 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. A DIA should always be conducted if such data is likely to be managed in a given activity.

4. **Is data management taking place in a particularly sensitive response context?**
   Incertain operational settings, humanitarian data management activities warrant additional caution. A context can be 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. Where private actors are involved, consider issues around data access, governance and ownership.

5. **Will the data management activity be systematic or large-scale?**
   Systematic and/or large-scale data management activities require assessments that account for a longer timeframe and include plans to update or repeat the assessment at a later stage. Examples include annual Multi-Cluster Needs Assessments or a country-wide beneficiary registration system.

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

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

TOOLS FOR ASSESSMENTS

While there is no single approach to DIAs across the humanitarian sector, there are various publicly available tools and templates that can be adapted 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.[10]

- 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.[11]

- The International Red Cross and Red Crescent Movement uses a data impact assessment that is focused on data protection when restoring family links.[12]

[9] See for an example of a template Data Impact Assessment this **RFL template for National Red Cross and Red Crescent Societies**.

[10] 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.

[11] Brussels Privacy Hub (VUB) and International Committee of the Red Cross (ICRC) **Handbook on Data Protection in Humanitarian Action (2nd edition)**, 2020, p. 299.

[12] **RFL template for National Red Cross and Red Crescent Societies**.

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 other 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.

CONDUCTING THE ASSESSMENT

The following steps will help organizations ensure that a DIA is successful:

1. **Involve internal and external stakeholders with the right expertise**
   The roles and expertise needed to design and apply the DIA will vary based on the type of assessment, as well as the type and scale of the activity that will be assessed. Relevant expertise includes:
   - Legal and compliance expertise in data protection, privacy and human rights
   - Technical understanding of the data management activity
   - Knowledge of the context in which the data management activity is taking place

2. **Clarify the consequences of possible assessment outcomes**
   Define the potential outcomes and their consequences ahead of the DIA. 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 minimal and can be mitigated to be in balance with expected benefits.

   C. 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.

   D. 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 the context in which the data management activity takes place. This involves adding additional focus areas as needed in order to assess context-specific risks or concerns of affected people.[13]

[13] Privacy International and ICRC report **'The Humanitarian Metadata Problem: "Doing No Harm" In The Digital Era'**, October 2018.

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 significant 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 access the assessment results and be clear about how the results will be shared with different audiences.

RECOMMENDATIONS FOR IMPROVING THE USE OF DIAS

The Centre and the collaborators on this guidance note recommend that organizations focus on the following areas to improve the use of DIAs for operational data management:

1. **Designing standard assessment tools**
   Taking a standardized approach to DIAs and adjusting it for the given context reduces friction and saves time. Organizations can draw on commonly used and established assessment tools to design their own standard approach. Submitting a tool for internal legal and management review and endorsement helps streamline its future use.

2. **Develop the capacity to conduct assessments**
   Identifying, developing and updating the skills required for assessments helps prevent delays in conducting DIAs and reduces the chance of flawed or incomplete assessment outcomes.

3. **Share data impact assessment results**
   Assessment results should be shared to the extent possible and as long as it does not expose confidential or otherwise sensitive information.

Organizations are encouraged to share their experience in assessing the positive and negative consequences of operational data management with the Centre 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 **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.