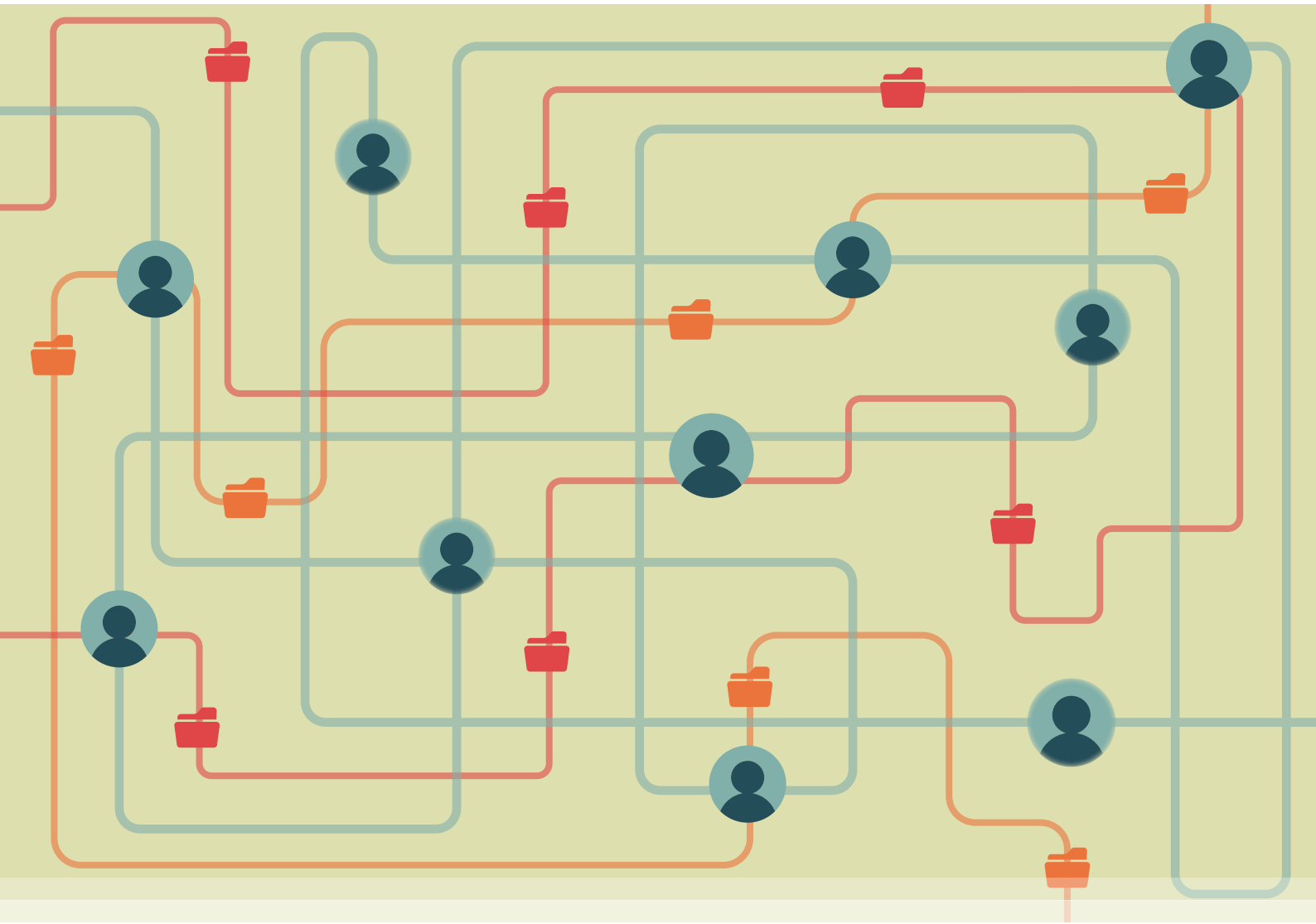
HPG working paper

# Data sharing and third-party monitoring in humanitarian response

Stephanie Diepeveen[ID], John Bryant[ID], Farhia Mohamud, Mahad Wasuge and Hassan Guled

September 2022



HPG Humanitarian Policy Group

ODI

Somali Public Agenda

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Federal Department of Foreign Affairs FDFA**

This report is made possible by the generous support of the Swiss Federal Department of Foreign Affairs (FDFA). The contents are the responsibility of ODI and do not necessarily reflect the views of FDFA or the Swiss Government.



**How to cite:** Diepeveen, S., Bryant, J., Mohamud, F. et al. (2022) *Data sharing and third-party monitoring in humanitarian response*. HPG working paper. London: ODI (www.odi.org/en/publications/data-sharing-and-third-party-monitoring-in-humanitarian-response).

This PDF has been prepared in accordance with good practice on accessibility.

Cover graphic: Emma Carter

# Acknowledgements

The authors wish to express their thanks to their colleagues at both ODI and Somali Public Agenda, including Oliver Lough, Sorcha O'Callaghan and Marta Lopes. Thank you also to Stuart Campo, Larissa Fast, Claudia Meier, Jonas Belina and Vincent Annoni for your insights and guidance throughout, and to all our interviewees who gave their time and expertise to inform this study.

## About the authors

ORCID numbers are given where available. Please click on the ID icon next to an author's name in order to access their ORCID listing.

**Stephanie Diepeveen**[ID] is a Research Fellow at the Politics and Governance Programme (POGO) at ODI.

**John Bryant**[ID] is a Senior Research Officer at the Humanitarian Policy Group (HPG) at ODI.

**Farhia Mohamud** is a Researcher at Somali Public Agenda (SPA).

**Mahad Wasuge** is the Executive Director of SPA.

**Hassan Guled** is a Researcher at SPA.

# Contents

# List of boxes, tables and figures

## Boxes



## Tables



## Figures

# Glossary

| | |
|---|---|
| **Aggregate data** | Accumulated data acquired by combining individual-level data. It refers to data that is: (1) collected from multiple sources and/or on multiple measures, variables or individuals; and (2) compiled into data summaries or summary reports, typically for the purposes of public reporting or statistical analysis (IASC, 2021). |
| **Data** | Information that can be easily interpreted, collated together, processed or shared for the purposes of improving knowledge (IASC, 2021). |
| **Data life cycle** | The stages a particular piece of data goes through, from collection through to analysis, sharing and eventual deletion. |
| **Data sharing** | The exchange of digital data between organisations. This can take different forms, for example, raw data, or aggregated or anonymised data. |
| **Digital rights** | The right to access, use and create digital media and technology – critical means to ensure freedom of expression and privacy. |
| **Funder** | In the context of this report, any organisation (including both donors and humanitarian organisations) that contracts a third-party monitor for data collection and analysis of programmes. |
| **Meaningful consent** | The ability of an individual to autonomously agree they are willing to provide information about themselves, with the full understanding that they know what data is being collected, who it is being shared with and why it is needed. Information should be easily digestible and the choice to opt out clear and accessible. An individual should not feel pressured to consent or be disadvantaged for choosing to opt out. |
| **Personal data** | Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data (European Commission, 2022). |
| **Third-party monitoring** | The contracting of third-party organisations by donors and humanitarian organisations for data collection and analysis of programmes. For more details, see Box 1. |

# Executive summary

Responsible data sharing is a growing area of concern in the humanitarian sector. The adoption of new digital tools and a drive for more granular monitoring of programmes have meant humanitarian crises are increasingly 'data-rich' environments. Efforts to gain better understanding of contexts, quantify the impact of programmes and coordinate responses have meant more data sharing seems unavoidable. Yet at the same time, concerns around the impact of such a trend have grown more prominent. Major data breaches, including those recently affecting the International Committee of the Red Cross (ICRC), have raised questions around the risks to already-marginalised people when data collected by aid providers is inadequately protected and falls into the wrong hands.

The introduction of private sector actors to support humanitarian action can bring new opportunities for using data, but also different sets of risks. Third-party monitoring (TPM) is a key part of this picture of humanitarian data that encompasses sharing and risks. TPM – the process of an independent entity assessing the outputs and performance of programmes – is a growing industry in the humanitarian sector. One report in 2016 estimated that in Afghanistan alone, approximately $200 million had been spent on TPM annually since 2006 (Sagmeister and Steets, 2016). With increasing pressure on funders to justify their spending, TPM is seen as a necessary element of the contemporary, digitally enabled humanitarian system. It is also a reliable and independent means of ensuring accountability through third-party monitors' (TPMs') impartial assessments of humanitarian programmes. Data is central to this work, with organisations often gathering and analysing valuable information on aid users that can be personally identifiable and sensitive. As a result, these monitoring organisations should be considered a key part of the humanitarian data system, which is more usually understood as being limited to humanitarian organisations, funders and crisis-affected people.

This working paper explores risks and mitigation efforts around data sharing for the humanitarian sector through a focus on the data sharing relationships involved in third-party monitoring. It provides insights into data sharing risks linked to the introduction of external, often private sector, organisations into the humanitarian ecosystem. It interrogates the nature and distribution of risk, data responsibility, and opportunities for mitigating risks and realising value through data sharing for the diverse stakeholders involved. The intention of this paper is to shed some light on a less-explored but important group of actors and processes of data sharing in the humanitarian sector. In doing so, it aims to highlight wider issues and propose recommendations that are applicable for the responsible sharing of data in the sector more generally.

## Key findings

**Data risks relating to TPM mirror wider patterns of risk around data sharing in the humanitarian sector.** While this process introduces new external (often for-profit) actors into humanitarian activity, the main risks to aid users and to humanitarian activity that emerge are the same as those of the wider sector. Issues of data responsibility, trust, well-being and meaningful consent remain, though with

specific inflections tied to the nature and conditions of the activity. This commonality indicates the potential value of sharing of lessons learnt on data risks and their mitigation across different actors and areas of activity in the humanitarian sector.

**Risks to the safety and well-being of those involved in TPM (including aid recipients, data enumerators, humanitarian organisations and funders) do not relate solely to data sharing.** There is insufficient attention paid to wider risks that are often heightened at the point of data collection. Since TPM is often justified on the grounds of the unacceptably high security risks to programme staff, risks are often carried by actors at the local level, including data enumerators and aid users themselves.

**TPMs often lack sufficient knowledge of the context and eventual use of the collected data to appreciate fully the risks associated with the process.** TPMs do not necessarily have an established presence in the place they are monitoring, are independent of humanitarian activity and often work through subcontractors. This can affect their awareness of risks around initial data collection and handling, and even compromise a context-specific understanding of what the data represents. A closer relationship between the TPM and realities on the ground, including closer working with local TPMs, could contribute to a more robust and complete assessment of risks and benefits.

**The large number, and fragmentation, of actors involved in data collection and management in the sector means few individuals or organisations have clear oversight of where the data has come from and how it is used.** Data sharing for monitoring purposes involves many actors: the organisation commissioning the monitoring, often multiple monitoring firms, humanitarian agencies, data collectors and aid users. The lack of dedicated responsibilities for the management of data risks means they are poorly understood and mitigated, with potential for heightened risks to aid users. Stronger consistent data protection standards could be held and enforced across this range of actors.

**TPM activities are highly contingent on trust – and mistrust. This leads to both inadequate oversight of data protection and to a limited willingness to share data.** Trust is unequally distributed across the humanitarian data system. At one end, donors and those contracting TPMs place a high level of trust in them, to the point that they can leave responsibility for data risk management to TPMs and limit their supervision of ongoing data management. At the other, there is often a lack of trust between TPMs and humanitarian agencies. As TPMs undertake monitoring and accountability tasks, their roles and requests for data are often met with suspicion by humanitarian agencies. This mistrust results in a lack of willingness to share data on the part of humanitarian agencies.

**Third-party monitoring creates tensions between funder accountability demands and risks to people's well-being.** While funders have pushed for greater accountability to ensure that programmes are being implemented as intended for the benefit of end users, humanitarian implementers raise concerns that collecting additional data can bring increased risks, as well as an unnecessary reporting burden. The stakeholders involved have placed different emphases on what is a justifiable balance

between a desire for accountability and concerns about risks to security and well-being. This remains an unresolved area for those involved, and one that requires careful discussion and planning in the early stages of a TPM project.

**Donors and those contracting TPM are increasingly seeking to use TPM data for learning purposes, as opposed to solely for accountability. However, there are challenges in achieving this outcome.** The push to learn is taking place without the requisite capacity to incorporate learning into programming, or consideration if the questions and insights from TPM are appropriate for learning by the different actors involved in implementation. This includes a lack of steps to share insights between different actors to facilitate learning. The absence of clear learning outcomes suggests that a lot of data for learning purposes is collected unnecessarily.

# Recommendations

## Overall recommendations

**How TPM data is created and held, and by whom (enumerators, local and international TPMs, implementers, funders), should be made more visible to all actors involved in its management.** While attention to data protection is growing, awareness of data handling practices is often fragmented across the different actors involved. Greater collective visibility of data handling practices could help to identify risks and improve awareness of the distribution of roles and responsibilities. A first step likely requires investigating the incentives and structures that contribute to fragmentation.

**Data collection processes should be subject to the same careful considerations of risk as data sharing more broadly.** Seeing 'data sharing' as a process that only happens between groups of funders and humanitarian organisations gives an incomplete understanding of the humanitarian data ecosystem. Many of the potentially harmful dynamics and risks of data sharing begin when it is initially collected. Therefore, efforts to mitigate these risks need to also re-centre affected people as being the first sharers of their own data and under-supported enumerators as being key actors. Both groups need to be better informed as to why data is being collected, while enumerators also require clearer support.

**All organisations involved in data sharing should take greater responsibility for the management of data risks across the range of data handling activities.** This includes looking beyond one's own activities and risks, to better understand how risks are distributed across stakeholders. Especially in insecure environments, security and trust-related risks are concentrated with those at the local level. Management tools like cost–benefit analyses of data sharing, evaluations and policy guidelines should give greater attention to the distribution of risks, and whether the benefits and compensation are sufficient.

## Recommendations for funders

**Organisations contracting TPM should lead in ensuring responsible data handling and take action to minimise risks for all stakeholders involved in the TPM.** Often, given the diverse locations, activities and subcontractors involved, no single actor has oversight of responsible data practices across a TPM programme or project. As those that have initiated TPM activity, organisations who contract TPM hold a unique position to set standards for data responsibility. This could be done, for example, by ensuring that adequate data handling clauses are part of TPM contracts, including a requirement that policies are transferred to all TPM subcontracts. At the same time, each participating actor should also act responsibly to uphold the highest standards of data management.

**Funders should be precise and realistic about the potential applications of TPM data.** An increasing desire to use TPM data to support learning (for example, for more efficient programme delivery) must be tempered by a clear assessment of whether the correct data is being collected, whether there is sufficient support in place to minimise risks, and whether learning outcomes can be achieved. In the humanitarian sector, there is an ambitious but not always clearly supported drift towards TPM data sharing for learning. Often learning is discussed in a broad manner, without clarity about how TPM data can be applied to improve programming. In situations where learning outcomes are unclear, data collection and use should be minimised to manage risks.

## Recommendations for third-party monitors

**TPMs should be considered part of the humanitarian system. They should have the same level of responsibility to minimise risks to crisis-affected populations and to manage and share data responsibly, as well as to uphold the same standards.** While TPMs are contracted to provide an independent perspective on humanitarian delivery, their data collection and sharing activities take place alongside and involve the same people and organisations. Considering them as separate actors can obscure the total scale and diversity of data-related risks facing crisis-affected populations and humanitarian actors.

**TPMs should uphold data minimisation.** TPM is often a data-intensive exercise. However, the amount of data collected can be disproportionate to that required to answer questions or to what the funder has capacity to absorb. A commitment to data minimisation can also help to build stronger relations of trust with implementing agencies, from whom data is requested, while minimising security risks for enumerators and aid users in data collection.

# 1 Introduction

Data sharing has the potential to improve humanitarian delivery, whether through more precise and real-time insights into situations on the ground, more efficient and evidence-based operations with less wasteful duplicated data gathering, or through greater accountability. At the same time, the question of what responsible data sharing, use and analysis looks like in the humanitarian sector is an important and critical debate. It grows ever more pressing as digital risks become more apparent and digital rights better articulated.

Data sharing invokes questions about digital rights, and whether meaningful consent is possible from end users in humanitarian contexts. Large-scale data breaches paint a sobering picture of the real risks that data can pose to the humanitarian commitment to 'do no harm'. Government donors and humanitarian organisations are increasingly interested in responsible data sharing and use, and there are louder calls from civil society advocates to recognise the agency and rights of formerly passive 'data subjects' to have greater control. Still, gaps remain in understanding the range of stakeholders involved, and who bears the risks. Addressing these risks is now a critical issue, given the rising use and value placed on data by humanitarian actors. Data sharing is seen as an opportunity to support sector reforms, by enabling more granular monitoring and evaluation that is more responsive to changing needs, and potentially a more remotely managed, digitally enabled system. However, there is a growing recognition among humanitarian actors that these opportunities must be considered in the context of the range of risks that data misuse can present to some of the world's most marginalised people.

This working paper aims to help humanitarian actors and donors better navigate the tensions between the opportunities presented by digital data for humanitarian accountability and learning, and the actual and potential risks involved. The humanitarian sector is complex, encompassing a diverse range of stakeholders. This diversity of actors and activities is reflected in data sharing practices, as data is used for a range of purposes and contexts, including needs assessments, delivery and implementation, and monitoring and evaluation. To tease out some practical issues within this much bigger set of data sharing practices, this paper focuses on data sharing and the introduction of new, private sector actors in the humanitarian system, specifically independent (often for-profit) organisations that provide independent monitoring, also known as 'third-party monitoring' (TPM). This study seeks to improve the understanding of TPM, as it relates to humanitarian data and the risks of data sharing.

## 1.1 What is third-party monitoring?

TPM takes different forms within the humanitarian sector; at its core, it refers to the contracting of third parties by donors and humanitarian agencies for data collection and analysis for verification and/or accountability. Often this is done by private for-profit entities, and includes local and international organisations that subcontract local partners (UN in Afghanistan Risk Management Unit, 2015). TPM sits alongside other forms of programme monitoring as a type of independent monitoring mechanism (Sagmeister and Steets, 2016). Such monitoring is used in insecure environments, to improve efficiency

and when there might be a lack of confidence in partner reporting, supplementing rather than replacing implementing agencies' own monitoring requirements. Because TPMs are not involved in the implementation of humanitarian activity and are separate from the funders of humanitarian activity, they are seen to provide an independent, impartial perspective on programme implementation.

While TPM is an important and growing area of data sharing within humanitarian action, it remains an under-researched area of activity (while TPMs are under-researched as actors). TPM introduces new actors into the humanitarian system who are by definition external to humanitarian delivery and contracted to provide an independent perspective. They interact with donors, humanitarian agencies and affected populations to collect, analyse and share information on delivery. Digital methods are often critical to their work, given the frequently insecure contexts, driving a push for remote monitoring as well as the promise of more granular and predictive analysis offered by such tools.

Recent studies have highlighted the importance of TPM as an activity and TPMs as a set of actors, since TPM is a rapidly growing industry in the humanitarian sector. Despite their integration into the humanitarian system, the roles and associated risks around TPMs within the humanitarian data system are still opaque:

> Donors often outsource to third parties to monitor programmes, for which third parties request and often collect the most detailed and sensitive data. While their work is legitimate, there is a lack of understanding about third party monitors and how they collect, use, and store data, a topic that surfaced repeatedly across interviews (Fast, 2022: 24).

## 1.2 Background and justification

The humanitarian sector is becoming increasingly aware, albeit belatedly, of the range and potential impact of the risks that digital technologies and data can present to response organisations and to the people they seek to assist. Since data sharing involves a variety of tasks, from collection to storage, processing, sending and analysing, the scope of vulnerabilities is wide. Vulnerabilities can also vary across these different tasks, depending on who is involved, with what technology, and what their interests and capabilities are in relation to the data and the humanitarian context. To further this agenda, the International Committee of the Red Cross (ICRC), United Nations Office for the Coordination of Humanitarian Affairs (OCHA) and the Government of Switzerland have led on the creation of the Humanitarian Data and Trust Initiative (HDTI),[1] which has provided a critical discussion and research agenda into the use of and risks around data sharing between humanitarian agencies and donors. In so doing, this work points to the need to expand the sector's understanding of both how data is shared and used in the sector, and how to more fully consider the complex group of stakeholders involved in such a process.

1 https://centre.humdata.org/introducing-the-humanitarian-data-and-trust-initiative/

There are many different types of data that are produced and shared within the humanitarian sector. These include, for example, data about individuals, which can be personal or non-personal, and in aggregated or disaggregated forms, and location-based data or administrative data, which is associated with a place or entity (see also Fast, 2022). Many different types of organisation are also involved with data. Different organisations collect, analyse and store data, while a larger group – including private actors, host governments and affected populations – are increasingly interested and aware of the value of information encased in data. While data sharing agreements and processes are increasingly codified, a limited focus on one single set of relationships – donors and the humanitarian organisations they fund – has resulted in an incomplete picture of who is involved and the distribution of vulnerabilities for harm and risks. This limitation is also present in common understandings of 'data sharing' as an activity, which is often studied as an activity in isolation. However, in practice, data sharing is part of a wider process: it is only possible and useful in the context of data creation and collection on one side, and its analysis and application on the other. To adequately mitigate the risks of data sharing, therefore, it is important to consider the impacts of the wider set of data practices that it necessarily entails, from data collection to its use. Consequently, in investigating data sharing around TPM in the humanitarian sector, this paper considers not only risks around the act of data sharing itself, but also the interdependent and interrelated ways of engaging with data that necessarily surround data sharing between a third-party monitor and a donor.

While, empirically, we focus on risks around data practices with funded TPM, our findings have wider relevance to the complex and diverse forms of data sharing that take place in the humanitarian sector. First, the many activities that take place alongside data sharing suggest the need for a more holistic approach to unpacking its benefits and risks. Second, both donors and humanitarian organisations are increasingly turning to TPMs to provide valuable monitoring and evaluation services. Finally, since TPMs share many of the data collection and management approaches of humanitarian organisations, the study also has lessons for the wider sector beyond data sharing. At a time of increasingly urgent demands for a humanitarian system that is more accountable not just to those that fund it, but also those who use its services, an overly complex and opaque data system is unhelpful. Such a system presents new and complex risks that many users and humanitarian staff are unfamiliar with and that ultimately threaten to diffuse responsibility and limit the means available to hold those involved to account.

## 1.3 Structure of this paper and underlying methods

This working paper investigates risks and mitigation efforts around data sharing for humanitarian sector TPM across the data 'life cycle'. We first mapped out the different actors involved in the creation and exchange of data around TPM, and then explored their different experiences of the benefits and risks of data through a document review and semi-structured interviews. Our framework for considering risk started from previous HDTI research (Westphal and Meier, 2020), and then used open-ended questions to probe additional areas of risk. In total, we conducted 40 interviews with various stakeholders.

**Table 1** Interviews conducted with stakeholders

| Type of stakeholder | Number of interviews |
|---|---|
| Donors | 10 |
| Implementing agencies and organisations | 10 |
| International third-party monitors | 4 |
| Somali-based third-party monitors | 10 |
| Researchers/other | 6 |

We focused on TPM in the context of humanitarian action in Somalia. Somalia presents a case study where TPM has become relatively well developed, linked to the protracted nature of remote funder working and concerns about accountability. During the Covid-19 pandemic, access was further restricted, with 'most programmes and activities requiring remote management with limited monitoring capability' (OCHA, 2021: 39). We also reviewed public reports, and academic literature on data sharing in relation to TPM more widely.

Ethics and time constraints limited the scope of the study and indicated room for future research. First, while pointing to the importance of accounting for the engagement and perceptions of affected populations of data sharing, we were unable to conduct interviews with recipients of humanitarian assistance directly. The research team did interview enumerators and local TPMs in Somalia who had directly engaged with aid users. However, our views of affected populations were nonetheless secondary. The frequency and repetition with which some end users had been interviewed by various humanitarian actors (for example, from needs assessments to monitoring) suggests careful thought is needed into how best to conduct any further research on this topic. Second, due to confidentiality concerns, we were not able to review most TPM reports for the actors interviewed. As such, much of this research is about the perceptions of different actors on data sharing practices. Given this situation, we highlight in the paper where contradictions emerge in stated perceptions. How and why these divergent perspectives play out in practice could also be worth further investigation.

# 2 Third-party monitoring and data sharing: practices and opportunities

This chapter provides a background to data sharing practices and to TPM in the humanitarian sector. It focuses on the rationale and perceived benefits that come through the use and sharing of data for TPM. First, it outlines the general importance of attention to data sharing in the humanitarian sector. It explains how data sharing is becoming increasingly central to humanitarian action, not as a subset of activity but integrated into operations, including assessments, delivery and evaluation, and why this makes it so important to understand the potential for harm. Second, it looks specifically at TPM: what it is, how and where it is taking place, and the specific data roles related to it. Third, it concludes with how stakeholders in the humanitarian sector have understood the benefits of data sharing for the purposes of TPM.

## 2.1 Data sharing in the humanitarian sector

The incentives for humanitarian organisations to share more data are growing (Fast, 2022). Data transparency is now recognised as a necessity for many agendas, and can support accountability on the part of humanitarian agencies for delivery on their programme objectives. More coordinated and streamlined data collection processes can contribute to more efficient and informed programmes and decision-making, building from information collected from experiences on the front lines. Also, sharing data can enable a greater array of stakeholders to learn from and incorporate insights from that data. Data is often proprietary with limited access. Greater data sharing, therefore, can help to better equip smaller, local actors with fewer resources and lower capacity to engage effectively, through data sharing by larger actors who are more equipped to collect, analyse and use data. Commitments to improve data sharing in the name of beneficial outcomes for the humanitarian sector have been key elements of recent advocacy (Centre for Humanitarian Data, 2022) and underpin larger goals in reform agendas like the Grand Bargain (Metcalfe-Hough et al., 2021).

From the perspective of most organisations involved, the primary reason for data gathering and sharing with funders remains accountability. To justify the continuation of humanitarian aid, including to funder publics in the global North, and to demonstrate that money has been spent well, humanitarian programming needs to be proved effective, while fraud, diversion and misuse need to be demonstrated to be low. The logic behind TPM is that independently operated surveying and other tools can effectively monitor the receipt of aid and services on the ground. However, from the perspective of implementers and funders, sharing evidence of programme impact may also provide a basis for more flexible, less earmarked, multi-year funding over the longer term. TPM and TPMs, as an activity and a group of actors, have an important function in this equation, offering the independent monitoring perceived to be necessary for this exchange.

In the humanitarian sector, data sharing also serves an ever more important role for learning, capacity building and constructing a context-level picture of a crisis. Crucially, a more open data system is also one that has the potential to benefit affected people themselves by creating a more participatory approach to context and needs assessments that are not just the preserve of well-resourced international organisations.

As the justification for data sharing grows, the importance of responsible data practices also increases. Evidence of large-scale data breaches, with the loss of personally identifiable data on recipients of humanitarian action, provides a sobering picture of the potential for data to be accessed by malicious or unintended actors. Though the aid sector had previously been victim to smaller-scale hacking attempts, the 2017 'Red Rose' hack, in which a corporate rival of a digital payments platform gained access to sensitive information of 8,000 individuals receiving aid across West Africa, became a prominent example (Parker, 2017). Fears of a mass breach harming many already-marginalised people with consequences for the entire aid sector have been frequently raised since (Bryant, 2021: 24). As Afghanistan was retaken by the Taliban in August 2021, the country's detailed biometric registry, including details of those working for the former administration, fell into the hands of those carrying out reprisals (Jacobsen and Steinacker, 2021). Last year, further details of the handover of biometric data of Rohingya refugees by United Nations (UN) agencies to the Governments of Bangladesh and then Myanmar – the state responsible for their persecution and displacement – came to light (HRW, 2021). Most recently, the ICRC was the target of a cyber-attack, likely by a malicious state actor, in which the personal details of half a million aid users were compromised. Though concerning, the ICRC's public admittance of the incident is not common, and it is likely that large UN agencies and other humanitarian entities have also been targeted.

In such an apparently fraught context, how to maximise the benefits of data sharing while avoiding these incidents and promoting responsible practices remains a pressing – but difficult – question that has started to attract wider attention. This paper aims to make a practical intervention into addressing these tensions and trade-offs by exploring the type and distribution of benefits and risks of data sharing for accountability purposes, specifically when involving independent, for-profit firms.

## 2.2 The role and rationale for third-party monitors in the humanitarian sector

With increasing demands for accountability in humanitarian action, including in insecure, inaccessible contexts, there is a push among many donors for greater use of TPMs. A variety of benefits of TPM in general were raised by interviewees, specifically funders who commissioned TPM. First, TPM helped to address difficulties facing funders in ensuring the accountability of programme delivery in insecure and/or volatile environments. Funders viewed TPM as one way to gain greater insight into what was taking place on the ground when staff were remote. Second, because they were not involved in implementation, TPMs were viewed as having greater independence and were therefore more likely to provide a full and critical picture of activity on the ground. Third, we found that TPMs were perceived to often have greater data literacy than humanitarian actors – including the capacity to collect, analyse and visualise data. As private sector actors with part of their unique selling proposition being data

collection and analysis for monitoring and evaluation, they were seen to be specialised actors that could bring greater rigour to monitoring. Finally, as TPM becomes increasingly integrated into programmatic activity in the humanitarian sector, some have started to ask if their data can have additional purposes – for example, supporting programmatic learning and adaptation by providing independent and real-time insights. Different views, and potential tensions, around the perceived added value of TPM are touched on later in this paper.

### Box 1 Third-party monitoring in Somalia

To explore TPM in more detail, we focused on its use in Somalia. A robust TPM process materialised in Somalia as part of a move to improve monitoring in the early 2010s in response to concerns about mismanagement. A few funders set up TPM with their multi-year programmes after large-scale corruption and diversion scandals emerged in the aid system around the 2011–2012 famine. At the time, TPM was a relatively new approach for humanitarian donors. Since then, TPM has become increasingly common among donors in Somalia, giving rise to a proliferation in international and local actors involved in collecting, analysing and reporting for TPM. Donors have utilised different ways of collecting data for monitoring through third parties in Somalia. In addition to data collection through local third-party organisations, some have also created call centres, as a complaints mechanism but also to obtain data on issues around implementation. While not representative of the wider sector given the country's longer history and industry around TPM, Somalia provides insights into the complex dynamics of different interests, perspectives and risks that can arise around TPM activity when funders are located remotely. As such, it is relevant to other humanitarian contexts such as Yemen, northeast Syria and northeast Nigeria.

For its advocates, TPM is a key element of a humanitarian data system that facilitates responsive project management, providing organisations with the ability to spot issues in 'near real time' and respond accordingly, 'embedded' in the programme cycle. Though evaluations remain output focused, extensive monitoring is useful for improving programme delivery. If humanitarian actors can gain a more precise understanding of where there are gaps in meeting the needs of vulnerable populations (for instance, which locations are struggling with effective delivery), they might be better able to fill those gaps. There is a working assumption that more granular data might limit the risks of uneven distribution of assistance or that it could mitigate against some forms of exclusion.

# 3 Risks of data sharing around third-party monitors

This chapter considers how wider risks around data sharing in the sector play out around TPM, and what potential new risks arise linked to the particularities of introducing new, often for-profit, actors into the humanitarian system in insecure environments where funders are not present.

Looking at data sharing between donors and humanitarian agencies, the Global Public Policy Institute (GPPi; Westphal and Meier, 2021) highlight two categories of risk: to individuals and groups supported by humanitarian assistance, and to the perceptions and reputations of humanitarian actors. High-profile data breaches from organisations like the ICRC present risks for the reputations of organisations that work with some of the world's most vulnerable people; yet the risks of data breaches fall overwhelmingly on aid users themselves, whose information is compromised (ICRC, 2022). In humanitarian settings, data risks do not just relate to personal data. The risk of ascertaining sensitive data by combining non-sensitive datasets – a process known as data 'mosaicking' – is becoming better understood.[2] Further, data pertaining to entire groups of people – for example, the exact coordinates of displacement camps – may put people at risk. The seizure of such data by hostile actors with the aim of causing harm was the key concern cited by humanitarians interviewed in this study – a risk not without precedent. Risks linked to data 'mosaicking' also increase when one organisation holds huge amounts of data on a particular place, for example, with TPM, in situations where a few firms have a monopoly on TPM contracts.

This range of issues has meant data sharing in humanitarian settings may carry higher risks than in other contexts. The risk can also increase as the number of different organisations holding data increases. Though individual organisations may have stringent data protection policies, the platforms and processes involved in data sharing come with their own potential weaknesses. As explored in the next chapter, organisations have different perspectives as to what constitutes the greatest risks, while also having varying capacities to understand and mitigate these dangers.

Whether TPMs present unique risks as actors within the humanitarian data system is less clear. Staff from both humanitarian organisations and TPM firms stressed their high standards of data protection practices, anonymising of data sets and sharing agreements with their contractors. There is no reason to think of TPMs as having a more or less rigorous approach to how they manage and share data than humanitarian organisations. Determining this requires additional research, given that it is likely that organisations will have different understandings of risks: for example, an organisation closely involved

2 'Mosaicking' is a process of combining non-sensitive datasets to reveal particular groups, potentially to facilitate persecution. For example, transaction data showing when and where cash was withdrawn using debit cards common to refugee assistance schemes could be combined with the locations of places of worship, identifying members of a religious group nearby at common prayer times (Capotosto, 2021). Mosaicking has been described as a 'huge concern' by humanitarian staff working with open-source mapping (Bryant, 2021: 24).

in implementation may better understand context-specific risks, while an organisation specialising in data protection may understand the technical possibilities for protecting data privacy. While there were anecdotal instances of some standards relating to timely deletion of data not being followed, this was the case for both TPM and humanitarian organisations. Further, risks to organisational reputation stemming from poor data practices were as much a key concern of TPMs as they were of humanitarian organisations.

Nonetheless, we did identify some risks linked to TPMs as distinct actors within the humanitarian sector. Specifically, we found the degree of disconnect between those collecting and those using data was high. Enumerators and local TPM staff on the ground were often unsure of how the data they collected was used. On the other side, donors and implementers expressed confidence in the assurances of TPM data reliability, while usually being uncertain of the circumstances in which that data was generated.

We found that TPM presented similar types of risk to other areas of humanitarian activity – both in terms of direct harm to aid users and to reputational/perception risks affecting humanitarian action. However, there emerged specific risks relating to four features of TPM activity: 1) the insertion of remote/distance relationships; 2) the insecure environment that underpins the justification for TPM and data collection; 3) stakeholder coordination and the usefulness of the data; and 4) the introduction of third parties to existing, sometimes fragile, relations of trust. Below, we outline some of the key areas of risk amplified through TPM in connection with these four features.

## 3.1 Increased risk of reidentification of affected people as data is shared

TPM is often used in insecure and volatile contexts where security concerns prevent funders from directly accessing the site of humanitarian activity. Each time data is shared between actors, the possibilities for where and how risks might arise expand: not only does the number of times data is shared increase vulnerabilities, but also each organisation operates with its own data protection procedures that may not align with those of others. As TPMs work with other partners to collect data – often smaller TPMs on the ground, as well as enumerators and implementing agencies – funders and humanitarian organisations can lose some sight of who has access to data and in what form, including beyond the end of a project. Actors stressed attention to data protection, including formalising data sharing and data protection agreements; however, they admitted it was difficult to know different actors' actual practices. One local TPM interviewee stated:

> There could be such thing [as risks of reidentification], but we don't have control over how and what their data will be used for. [local TPM]

## 3.2 Heightened physical risk to TPM data collectors

Consistently, enumerators for TPM in Somalia highlighted physical security as the primary challenge to their work, from physical risks associated with travel to remote locations (for example, by boat), to

collecting data in Al-Shabaab-controlled areas. They work in insecure environments, frequently outside the protection of a large UN agency and/or international non-governmental organisation. Previous HDTI studies have excluded the process of the initial collection of data from studies of data sharing, though noting their indirect relationship (Fast, 2022). We found that excluding data collection from an analysis of TPM data sharing, and data sharing more widely, obscured the scope of risks associated with data sharing. This risks over-emphasising TPM as a way to minimise the risks of operating directly in insecure situations. However, rather than fully remove security risks, TPM transfers the risk to local actors involved in data collection, who then share data with international TPMs and funders. This displacement of security risks resonates with previous studies on TPM, which call for a greater duty of care and insurance in TPM contracts (Harmer and Majid, 2016; Sagmeister and Steets, 2016). While physical security risks are a reality for those collecting data in humanitarian response contexts, TPM as an activity is often explicitly justified by funders on the grounds of unacceptably high security risks that prohibit response organisation staff from monitoring their own programmes. As a result, the risks of TPM – both to data enumerators' physical safety but also in terms of the precarious contractual nature of the work – should be highlighted as a key issue in the process:[3]

> If something happens to you, especially, when operating in Mogadishu, there is no protection and no guiding measures. Roads are sometimes blocked while we are in the field, and different dialects are used in the IDP [internally displaced persons] camps. It is our own problems and we ought to solve. [Enumerator]
>
> If we are working in some of the difficult areas, we must make sure we're working with somebody very local … So we will also need to engage somebody else just for safety and usually agencies who contract you will not take that into consideration. [Head of local TPM]
>
> The morning I was collecting the data in that area, four girls had been physically abused the night before. I could fall into that trap as a girl, no matter if you are an enumerator or a resident girl. … My TPM considers those security challenges and gives us the choice to decline to go far-insecurity zones, but I don't dare decline any field work opportunity because it will indirectly affect my performance and reliability. If other jobs come up, I won't be considered as a potential candidate; they will automatically look for someone who can do it. [Enumerator]

## 3.3 'Silo-ing' and lack of interoperability limits usefulness of the data

Some interviewees involved in TPM and in research suggested that a lack of stakeholder coordination limited the efficacy of TPM. Funders and implementing agencies set up contracts for data collection, including for TPM, for their individual purposes. There was a strong hesitancy to share data beyond each contracted TPM project, partially driven by concerns over personal data and reidentification and

3 In one particular case, Harmer and Majid (2016: 24) cite a testimony in which an interviewed Somali TPM was warned of the danger of a violent reprisal from a non-governmental organisation (NGO) they were surveying, should evidence of that NGO's fraud be made public.

data privacy risks. As a result, agencies collected data in different ways and for various organisations. While privacy concerns are critical to address, at the same time, a lack of interoperability limits the insights that can be achieved through data. It limits the type of questions that can be asked about why and how different situations are unfolding (for example, if combining geographical, household and distributional data). Lack of interoperability and sharing also contribute to duplication of data collection, which potentially places a heavy burden on aid users – who may be called upon repeatedly to provide data.

## 3.4 Heightened tensions between humanitarian actors

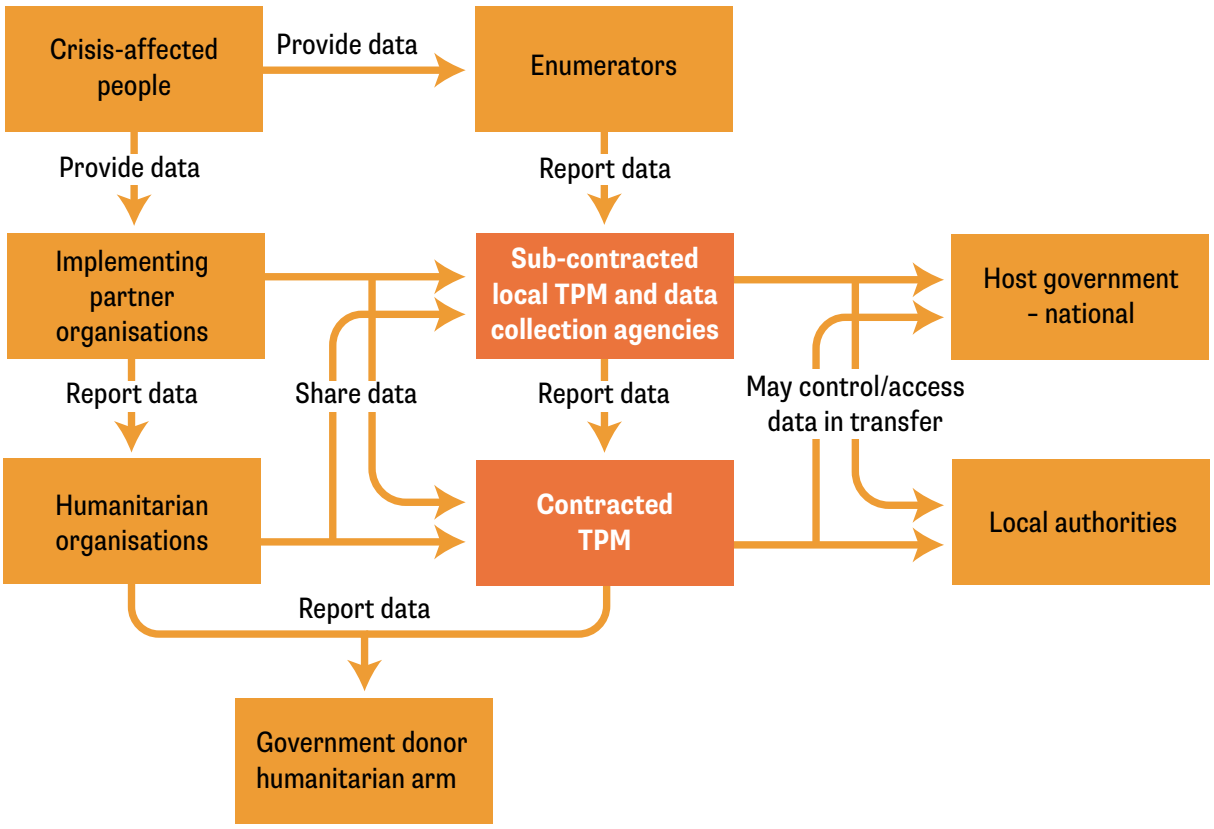
The risks of data sharing to relationships of trust within and around humanitarian activity are already established (Westphal and Meier, 2020; Willitts-King and Spencer, 2020). TPM brings an added dimension of risks to the perceptions of humanitarian activity and actors. First, it can complicate relations of trust between funders and implementing partners. TPM could be perceived to indicate a relative mistrust of funders in implementing partners, versus funder trust in the contracted TPM. Second, varied attention to data protection and its enforcement can suggest variation in levels of trust. For example, we found that funders were not always positioned to nor invested in following up on TPM data protection practices. In contrast, oversight of enumerators did seem to attract more consistent attention. Enumerators were monitored through global positioning service (GPS) devices and photos. TPM opens up questions about the grounds for trust among different stakeholders; if not navigated carefully, this could lead to areas of omission versus overemphasis on data protection, as well as jeopardising trust within some parts of the sector.

Equally, some actors suggested that depending on how TPM was implemented, this could also form a basis for building trust within humanitarian activity. Some funders suggested that TPM could strengthen end users' trust in funders, by giving aid recipients a voice to discuss programme implementation. However, this was debated by some others, who emphasised end-user fatigue and additional data collection harming the relationship with aid recipients.

# 4 The distribution of perceived risks and their mitigation across the data life cycle in Somalia

TPM reveals the diverse group of stakeholders involved in data sharing in the humanitarian sector. This chapter explores the different entities in this data 'life cycle', with a particular focus on how risks are distributed and experienced among these different stakeholders. It begins with aid recipients and then enumerators, as the first actors to be involved in the data life cycle with the collection of data. It then considers the roles of TPMs, both larger TPMs that are often contracted by funders and based outside of Somalia, and local Somali TPMs who are subcontracted by the larger TPMs. Finally, it considers risks for funders of TPM, implementing agencies of humanitarian activity, and local and national governments. This chapter finds that risks are unequally experienced across the data life cycle, with no single actor possessing a sufficient picture of the distribution of risks. More so than with a particular set of data practices of one entity, the extensive and complex ecosystem of actors described here ultimately raises questions around risk mitigation and overarching responsibilities.

**Figure 1** Illustrative diagram of key stakeholders involved in data sharing for third-party monitoring




Source: Adapted from Westphal and Meier, 2020

## 4.1 Aid recipients

People who receive assistance in crises are also valuable sources of data that is used by a variety of humanitarian and other actors. This data includes, but is not limited to, personal and potentially sensitive information. The interests and perspectives of these 'end users' on data sharing – whether specific to TPM or more general – remains a key gap in understanding. The nature of humanitarian contexts makes it difficult for people in need of humanitarian aid to make meaningful choices about how they share information on their circumstances, given their interest to continue to receive that aid.

Stakeholders involved in TPM had different views of the risks facing aid users and how best to mitigate them. The most frequent issue highlighted was a concern over the disconnect between the frequent surveys that crisis-affected people were asked to participate in and any actual material benefit in programming they experienced as a result. This was seen by enumerators as a key source of frustration for affected people, characterised by questions on 'whether the risk is worth it' in engaging with such a process.[4] Though less frequently raised, this sense of fatigue was seen to be compounded by the little, if any, evidence that the outputs of data collection processes were shared with end users. Interviewees identified little direct benefit to crisis-affected people from data collected for TPM:

> People are getting tired of giving data. They need to see changes in their life and the districts. [Enumerator]

One local Somali TPM suggested that interviewing beneficiaries had become increasingly transactional: a sense that giving information through extensive and repeated interviews should be in exchange for some material benefit or compensation. While it was beyond the scope of this paper to interview aid users about their engagement with TPM data sharing, views raised by local TPMs and enumerators interviewed in Somalia suggested this to be an important area for further research.

## 4.2 Enumerators

Enumerators are staff employed by TPM agencies for the purposes of collecting data from end users. On the front lines of data collection, they conduct the interviews and surveys to gather information, including qualitative and quantitative, personal and location data. In addition to data collection, enumerators can also be involved in translation, quality checks, data entry and data cleaning. Data is collected through digital devices and software such as KoBo Collect or Open Data Kit Collect. Often enumerators do not retain access to data after collection – though there are exceptions, for example to cross-check during data analysis. Very few enumerators were aware of what happened to the data they collected, beyond a general sense that it informed reporting, fundraising and decision-making. There were mixed views about whether they wanted to know more.

4 Lough et al. (2022) also highlight frustrations from aid users in the Rohingya refugee camps in Bangladesh over a perceived lack of agency over the decisions made in processes where they were asked to provide data.

Security risks were a primary concern for enumerators. Some believed that it was their individual responsibility to ensure safe practices and compliance with social norms during data collection. For example, in one case, an enumerator decided not to comply with the TPMs' Covid-19 mask requirements in focus groups, given local suspicions of masks. In another case, an enumerator was afraid to report on siphoning of funding for cash transfers by leaders, given the personal security risks of reporting the activity. Enumerators interviewed suggested compensation was not proportionate to the high level of security risks.

Work conditions had a strong influence on how enumerators experienced risk. Their work was often (though not always) short term and based on casual contracts, usually with payment after the task was completed. Casual work can heighten security risks. For example, one female enumerator explained that she lacked an employment identification (ID) card and was left with little formal protection during enumeration work:

> I am not a full-time employee; I have no rights nor protection. I don't have an ID … The terms in the contract are short term and only define the days of work and the pay I will receive. There are no terms that will safeguard me if something happens to me in the field, I get kidnapped, and so on. [Enumerator]

Local TPMs often train and monitor enumerators to minimise risks to data quality and data protection. Typically, this involves mandatory training prior to data collection. Some enumerators appreciated trainings, while others suggested they were insufficient. Challenges raised regarding training included language barriers in the regions in which they worked and lack of technical training to ensure quality data. Additionally, TPMs would ensure oversight by monitoring enumerator activity – for example, through use of photos with GPS readings. Enumerators would also often use TPM-owned phones. Within this context, enumerators tended not to express strong or persistent concerns about the contractors' data security and data protection protocols.

Overall, given the work conditions and security risks, enumerators tended to perceive that their work was underappreciated by those that made use of the data they collected. From a risk perspective, this indicates potential challenges to trust and well-being:

> Enumerators need training and to be treated well. We are the ones risking our lives to dig data, yet we are underpaid. [Enumerator]
>
> Donors and implementing partners do not give credit to those who risk most. We often don't see the product of the data we collected and sometimes, despite our recommendation, the interventions do not get improved. [Enumerator]

## 4.3 Subcontracted local third-party monitors

International TPM firms can subcontract local organisations to assist with data collection, as in the case of Somalia, in situation where they often lack a physical presence. Somali-based TPM firms work directly with enumerators for data collection, and then report to the international consulting firms. The increase of TPM firms in Somalia in response to the growing emphasis on TPM has meant more competition for contracts for local providers.

In general, local TPMs described data collection exercises in Somalia as formalised processes, with little room for informal data collection or discretionary/extended involvement in analysis. Many were not aware of what happened to the data once it was sent to the contracting organisation. In many ways, the relationships between local and internationally-based TPM firms mirror those of local and international humanitarian response organisations. Highly contractual, formal relationships with international firms make it difficult for those local organisations wishing to take a more active role in data ownership and analysis to stay informed, access analysis spaces and decision-making forums, or see where the data they have collected ends up (Wasuge et al., 2021):

> Enumerators are often not very well informed, they may not see the reports, they don't anticipate the discussions they will have, etc. [W]hen we want to see the report, it is often difficult to get that information that you send back. [A]ll of the deadlines that you have to meet and demands from the donor, often people who collect the data are forgotten. [Head of Somali-based TPM firm]

Subcontracted local TPMs indicated that there was top-down pressure from contracting organisations to ensure data protection and privacy protocols were followed. However, there was still inconsistent interpretation of what this meant, including around what constituted 'sensitive data', though those interviewed usually erred on the side of caution. There was also little consideration or awareness of sensitive data outside of personal data.

Requests for data from funders could, however, override concerns to, for example, delete data. The lack of any national legislation on data protection meant that legal requirements came mainly from the contracting organisation. Also, while there was the perception that there were high data protection requirements, in some cases this translated into using non-encrypted channels to share data.

## 4.4 International third-party monitors

Funders tend to form longer-term and more significant TPM contracts with larger, often international TPM organisations, who work with local subcontractors to deliver on data collection responsibilities. Often, these international TPM firms, contracted to carry out multi-year monitoring for funders, form a close working relationship with the funder. The TPM firm provides the funder with a window into the implementation of humanitarian activities at the local level. From the funders' perspective, this gives a greater perceived assurance that they can properly oversee local activities while remote. However, this has also meant accusations of 'donor micro-management' in the past, with a poor TPM report

the first step towards a cut in funding (Integrity, 2015: vi). As a result, some funders suggested that implementing partners viewed the international TPM firm as an extension of the funder. Equally, some funders described TPMs as an extension of their organisation, indicating that, through close working and potentially high levels of trust, the TPM firm was acting in line with their interests.

The contracted TPM firms are at the centre of many data sharing relationships. They often work with multiple actors, including implementation agencies, subcontractors and donors, mediating and coordinating data sharing between them for the purpose of TPM reports. To deliver on their monitoring contracts, international TPM firms must work with implementing agencies and often local subcontractors to collect necessary information. Data shared is often anonymised, but can include personally identifiable information. Although not representative across the board, in one case outside of Somalia the contracted TPM firm formed clear data sharing agreements with each partner involved; here, they took care to inform the funder of the scope of agreements and confirmed when data was deleted. Some TPM firms impose strong technical checks on data collectors specifically. For example, photos and GPS-tracked devices can be used to ensure that enumerators are competing their tasks as instructed.

As TPM firms work with different actors in the humanitarian sector or in monitoring, their presence and activity can raise sensitive issues of trust between implementing agencies and donors – for example, signalling funders' mistrust of implementing partners. Importantly, if they are working through subcontractors, international TPM firms might not be fully aware of the risks on the ground concerning implementing partners and local TPM firms, thereby introducing additional reasons for mistrust and security risks.

## 4.5 Donors and other organisations contracting third-party monitoring firms

Donors and other organisations that contract TPM firms will request data from the organisations they fund primarily for accountability purposes. As such, the data tends to be aggregated and high level, usually losing any personally identifiable information. Demands for disaggregated data from funders remain limited, though there are occurrences.

Despite a broadly positive view of the reliance on TPMs among funder interviewees, distancing between the funder and the task of data collection was identified as an issue. Some funders expressed an interest in having a more direct relationship with TPMs:

> I'm absolutely sold on the need for TPM … Our own ability to generate data is quite limited, so we need agreements, call centre capacity, [and] monitors on the ground. [Donor]

Most commonly, TPM funders identified risks in data sharing related to re-identification of affected people. There were also concerns about the underuse of data, and the need to ensure transparent and trusting relationships with implementation agencies and TPMs for accountability and ongoing effective programme delivery.

Funder requirements drive much of the push for standardisation of data practices and protections throughout the humanitarian data system. Other actors saw funders as holding the greatest degree of power and influence in data requests and practices. Yet funders themselves also emphasised some pushback from their implementing partners on data requests. This was especially prominent in discussions on 'informal' requests for data sharing that lay outside formalised reporting processes. While such requests may be useful for context analysis and learning, they may also be less rigorous in terms of data standards and protections.

Interviewees also noted a greater appetite among funders to use monitoring data for learning and for building a more cohesive picture of crisis contexts. The barriers to collating such information are considerable, since a lack of compatibility between datasets and varying quality make 'real-time dashboards' unrealistic and highly resource intensive. Informal practice networks within funders like the UK's Foreign, Commonwealth and Development Office have also facilitated data sharing, though there is recognition that the use of TPM data for sector-wide learning would necessitate different types of data gathered through more open-ended methodologies.

## 4.6 Implementing agencies

Implementing organisations comprise the largest UN agencies, with global budgets running into the billions of dollars, to local community groups and NGOs at the end of subcontracting chains tasked with delivering small-scale projects. While high-level coordinators were broadly satisfied with collated data about the relative size of a response, funding flows and other insights, implementers were continuously seeking better-quality and more granular data to inform programme implementation and responsive mid-project changes (Lewis and Forster, 2020: 10). It is this motivation that is behind much of the push for publishing and sharing data, though as entities also competing for limited funding, data can be a valuable commodity for these actors.

Implementing agencies have different tolerances for data sharing. This was reflected in relation to TPM. Among the barriers are these perceptions of a form of competitive advantage gained through being the custodians of primary data, but also concerns about possible misuse by third parties, along with limited internal capacities or awareness of shared platforms or protocols where such data could be usefully shared (Lewis and Forster, 2020: 16). While all those interviewed said any data shared would be anonymised, Red Cross national societies were especially averse in principle to data sharing initiatives with the aim of improving implementing organisation coordination. Here, the safety of the affected people they worked with and the movement's adherence to humanitarian principles were cited as key reasons.

In relation to TPM, interviewees from implementing agencies noted their rigorous data protection protocols, including systematic processes for deleting data at the end of monitoring periods. This formality extended to data sharing agreements that humanitarian organisations signed with each other. Frustrations over agency bureaucracy and a refusal to share data with others were also common. This was especially the case when overlaid with existing power inequities between local and international implementing organisations, in which the former were often contracted by the latter without the sense of a reciprocal relationship for data sharing.

The risks to affected people in data breaches and misuse were commonly cited, with this also seen as posing reputational risks to agencies themselves. Reputational risk was also cited as an undesirable possibility of greater data sharing, if more granular data exposed programme shortcomings to funding bodies unfiltered by explanations of context and circumstances. A minority of implementing agency staff cited over-diligence towards data standards as a barrier to data sharing.

## 4.7 National and local government authorities

Previous HDTI-supported research has indicated risks around data sharing can arise through the indirect or informal engagement of the host governments. Our research revealed that host governments at the national and local levels could be critical to effective data sharing for TPM, especially when considering data sharing as part of a broader process that included data collection.

In Somalia, local authorities could play a key role in enabling data collection. One interviewee from a Somali TPM specified that, even though Somalia lacked data protection legislation, several levels of government clearance were still required. Lack of coordination among local authorities could result in delays in data collection, for example when data collection across different locations required clearance from multiple federal member states.

Outside Somalia, too, host governments have been involved in commissioning TPM. Clear communication about the TPM process and nature of reporting can help to mitigate against sharing of raw data with host governments; however, in cases where they are involved in commissioning the studies, similar to other donors, it could be possible for them to request to see raw data. Here, the nature and terms of the initial data sharing and data protection agreements could offer a starting point to minimise sharing of data.

# 5 Thematic and cross-cutting insights

Data sharing for TPM is necessary to improve not only funder accountability, but to better understand community dynamics and the reality of humanitarian delivery. However, data sharing involves new potential risks of harm to end users and to those involved in data collection and analysis, and even to the reputation and continued engagement of implementing agencies. Such complexities suggest the importance of determining how best to collect and share data in ways that minimise risk, and of context-specific analyses into how risks and benefits are distributed. We suggest the following unresolved areas of tension that must be confronted if actors are seeking to engage in TPM data sharing that maximises benefits and minimises risk.

## 5.1 Navigating trust and mistrust

Trust is a significant issue in the humanitarian sector and is often assumed to exist between aid users and providers, as well as between organisations across the sector. Yet a lack of trust has been cited as one of the key reasons for minimal progress on several humanitarian sector reform agendas (including, for example, providing more support and funding to local organisations). It is also, arguably, a factor in why TPM exists as a process and industry. Issues of trust also arise in a particular way in relation to TPM data sharing and invoke a distinct set of risks around how data is shared. Assessing how TPM and data management and sharing impact trust across the sector – and how trust determines how far data sharing can go – presents some contrasts and unresolved points of tension.

Trust is unevenly distributed across the humanitarian data system. Interviews suggested at least a degree of distrust between some key actors and some funders, for example, suspicions that humanitarian agencies and UN agencies had a default incentive to hide evidence of underperformance. Partly in response, TPM has provided an independent means of detecting problems that has avoided more fraught direct allegations or finger-pointing:

> You're going to need an independent fire detection body. The pushback we got from partners initially was explicitly framed in terms of trust – so 'oh you don't trust us' and 'it's not in our MoUs [memoranda of understanding]' … [However] they are now positive because we've moved from 'listen we don't trust you' to this being a service, a way to independently assess performance to detect problems as they arise. [Donor]

For funders of TPM, it was this independence that meant the TPMs they contracted were, in general, highly trusted to give impartial and accurate assessments of programmes. With them even likened to extensions of the funding body itself, the trust in the data shared by TPMs was high, as was trust in their responsible data practices. Although few interviewees were aware of them, it was assumed that TPMs had rigorous data management practices. While TPMs who proactively shared their data practices, and updates on data collection and deletion, also asserted such activities assured funders that risks related to data breaches were being minimised, this was less common. While high trust from

donors in both the data itself and how it was managed was beneficial for good working relationships with TPMs, high-quality management is often assumed – potentially a point of concern in ensuring oversight and good practice.

Trust was less assumed in funder relationships with humanitarian organisations. Here, strong relationships of trust between different stakeholders were attributed to transparent, rigorous and meticulously followed data procedures and communication. Underpinning trust in some cases were large data security checks and referencing processes. But while these formal procedures may have helped build trust, more informal requests for data from funders to implementing partners also played a role, with partners that were commonly called on to fulfil more ad-hoc requests for data also perceived to be more trusted.

From the perspective of humanitarian organisations, any mistrust around TPMs was not concerned with adherence to data responsibility practices, which was considered to be high. Instead, humanitarian organisations commonly felt TPM assessments were not sufficiently informed by contextual knowledge or appreciative of the operational challenges that impact programme delivery. This mistrust translated into a hesitancy to share such data and risks obstructing better data sharing between actors, even when it would be beneficial to common objectives around learning and coordination. A common assertion from interviewees was that data responsibility guidelines were used as a convenient justification by some humanitarian organisations for not sharing non-sensitive data.

This mistrust has implications for a more open, collaborative approach to data sharing. To improve trust, some funders have sought to bring partners into the design stage of the TPM project, so they can understand and buy into the process. Others emphasised transparency and consistency in how TPM results would be used – for example, retaining commitments not to penalise partners for TPM results – helped to build trust between implementing agencies and funders. Some funders included partner feedback and subsequent changes in reports as annexes to help in being transparent about the TPM findings. Investing in the design and negotiation phase of setting up a TPM and involving key stakeholders – including implementing agencies – could help to strengthen stakeholder buy-in and ensure the smooth operation of the TPM activity.

It was also clear that trust did not extend to individual data collectors, as suggested by the rigorous levels of scrutiny and digital tools to monitor whether the data collection process was being carried out to a high standard. There was a strong emphasis among interviewees on oversight of enumerators. Further, there has been attention to – in interviews and in other reports – the potential for enumerators to have both competing interests and biases stemming from their own integration and networks with local communities (Sagmeister and Steets, 2016). Though this assertion was repeated in several funder and implementing partner interviews, it shows that trust is unevenly distributed across the system and often does not extend to enumerators and their initial data collection. The connections that enumerators could have with target communities and individuals, and the trust that would be a part of that relationship, was presented in some interviews as a negative to be minimised, on the grounds it would be detrimental to a perceived objective data gathering process.

## 5.2 The distribution of data responsibility

How is responsibility for mitigating data sharing risk distributed across the humanitarian system? Given that multiple stakeholders are involved throughout the data life cycle (from collection through to deletion of data), each with their own data requirements and a partial view of the data's uses and risks, there was not a single actor that consistently took ownership for ensuring data responsibility throughout the TPM process. The ability to effectively exercise responsibility over data use and sharing practices was limited by the need for stakeholders to operate with some degree of trust in TPM relationships.

During TPM data collection, analysis and reporting, some interviewees suggested that TPMs were responsible for how data was used. In contrast, others emphasised that funders of TPM owned the final TPM product and they, as opposed to TPMs, often had responsibility over the sharing and use of findings. At the same time, data protection was perceived to be just one among a series of interconnected issues facing funders in choosing a TPM organisation. For some funders, the identity of the partners and how they understood the local context were greater determining factors in whether to contract them.

There is no clear line of responsibility for ensuring secure, safe data handling practices in TPM in general. While funders set out the terms of a contract and use of reported data, their lack of presence on the ground can create space for others to take on data responsibility, including TPMs and implementing agencies. Yet this does not mean that other stakeholders are unconcerned with data protection and data security. Almost all respondents suggested that their organisations took data protection and data security seriously and saw themselves as needing to play a key role in managing risks. Where there may be room for improvement is in implementing agencies adopting a more consistent and coordinated set of approaches to processes. This could include their responses to data requests from TPMs, or advocacy, such as pushing for data minimisation and improving data sharing practices. Some funder and implementing agencies have sought to help their partner organisations invest more in enhancing data security. At an organisational level, this could include sharing information on data protection options. At an individual level, this has involved trainings for individual enumerators around secure data collection and handling. In Somalia, each TPM project often had its own mandatory training for enumerators, irrespective of whether they had already undergone training. In some cases, training included responsibilities and roles tied to data protection, consent and the principle of 'do no harm'.

## 5.3 Navigating power dynamics around enforcement

Linked to questions of trust and responsibility over data sharing risks are questions around who can influence data handling practices across the humanitarian data system. TPM requires data sharing across multiple actors: implementing agencies must share beneficiary data with TPMs, while

TPMs share between local partners on the ground in insecure areas and (often remote) project managers and data analysts. TPMs then share again with funders, who are also remote. One local TPM commented:

> The more layers you have at a local to global level, without those set data sharing agreements in place from the very onset that is a challenge. ... Often the process is quite decentralised and you can be unsure who is doing what and who is coming in. ... We have to differentiate between whether we'll be dealing with a large actor who is also our donor, or whether there's a national ministry or range of implementing partners, that can all complicate this process. [Local TPM]

As the commissioning and contracting body, the funder sets the expectations for data handling by contracted TPMs. However, some implementing agencies were hesitant to immediately comply with data requests from TPMs and pushed back on data requests. Their agreement was also with the funder, and not the TPMs, and therefore the terms for sharing with TPMs could be ambiguous. Some funders would facilitate initial interactions between the monitor and the implementing partner, or would provide a request for data on an official letterhead, to indicate how the monitor was working closely with and on behalf of the funder. Formalising TPMs' requests for data from implementing partners has helped to enable data sharing.

Some implementing agencies consistently pushed back on data requests for TPM. Implementing agencies' ability and confidence to push back on data requests can grow with experience, and when they have a better understanding of sensitive data, risk and data analysis. Some have found that, in response to probing data requests, sensitive data did not need to be shared to address the questions that the TPM was seeking to answer. A few implementing partners found there were opportunities to have detailed conversations in response to TPM data requests about data processing, retention and requirements.

However, effective push-back not only requires knowing what questions to ask, it also requires resources: researching and discussing the sensitivities around data in specific political contexts, and negotiating what data is required and how risk can be minimised, is resource intensive. This means that not all implementing agencies are equally equipped to push back on TPM data sharing requests.

## 5.4 Third-party monitoring data sharing for accountability versus for learning

TPM has its origins in monitoring and evaluation, with the principle that a third-party entity can evaluate a programme impartially and so its findings carry greater rigour. The recent shift to using data collected in this way for the purposes of learning between different organisations – for example, to improve programmatic delivery – potentially changes this dynamic. It may, for instance, necessitate more detailed, more qualitative approaches to gathering data and the use of evaluators who are familiar with the context.

This shift also points to a broadening of how value from TPM data might be created, and for whom. Somalia in the early 2010s was among the first contexts where TPM started to grow as an aspect of funder activity, responding to challenges in accountability where funders had little access to implementation activities on the ground. This narrow focus for TPM meant that the data collected and analysed was directed mainly to the funder, with less attention to how it might benefit others involved or implicated, from enumerators to implementing partners. The shift to learning seems to reflect an attitude about 'what more can be done' with data to benefit a wider range of affected/implicated stakeholders.

However, thinking more broadly about the potential uses of data requires considering what questions the data is suited to answer, and how this might help to expand the reach of benefits. As indicated above, there was little awareness of the benefits of TPM data collection and sharing at various points in the data life cycle, specifically among enumerators and end users. In thinking about expanded uses of data, it is important to consider where the data can provide insights from a technical point of view, in combination with other data, and for whom. Could learning help to expand the distribution of benefits? And how do the potential benefits weigh against the potential risks of using data in more diverse ways and for different purposes? Does data need to be altered to be less sensitive before considering wider uses? Additional use cases by different actors likely requires an expanded consideration of risk. For example:

> I get frustrated with the idea that organisations are more worried about how their work will be portrayed rather than how they can learn. [This] relates to trust but also how to find a way to sit down with TPMs and others and ask where we see priorities for action and let's focus on that. So trying to move away from the feeling of evaluation to something they could co-design and actually inform and improve their work. [Third-party monitor]
>
> When you're working with consortia, each partner will have their own internal learning exercises; they'll be a wider exercise and then the TPM will have a separate learning objective. There's actually a risk of learning fatigue … the main gap is the ability to translate learning and that data into actual change in programming especially when you have just a one or two year timeline. There is money invested into learning which is good, but you need to ask whether it was really worth it if there is a lack of follow-through. [Third-party monitor]

## 5.5 Taking a narrow or expanded view of 'digital literacy'

Partial and diverging views on data sharing risk and mitigation efforts indicate scope for greater learning and awareness around when and how data-related risks arise, and how to effectively respond. The locations of data literacy gaps in the humanitarian sector are not necessarily straightforward to identify or address. While there has been attention to training enumerators and local TPMs on data protection and data privacy protocols, there is a wider sense that data literacy – in terms of knowing when and how data quality is sufficient and tailored to addressing specific questions – is less clear.

There can be a willingness and interest to improve data protection processes across stakeholders in the humanitarian data system. However, building the capacity of stakeholders to understand challenges around data collection, sharing and analysis is more complex. While an individual can be taught how to follow a protocol for data protection on a specific application, this does not mean they are trained with the skills to apply the same principles and tools to ensure greater data protection with other software. Data literacy needs to generally improve across the humanitarian sector, from local through to international responders.

## 5.6 Weighing data protection risks against potential benefits of data sharing

There is uncertainty among TPM stakeholders about how to assess data protection risks against potential gains in transparency and accountability through TPM. Technical options to promote accountability and transparency through data sharing, while at the same time maintaining high standards of data protection, are often poorly understood. Frequently, data sharing can be overwhelmed by a concern for data protection and ensuring no harm from that sharing. This seems to stem from uncertainty among humanitarian organisations about the scale and scope of data protection risks and the securities offered by different data protection measures. However, how actors seek to protect data can be counterproductive. As indicated above, concerns for 'do no harm' often involve little direct oversight of the risks and choices presented to end users and those who engage directly with them for data collection. Equally, there is pressure in the humanitarian sector for greater transparency of implementation activity. Yet, transparency 'of what' and 'in what form' are key questions to be addressed alongside opening up data to allow for greater analysis and use.

Thus far, data protection and protection from harm have been key reasons for restricting data sharing in the humanitarian sector, limiting transparency. Once created, the potential ease of replicating data indicates the importance of taking seriously potential risks from the onset. Data protection is likely best carried out through data minimisation. However, this involves making assessments about justifiable risks around data creation and sharing, recognising that once created, data contains the risk of being unintentionally shared, to varying degrees. At the level of data enumerators, data privacy and the potential risks to reputation and future work appear clear. However, the disjuncture in awareness of risks among funders, TPMs and implementing partners can make it difficult for any single actor to make informed decisions to maximise the principle of 'do no harm' around TPM, while promoting transparency and accountability.

# 6 Conclusion

Considering TPM and TPMs as a separate activity and group of actors in the humanitarian system highlights new data sharing relationships, opportunities and risks. In a context like Somalia, the data these firms generate is relied upon for monitoring and evaluation, and they play a pivotal role in creating and managing sensitive data. Yet, despite being private sector actors, the data risks associated with their practices are not unique and reflect those of others working in the humanitarian sector. Focusing on data sharing risks around TPM illuminates wider risks around data sharing in the sector. The same concerns about risks to reputation and the perception of humanitarian activity, and to the well-being of aid users, arise, as well as wider issues around trust, data responsibility, coordination and data minimisation.

By looking at the context for data sharing around TPM, this paper also reveals wider issues around data in the sector that are not always discussed, specifically the risks that are not directly tied to the specific data sharing relationship between the TPM and funder. Risks are often heightened at the point of data collection, a key element of data sharing, with aid users as the first 'data sharers'. At the same time, TPM, given the context and nature of the activity, has its own set of considerations around the benefits of data use, but also the nature of risk. Because TPM is frequently a solution to ensuring accountability in volatile contexts, there are also often heightened issues around trust and security for actors involved on the ground.

Further, as external actors, TPMs often end up working with, and sharing data across, multiple stakeholders, including subcontractors, implementing agencies and aid users. This results in a complex set of data sharing relationships, where it is difficult to obtain full oversight of data protection practices. Effective data practices and responsible sharing are as much reputational issues for TPMs as they are for humanitarian agencies. This means that, despite a lack of common data sharing standards, relatively high standards are maintained. Instead, the primary risks are a result of few individuals or organisations in this long data life cycle having clear oversight of the full extent of risks and purposes of the information they handle.

The risks of data sharing are unevenly distributed. While largely confined to reputational risks for agencies, there can be significant security and personal identification risks for enumerators and aid users. Adopting a broader view of data sharing that looks across the range of stakeholders involved and implicated is therefore important. Often the interests and experiences of local subcontractors, enumerators and aid users are lost within the humanitarian data system. Responsible data practice requires being cognisant of the potential for benefit, harm and influence of diverse stakeholders, and seeking to mitigate inequalities of power present in both the aid sector and smaller TPM industry, which share many dynamics.

This paper has sought to improve clarity around data sharing in independent monitoring in the humanitarian sector, which is often a technical and specialised area of activity. However, by looking across the diverse actors involved in data sharing, and how they relate to one another and to data,

we suggest that TPM is an important area of study, not only in its own right but also for the insights it provides into data sharing in the sector more widely. It affirms the importance, and the complexity, of continuing to push for more consistent responsible data practices in the sector. And, finally, it offers a window into the distribution of risks and benefits of data use in the sector, showing the importance of looking beyond direct data sharing relationships to other related stakeholders and data-related activities, to fully understand the benefits and risks at stake.

## 6.1 Recommendations

In investigating the diversity and distribution of risks around data sharing for TPM and accountability activities in the humanitarian sector, we present several recommendations for the sector, and for funders and TPMs, to better recognise and mitigate potential risks to humanitarian activity and to the well-being of aid users and other stakeholders involved.

### Overall recommendations

**How TPM data is created and held, and by whom (enumerators, local and international TPMs, implementers, funders), should be made more visible to all actors involved in its management.** While attention to data protection is growing, awareness of data handling practices is often fragmented across the different actors involved. Greater collective visibility of data handling practices could help to identify risks and improve awareness of the distribution of roles and responsibilities. A first step likely requires investigating the incentives and structures that contribute to fragmentation.

**Data collection processes should be subject to the same careful considerations of risk as data sharing more broadly.** Seeing 'data sharing' as a process that only happens between groups of funders and humanitarian organisations gives an incomplete understanding of the humanitarian data ecosystem. Many of the potentially harmful dynamics and risks of data sharing begin when it is initially collected. Therefore, efforts to mitigate these risks need to also re-centre affected people as being the first sharers of their own data and under-supported enumerators as being key actors. Both groups need to be better informed as to why data is being collected, while enumerators also require clearer support.

**All organisations involved in data sharing should take greater responsibility for the management of data risks across the range of data handling activities.** This includes looking beyond one's own activities and risks, to better understand how risks are distributed across stakeholders. Especially in insecure environments, security and trust-related risks are concentrated with those at the local level. Management tools like cost–benefit analyses of data sharing, evaluations and policy guidelines should give greater attention to the distribution of risks, and whether the benefits and compensation are sufficient.

## Recommendations for funders

**Organisations contracting TPM should lead in ensuring responsible data handling and take action to minimise risks for all stakeholders involved in the TPM.** Often, given the diverse locations, activities and subcontractors involved, no single actor has oversight of responsible data practices across a TPM programme or project. As those that have initiated TPM activity, organisations who contract TPM hold a unique position to set standards for data responsibility. This could be done, for example, by ensuring that adequate data handling clauses are part of TPM contracts, including a requirement that policies are transferred to all TPM subcontracts At the same time, each participating actor should also act responsibly to uphold the highest standards of data management.

**Funders should be precise and realistic about the potential applications of TPM data.** An increasing desire to use TPM data to support learning (for example, for more efficient programme delivery) must be tempered by a clear assessment of whether the correct data is being collected, whether there is sufficient support in place to minimise risks, and whether learning outcomes can be achieved. In the humanitarian sector, there is an ambitious but not always clearly supported drift towards TPM data sharing for learning. Often learning is discussed in a broad manner, without clarity about how TPM data can be applied to improve programming. In situations where learning outcomes are unclear, data collection and use should be minimised to manage risks.

## Recommendations for third-party monitors

**TPMs should be considered part of the humanitarian system. They should have the same level of responsibility to minimise risks to crisis-affected populations and to manage and share data responsibly, as well as to uphold the same standards.** While TPMs are contracted to provide an independent perspective on humanitarian delivery, their data collection and sharing activities take place alongside and involve the same people and organisations. Considering them as separate actors can obscure the total scale and diversity of data-related risks facing crisis-affected populations and humanitarian actors.

**TPMs should uphold data minimisation.** TPM is often a data-intensive exercise. However, the amount of data collected can be disproportionate to that required to answer questions or to what the funder has capacity to absorb. A commitment to data minimisation can also help to build stronger relations of trust with implementing agencies, from whom data is requested, while minimising security risks for enumerators and aid users in data collection.

# References

**Bryant, J.** (2021) *Digital mapping and inclusion in humanitarian response*. London: ODI (https://odi.org/en/publications/digital-mapping-and-inclusion-in-humanitarian-response/).

**Capotosto, J.** (2021) 'The mosaic effect: the revelation risks of combining humanitarian and social protection data'. ICRC Humanitarian Law and Policy, 9 February (https://blogs.icrc.org/law-and-policy/2021/02/09/mosaic-effect-revelation-risks/).

**Centre for Humanitarian Data** (2022) *The state of open humanitarian data 2022: assessing data availability across humanitarian crises*. The Hague: Centre for Humanitarian Data (https://centre.humdata.org/the-state-of-open-humanitarian-data-2022/).

**European Commission** (2022) 'What is personal data?' Webpage. European Commission (https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en).

**Fast, L.** (2022) *Data sharing between humanitarian organisations and donors: toward understanding and articulating responsible practice*. Oslo: Norwegian Centre for Humanitarian Studies (www.humanitarianstudies.no/resource/data-sharing-between-humanitarian-organisations-and-donors/).

**Harmer, A. and Majid, N.** (2016) *Collective resolution to enhance accountability and transparency in emergencies: Southern Somalia report*. Transparency International (www.humanitarianoutcomes.org/publications/collective-resolution-enhance-accountability-and-transparency-emergencies-southern).

**HRW – Human Rights Watch** (2021) 'UN shared Rohingya data without informed consent. Bangladesh provided Myanmar information that Refugee Agency collected'. HRW blog, 15 June (www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent).

**IASC – Inter-Agency Standing Committee** (2021) 'Data responsibility in humanitarian action: operational guidance'. Operational guidance, February (https://interagencystandingcommittee.org/system/files/2021-02/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action-%20February%202021.pdf).

**ICRC – International Committee of the Red Cross** (2022) 'ICRC cyber attack: sharing our analysis'. Statement, 16 Feburary (www.icrc.org/en/document/icrc-cyber-attack-analysis#:~:text=One%20month%20has%20passed%20since,people%20worldwide%20had%20been%20hacked).

**Integrity** (2015) 'Cross cutting evaluation of DFID's approach to remote management in Somalia and North-East Kenya'. Evaluation report, January (www.oecd.org/derec/unitedkingdom/DFID-Approach-RPM-Somalia-NE-Kenya.pdf).

**Jacobsen, K. and Steinacker, K.** (2021) 'Contingency planning in the digital age: biometric data of Afghans must be reconsidered'. Peace Research Institute Oslo, 26 August (https://blogs.prio.org/2021/08/contingency-planning-in-the-digital-age-biometric-data-of-afghans-must-be-reconsidered/).

**Lewis, H. and Forster, G.** (2020) *Data collection, analysis and use in protracted humanitarian crises*. Publish What You Fund (www.publishwhatyoufund.org/projects/humanitarian-transparency/).

**Lough, O., Spencer, A., Coyle, D. et al.** (2022) *Participation and inclusion in the Rohingya refugee response in Cox's Bazar, Bangladesh: 'We never speak first'*. HPG working paper. London: ODI (https://odi.org/en/publications/participation-and-inclusion-in-the-rohingya-refugee-response-in-coxs-bazar-bangladesh-we-never-speak-first/).

**Metcalfe-Hough, V., Fenton, W., Willetts-King, B. et al.** (2021) *The Grand Bargain at five years: an independent review*. HPG report. London: ODI (https://odi.org/en/publications/the-grand-bargain-at-five-years-an-independent-review/).

**OCHA – United Nations Office for the Coordination of Humanitarian Affairs** (2021) 'Somalia humanitarian response plan 2022' (https://reliefweb.int/report/somalia/somalia-humanitarian-response-plan-2022-december-2021).

**Parker, B.** (2017) 'Security lapses at aid agency leave beneficiary data at risk'. The New Humanitarian, 27 November (www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk).

**Sagmeister, E. and Steets, J. with Derzsi-Horváth, A. and Hennion, C.** (2016) *The use of third-party monitoring in insecure contexts: lessons from Afghanistan, Somalia and Syria*. Resource Paper from the Secure Access in Volatile Environments (SAVE) research programme. Humanitarian Outcomes and GPPi (www.gppi.net/media/SAVE__2016__The_use_of_third-party_monitoring_in_insecure_contexts.pdf).

**UN in Afghanistan Risk Management Unit** (2015) *Third party and collaborative monitoring: findings, opportunities and recommendations*. Kabul: United Nations in Afghanistan (www.alnap.org/system/files/content/resource/files/main/third-party-and-collaborative-monitoring-pv1.pdf).

**Wasuge, M., Musa, A.M. and Hagmann, T.** (2021) 'Who owns data in Somalia? Ending the country's privatised knowledge economy'. Somali Public Agenda, June (https://somalipublicagenda.org/who-owns-data-in-somalia-ending-the-countrys-privatised-knowledge-economy/).

**Westphal, F. and Meier, C.** (2020) *Research on the specific risks or constraints associated with data sharing with donors for reporting purposes in humanitarian operations*. Synthesis Report. Berlin: Global Public Policy Institute (www.gppi.net/media/GPPi_DonorDataSharingRisks_Report_August2021.pdf).

**Willitts-King, B. and Spencer, A.** (2020) 'Responsible data-sharing with donors: accountability, transparency and data protection in principled humanitarian action'. Briefing note. London: ODI (https://odi.org/en/publications/responsible-data-sharing-with-donors-accountability-transparency-and-data-protection-in-principled-humanitarian-action/).

The Humanitarian Policy Group (HPG) is one of the world's leading teams of independent researchers and communications professionals working on humanitarian issues. It is dedicated to improving humanitarian policy and practice through a combination of high-quality analysis, dialogue and debate.

**Humanitarian Policy Group**
ODI
203 Blackfriars Road
London SE1 8NJ
United Kingdom

Tel: +44 (0) 20 7922 0300
Fax: +44 (0) 20 7922 0399
Email: hpgadmin@odi.org
Website: odi.org/hpg