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**.