OCHA centre for humdata

THE CENTRE FOR HUMANITARIAN DATA

GUIDANCE NOTE SERIES
DATA RESPONSIBILITY IN HUMANITARIAN ACTION

RESPONSIBLE DATA SHARING WITH DONORS

KEY TAKEAWAYS:

- Sharing sensitive personal and non-personal data without adequate safeguards can exacerbate risks for crisis-affected people, humanitarian organizations and donors.
- Donors regularly request data from the organizations they fund in order to fulfil their obligations and objectives. Some of these requests relate to sensitive information and data which needs to be protected in order to mitigate risk.
- Common objectives for data sharing with donors include: (i) situational awareness and programme design; (ii) accountability and transparency; and (iii) legal, regulatory, and policy requirements.
- Common constraints related to sharing data with donors include: (i) lack of regulatory framework for responsibly managing sensitive non-personal data; (ii) capacity gaps; and (iii) purpose limitation.
- Donors and humanitarian organizations can take the following steps to minimize risks while maximizing benefits when sharing sensitive data: (i) reviewing and clarifying the formal or informal frameworks that govern the collection and sharing of disaggregated data; (ii) formalizing and standardising requests for sensitive data; (iii) investing in data management capacities of staff and organisations; and (iv) adopting common principles for donor data management.

INTRODUCTION

Donors have an important role in the humanitarian data ecosystem, both as drivers of increased data collection and analysis, and as direct users of data. This is not a new phenomenon; the need for accountability and transparency in the use of donor funding is broadly understood and respected. However, in recent years, donors have begun requesting data that can be sensitive. This includes personal data about beneficiaries and various forms of disaggregated data, such as household-level survey results and data about the delivery of assistance disaggregated by demographic and/or group dimensions (e.g. ethnicity, protection group, etc.).[1]

Concerns around requests for such data have led donors and humanitarian organizations to place more emphasis on identifying strategies for data responsibility: the safe, ethical and effective management of data. Data responsibility requires donors and humanitarian organizations to take actions that help minimize risks while maximizing benefits of data. This is particularly challenging in cases where donors request sensitive data. For example, the screening of aid recipients, which is often used to justify requests for personal data, is not only difficult to practically implement, but also highly problematic in terms of principled aid.[2]

[1] Because there are well-established and accepted standards and mechanisms for sharing financial information with donors, including a role for external audits, requests for financial data are not included in this guidance note. This guidance note deals with sensitive personal and non-personal data.

[2] Roepstorff, K., Faltas, C. and Hövelmann, S., 2020. **Counterterrorism Measures and Sanction Regimes: Shrinking Space for Humanitarian Aid Organisations**.

In addition, sharing seemingly innocuous data such as aggregated survey results can place already vulnerable people and communities at greater risk. What may be initially considered non-personal data[3] can allow for re-identification of individuals, communities and demographic groups. Re-identification occurs when data can be traced back or linked to an individual(s) or group(s) of individuals because it is not adequately anonymized. This can result in a violation of data protection, privacy and other human rights and can allow for targeting of individuals or groups with violence or other forms of harm.[4]

Many donors and humanitarian actors recognize the risks and benefits associated with sharing such sensitive data, but the sector has yet to establish a common understanding of how to balance these risks and benefits effectively. Recent efforts to address this issue have led to more clarity on current practices, as well as on the objectives and constraints of data sharing. In September 2020, the Government of Switzerland, the International Committee of the Red Cross (ICRC) and the United Nations Office for Coordination of Humanitarian Affairs (UN OCHA) Centre for Humanitarian Data (the Centre) organized a virtual Wilton Park dialogue to help build common understanding on this issue.[5]

This guidance note synthesizes the outcomes of this dialogue and a related desk review.[6] It describes the challenges around sharing sensitive data with donors and offers initial recommendations for how donors and humanitarian organizations can more effectively navigate this area.

DONOR REQUESTS FOR DATA

Donors regularly request data from their partners in order to fulfil different obligations and objectives. These requests can be either formal or informal.

- **Formal requests** tend to be included in grant agreements in relation to reporting criteria, and are typically based on legal requirements such as compliance with counter-terrorism laws. Such requests tend to be negotiated at the outset of a partnership or grant agreement, and are usually made in writing and scheduled in advance.

- **Informal requests** concern information or data that typically fall outside of the normal scope of reporting. These ad-hoc requests often carry implicit value, meaning that while they are not formally required, delivering this supplementary data is deemed beneficial for an organization's ongoing engagement and partnership with a donor. These requests represent a greater dilemma for humanitarian actors.

Few donors have formal data sharing policies or guidelines in place.[7] There is also a lack of shared understanding of terminology and of the objectives and risks around data sharing. There are different definitions and understanding of data-related risks, leading to inconsistent and sometimes contradictory practices around sharing potentially sensitive data with donors in a particular context.[8]

[3] Non-personal data is defined as data which 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 (adapted from **Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union**).

[4] See the **Working Draft OCHA Guidelines for Data Responsibility** and the **ICRC Handbook on data protection in humanitarian action**.

[5] Read more about the virtual dialogue in this **Wilton Park Report**.

[6] Willits-King, B. and Spencer, A., 2020. **Responsible data-sharing with donors: accountability, transparency and data protection in principled humanitarian action**.

[7] At the time of writing, only USAID and GIZ had publicly available guidelines on responsible data sharing. See USAID, 2019. **Considerations for using data responsibly at USAID** and GIZ, 2018. **GIZ's Responsible Data Principles**.

[8] Willits-King, B. and Spencer, A., 2020. **Responsible data-sharing with donors: accountability, transparency and data protection in principled humanitarian action**.

OBJECTIVES FOR DATA SHARING WITH DONORS

The most commonly identified objectives for donors requesting sensitive data from partners are situational awareness and programme design; accountability and transparency; and legal, regulatory, and policy requirements.

Situational awareness and programme design
Donors seek information and data from humanitarian organizations in order to understand and react to changes in humanitarian contexts. This allows donors to improve their own programme design and evaluation, prevent duplication of assistance, identify information gaps, and ensure appropriate targeting of assistance.

Accountability and transparency
Donors and humanitarian organizations have an obligation to account for their activities. Data can enable donors to explain and defend funding on foreign aid to taxpayers.

Legal, regulatory, and policy requirements
Donors are subject to certain national and international legal requirements, including political, legal and statutory requirements related to counter-terrorism, migration and law enforcement. In many cases, donors might want to use data to verify their compliance with these different requirements. Some donors include counterterrorism clauses in their grant agreements, which are intended to ensure that their funds are not used to benefit designated terrorist groups.[9] Similarly, donors might include clauses to cover anti-bribery, anti-fraud and anti-corruption measures.[10]

CONSTRAINTS FOR DATA SHARING WITH DONORS

Despite these objectives, data sharing with donors is not without its constraints, which include a lack of regulatory frameworks for responsibly managing sensitive non-personal data, capacity gaps and lack of purpose limitation.

Lack of regulatory frameworks for responsibly managing sensitive non-personal data
The sensitivity of personal data is generally well-known and addressed by a variety of policy and regulatory frameworks, but the same cannot be said for sensitive non-personal data. Protecting groups and their data remains challenging due to the current gaps in regulation and guidance and the overall lack of understanding regarding the sensitivity of non-personal data. These data policy gaps increase the risk of sensitive data not being stored or protected adequately or shared inadvertently by partners in order to satisfy donors' requests.

Capacity gaps
Responding to ad-hoc data sharing requests from donors can be viewed as an additional burden to humanitarian responders, diverting critical time, resources and focus away from other implementing activities.[11] Insufficient funding for data-related capacity development has limited many organizations' ability to provide their staff with the skills and resources required for managing data responsibly.[12] Gaps in capacity to fulfil donor requirements might also deter smaller and/or local NGOs from seeking funding, undermining localization efforts.[13]

[9] See NRC's **Toolkit for Principled Humanitarian Action; Managing CT Risks**.

[10] In order to ensure compliance, donors might request highly disaggregated data to corroborate their due diligence processes, ensuring their partners are not engaging with any 'sanctioned' person or entity'. See Walker, J., 2020. **Compliance Dialogue on Syria-Related Humanitarian Payments**. 'Sanctioned persons' is a general term which may include individuals, terrorist groups, governments as well as companies and other entities of legal personality. The EU, for example, has over the years considerably strengthened its legal framework for preventing money laundering and terrorism financing in recent years and is constantly enforcing in. See: NGO Voice, 2020. **The Impact of EU Sanctions and Restrictive Measures on Humanitarian Action.**

[11] Inter-Agency Standing Committee (IASC) Humanitarian Financing Task Team (HFTT), 2016. **Donor Conditions and their implications for humanitarian response**.

[12] Publish What You Fund, 2020. **Data Use Capacity in Protracted Humanitarian Crises**.

Purpose limitation
The principle of purpose limitation requires that data is only collected for specified, explicit and legitimate purposes, and that it not be processed further in a manner that would be incompatible with those purposes.[14] Even when donors specify legitimate reasons for requesting data in-line with the original purposes for which the data was collected (e.g. the delivery of humanitarian assistance), it can be difficult to ensure that the data will not be used for other purposes once shared. Data used out of context and for purposes that are not known at the time of sharing, or retained past the intended retention for a defined purpose represents a violation, even if unintended, of the data subjects' rights.

RECOMMENDATIONS

In view of the objectives and constraints detailed above, the Centre, the Humanitarian Policy Group (HPG) at ODI, the ICRC, and the Human Security Division of the Swiss Federal Department of Foreign Affairs recommend that donors and humanitarian organizations take the following steps to minimize risks while maximizing benefits when sharing sensitive data:

- **Reviewing and clarifying the formal or informal frameworks that govern the collection and sharing of disaggregated data**
  Donors and partners should examine the official, formal requirements and ad-hoc, informal requirements of data sharing, and analyse partner and donor staff interpret whether requirements correctly and consistently. They should assess whether there are implicit conditionalities between the willingness to share disaggregated data and the ability of different organizations to access and sustain funding from donors.

- **Formalizing and standardizing requests for sensitive data**
  When sensitive data is required to meet a mutually agreed objective, donors should formalize and standardize their requests for such data. Requests should be made in writing and should specify which data is requested, the format desired, and the intended use of the data. Donors should only request the information required to meet the specified purpose for which it is being requested and should indicate a timeline for destruction of the data. Humanitarian organisations should document all requests for data and ensure consistency in responding to these requests over time.

- **Investing in data management capacities of staff and organizations**
  Donors and humanitarian organizations should identify opportunities to invest in building data management expertise especially for non-technical staff. The donor community is uniquely positioned to encourage data responsibility by providing additional resources for training and capacity building.

- **Adopting common principles for donor data management**
  The sector already has a range of principles and commitments to inform different aspects of humanitarian donorship.[15] However, these do not sufficiently address concerns related to data responsibility. Donors and partners should engage in the development of common principles and guidelines for donor data sharing to fill this gap. The **Humanitarian Data and Trust Initiative**, co-led by the Government of Switzerland, the ICRC, and the Centre, offers a platform to facilitate this process as part of its ongoing work to build trust through dialogue.

Organizations are encouraged to share their experience in responsible data sharing with donors with the Centre for Humanitarian Data via **centrehumdata@un.org**.

[14] ICRC, 2020. **Handbook on data protection in humanitarian action**.
[15] Examples include the **Good Humanitarian Donorship Initiative** and the **Grand Bargain**.

COLLABORATORS: **THE HUMANITARIAN POLICY GROUP AT ODI; INTERNATIONAL COMMITTEE OF THE RED CROSS;** AND **THE HUMAN SECURITY DIVISION, SWISS FEDERAL DEPARTMENT OF FOREIGN AFFAIRS.**

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.