RESPONSIBLE DATAFORUM

# Responsible Data in the Donor Community

*A survey with the funders of human rights and accountability programs on how they address the ethical, privacy and security challenges that accompany data-driven advocacy, and how they support grantees to do the same.*

If you would like to learn more about Responsible Data, visit **https://responsibledata.io**

the engine room

THIS REPORT *is based on a series of interviews with 28 people representing 14 grant-making organizations on how they use data in their work. It presents donors' perspectives on usage, and makes proposals for next steps.*

## Acknowledgements

Thank you to all the interviewees for contributing your time and perspectives to this research. Any errors or omissions are, of course, the authors' responsibility.

# Contents

# Framing the issue

## What is responsible data?

> **Responsible data is**: *The duty to ensure people's rights to consent, privacy, security and ownership around the information processes of collection, analysis, storage, presentation and reuse of data, while respecting the values of transparency and openness.*
> *(Responsible Data Forum, working definition, September 2014)*

At all stages in a project, data needs to be collected, processed, stored, shared and deleted in a way that respects and supports the rights of the people reflected in it.

This includes digital security processes – it is crucial to ensure that data is transmitted and stored securely without exposing others to security risks – but is not limited to them. It means that the people whom the data describe can understand how and why their data is being collected and what will be done with it. Just as importantly, it means that they can have some influence over the process. These issues apply regardless of where the data comes from, whether that is field surveys, internal communications, or big data sources.

> *"[Most work in this field] now involves data collection, whether it is interviews, reporting, surveys or investigation. This is a blind spot."*

Ultimately, this is an ethical question about relationships with stakeholders. For funders, using data responsibly is an essential tool for building and strengthening long-term, reciprocal relationships between funders, support organizations, and advocates. All of these groups have a responsibility to better identify and understand the risks, and to take steps to mitigate them.

## About the engine room

The engine room is an applied research and direct support organization. We partner with advocacy initiatives working in-country and internationally to help them adopt and apply technology to advocacy efforts in ways that are safe, efficient and impactful. We also conduct applied research on the role of technology in advocacy. Reinforcing and promoting responsible data practices are a consistent challenge for both of these activity streams.

The engine room's Responsible Data Program partners with a wide variety of organizations and activist groups to understand current and emerging challenges, develop helpful resources, and convene dialogues towards improving responsible data practice in advocacy.

This research represents a preliminary effort to understand what role the funding community could play to support more responsible data practices among their grantees and, more generally, to contribute to safer and more efficient programming. Subsequent collaboration with the donor community and other international groups have informed analysis of these interviews, which were conducted in 2013 and 2014. Significant developments in awareness and resources that have taken place since the interviews were conducted, and some interviewees emphasised that funders have since begun to build their capacity and have more frequent, open discussions on the subject., Nevertheless, we believe that the issues raised in the interviews could provide a useful starting point for considering donors' roles and responsibilities in managing data and promoting responsible data practices – and suggesting ways to continue improvements.

# Donors and responsible data

Data is an increasingly important part of advocacy work. Intentionally or not, civil society, advocacy groups, activists, and human rights defenders are generating and dealing with a lot of it. This occurs through explicit data collection (such as surveys and mappings); and data automatically generated through record-keeping and everyday communications. Donors also receive, generate and maintain a tremendous amount of data about their grantees and their grantees' constituents. And while data and communication tools can strengthen advocacy work, they can also put communities and activists at risk if not managed carefully, endangering the goals and communities advocates seek to support.

## But what does 'managed carefully' mean?

It means investing the time and resources to think through possible risks and address them as far as possible. For donors, this relates in particular to two facets of their activities–how to handle and manage the data that they collect, and how they promote better practice in the use of data among their grantees.

The donor community has a key role to play in improving responsible data practices among grantees. Donors can have a powerful impact on improving programmatic data handling and helping grantees mitigate risk, in particular through the incentives that accompany grantmaking relationships. We also believe that this potential extends outside of the direct grantmaking relationship, and that donors enjoy a significant capacity to encourage good practice for responsible data usage in general.

Many individuals working within large funding institutions believe that a lot can be done to improve internal standards and procedures for managing data, as well as outward-facing policies for managing responsible data in programming. We hope that this research will help to document common challenges, facilitate dialogue, and ultimately contribute to the promotion of better institutional practice.

## Summary of interviewees, methods, and questions

Between June 20 and August 19, 2013, 28 people representing 14 grant-making organizations participated in informal interviews on the topic of responsible data.[1]

Participants represented donors funding human rights, accountability, governance and other international development work that uses or generates data. We spoke with program officers, program managers, directors, IT specialists and admin staff to better understand how they experience these issues at the project level, in their communications with grantees, and in internal operations.[2] Two of the grant-making organizations were solely 're-granting' organizations; the majority were private foundations. Of all 14 organizations interviewed, only four directly implemented project activities in addition to providing grants. The range of the size of grants provided by interviewees spanned from multi-million dollar, multi-year grants to very small, short-term grants. Interviewees were mostly program officers, but also included program managers, directors, and IT specialists.

Interviewees were asked a series of questions on how responsible data issues were understood and managed in grant-making and project reviews; the handling of grantee and project data; and internal institutional processes and information management.

[1] Nine of those 14 organizations had one interviewee; the other five organizations had between two and four interviewees each. Three of these interviews had two or more staff members present and answering questions. Interviews were conducted in person as well as via phone and VoIP.

[2] Interviewees comprised: 16 program officers, five program managers, two program directors, one admin specialist and three IT specialists.

# How do funders currently approach responsible data issues?

All interviewees agreed that funders have a duty to use data safely, and almost all thought that they had an explicit responsibility to support their grantees to do the same.[3]

However, most preferred to talk about organizational security policies and response methods, and paid significantly less attention to issues around agency and informed consent. As one interviewee put it, there is a "need to frame the issue not as technology-focused, but as data-collection-practice focused."

Despite this, interviewees only rarely addressed the full range of concerns around data use, including protecting people that grantees collect data about, respecting their agency in the way that data is used and ensuring that consent is fully informed.

Interviewees gave a variety of reasons for this, including:

- a reluctance to interfere in grantees' organizational affairs
- a belief that grantees are better placed to deal with problems themselves because of their greater local knowledge
- internal organizational dynamics.

[3] A small number of interviewees argued that the threats from poor digital security were not sufficiently severe to warrant action, citing a lack of examples of cases where organizations or individuals had experienced significant harm. The Responsible Data Program's Reflection Stories initiative (**https://responsibledata.io/new-project-responsible-data-reflection-stories/**) aims to address this by collecting real-life examples of threats and discussing potential mitigation strategies.

**Most funders acknowledged that poor information security practices, in which data gets into the 'wrong' hands, could lead to real harm for grantees.** Nine of the 14 organizations interviewed cited real-life examples in which projects had been affected in this way, with notable examples including:

- *A list of trainees was confiscated from a grantee based in a high-risk country while they were traveling, putting the trainees and the staff member at risk.*
- *A Western advocacy grantee deemed very low-risk was hacked by another Western advocacy group, and their emails and internal documents were used to discredit them and their campaign(s).*
- *Grantees were subject to surveillance by a government's authorities, and the communications data collected was used in legal trials against them.*

## What do funders know about the issues?

**Funders' own knowledge is limited:** Funders acknowledged that they were grappling to understand and respond to the various issues related to responsible data across a disparate range of funded program areas and geographical locations. Many said that internal conversations on the topic were extremely limited and spearheaded by a smaller subset of their organization, who were often described as those working in high-risk geographic locations worldwide, or on human rights or technology. Two organizations reported no internal discussion on the issue at all, with one interviewee admitting that it was "the first time in 12-13 years…that I've looked at privacy."

Because requests to address responsible data issues were not being made across the majority of program areas, **most interviewees appeared unconvinced that these issues were sufficiently relevant for a organization-wide response**. They also appeared hesitant to promote this approach given the human and financial costs it would entail.

## What do funders know about how their grantees manage data?

**Funders usually knew relatively little about how grantees respond to these issues**: The majority of interviewees did not appear to have discussed responsible data issues directly with their grantees. Perhaps as a result, many funders said that they did not know how their grantees understood particular issues or whether they had the capacity to deal with them.

> *"I think the [reason for the] lack of detail is that donors just don't know."*

**What funders do know often worries them**: Of those interviewees who expressed an opinion, most were concerned about their grantees' approaches to data usage. Some cited cases where real harms had occurred, and suggested that they served as an "early warning" for how the digital world is now affecting all programs that collect, use, and share data associated with people. In particular, there were frequent assertions that grantees paid insufficient attention to security and privacy, and failed to treat them as priority issues.

> *"People either aren't aware or don't care."*

Interviewees were typically unsure why this was the case. They suggested reasons ranging from grantees' overall lack of capacity to deal with problems in their environment, limited knowledge of technology, and a lack of interest in privacy among more technically adept organizations. There was also an active belief among grantees that these issues were not important.

> *"Even those who are more tech-savvy are still not thinking about users, or privacy or security"*

Where donors were better informed about their grantees' capabilities, it was usually the grantees who had taken the initiative to tell them.

Some organizations mentioned specific examples of occasions where a grantee had informed them about a risk that later needed action. One subgranter had particular concerns over donor reporting that involved submitting lists with individuals' names.

> *"[Grantees] worry about it. When it goes to the donor they have no control over keeping the info safe."*

Finally, interviewees focused almost exclusively on the implications for grantee organizations themselves. Almost none extended their concern to include the data subjects – people who often enjoy even less control over their data, and who can face even greater threats if the data is misused.

# How responsible are funders' own data practices?

Funders described vastly differing tools, systems, and policies to deal with data – with details even varying between interviewees in the same organization. Again, these practices were almost exclusively related to digital security issues.

Even when those issues were well understood, the mitigation practices funders cited were weak – reports of internal data and information security policies were rare and varied in scope. Even when strong policies did exist, interviewees pointed out that they were not necessarily being followed.

Notably, even organizations that reported sharing data internally in secure ways did not extend the same levels of security to communications with their grantees (or others outside their organization).

### Varying organizational security protocols: some examples

*Five organizations described some level of secure communication, including encrypted email, encrypted file sharing, and virtual private networks (VPNs). A few other systems were described as being secure, though it was unclear what made them so (examples included "web-based grant management," "a protected website for grantees," and "robust design for security.")*

*One organization did not send sensitive documents via email for particular programs; another had an established physical safety policy but was still developing an internal information and communications policy, while two others had recently conducted internal penetration tests (one in the wake of a nebulously described attack by a nation-state actor). One of these two organizations did not appear to have basic secure systems, tools, or policies in place.*

It was often unclear from the interviews whether staff could access secure tools and systems if they were needed in certain contexts. Several interviewees complained that centrally managed IT systems within organizations – in which staff typically lack administrative privileges – prevent them from installing trustworthy, effective privacy and security software.

# How are funders helping grantees address responsible data challenges?

## Making grantees aware of risks

Many interviewees reported that project officers were the primary, and often the only individuals tasked with monitoring responsible data issues linked to projects.

Interviewees regularly praised local or region-focused staff for their ability to raise red flag issues, and for using their knowledge of the local context. However, it was unclear whether these individuals (many of whom focused on a thematic area like transparency or corruption) would be able to flag problems in areas they were unfamiliar with (whether this regarded an unknown type of technology, approach, or vulnerable community). This puts the onus for identifying risks on to the grantee or the people they are trying to support.

> *"We really need organizations to come to us and tell us what their needs are."*

This can be effective when grantees are able to identify most serious problems related to data use, which does not always require technological knowledge. One interviewee found that the people best at assessing risks often had low levels of technological knowledge, but a strong intuitive sense of whether the data could put people at risk, and how this could affect the project overall.

## Supporting grantees experiencing a specific problem

Around half of the funders interviewed said that they would provide support to grantees experiencing a particular problem (such as linking them with an information security organization). However, of those, a significant proportion said that this support would only be provided if the funding organization had a strong commitment to the grantee. The grantmakers interviewed described reaching out to their networks to help them identify and address issues.[4] Few gave specific examples of cases when this support had been provided.

**None of the interviewees said that they were providing regular, substantive training on responsible data issues for their grantees**, though a few cited isolated examples where digital security sessions had been organized in regions considered to be at higher risk. One interviewee stated that their organization often had overly optimistic expectations of what digital security training sessions could achieve. They warned against expectations that these trainings could change grantees' entrenched behaviors, or that ad hoc training efforts could lead to substantial investments in digital security by grantees.

> *"Embedding trainers with extensive and integrated training over at least a year might work better."*

There was little evidence of processes to deal with problematic data usage by grantees. Those measures that were taken were often more reactive than proactive, with resources only invested retrospectively, when there was evidence of a problem.

[4] (Please note that since this issue varies from person to person both within and among organizations, we looked at these responses on an individual instead of organizational basis.)

# What are the challenges for donors trying to engage with responsible data issues?

## Organizational culture change

Interviewees frequently either struggled to communicate within their organizations about why responsible data concerns mattered, or were themselves unclear and unsure about how relevant these concerns were.

> *"The risks are perceived as largely theoretical. We have heard about things from other countries, but there have not been any major issues for our operations."*

Some interviewees had concrete suggestions about how to articulate arguments for pushing responsible data usage up organizations' priority list. One suggested framing the issue as "what can we do with grantees to make things better," noting that project officers in their organization would be unlikely to be interested in a session that was presented as being about "data protection".

Others highlighted the need to counter a prevailing sense of apathy or fatalism by focusing on existing practical ways of tackling problems. Several interviewees also said that that they would like to be sharing more information:

> *"There are few resources to tell donors what to do. Guidance from [other donors] would be helpful."*

## Adapting assistance to the local context

Interviewees suggested that it was difficult to adapt measures for ensuring responsible data use to local circumstances. This also seemed to be linked to the fact that grantmakers often have longstanding personal relationships with grantees, in which case introducing new requirements (or even ideas) can be difficult.

One interviewee who has worked on building responsible data capacities for both funders and grantees observed that local improvements were usually short-lived until "something went wrong again." This echoed an observation by another interviewee that the expectations of what was possible or probable after a training were often over-hyped, and that funders should not expect grantees to change entrenched behaviors or start making substantial investments in digital security after short-lived training sessions. Interviewees also regularly expressed concerns about the availability of accurate, unbiased advice.

## Organizational obstacles

Monitoring and addressing responsible data issues involves investing resources in building institutional knowledge or training, but for the most part funders painted a picture in which responsible data was rarely prioritized.

**Limited internal appetite for training**: Among the 14 organizations who mentioned training, only two had held trainings touching on digital security. The first had held two in the past five years, and the second held them annually with all staff participating. Several said that improving practices was difficult because of the lack of internal incentives (financial and otherwise) to allocate the additional resources that were needed. In still other cases, training was limited to a few specific departments but not spread across the organization as a whole.

> *"I don't see a lot of [donors] investing holistically in technology education for their program officers, or bringing technologists in as equal partners in to discuss program strategy."*

**Limited time and resources**: Significantly, several funders also mentioned that they were already overstretched, with responsible data issues only one of a series of concerns where they felt they lacked knowledge. (This may contribute to the apparently frequent practice of involving external consultants on a case-by-case basis.) Another mentioned institutional reluctance to commit financial resources to more responsible data practices, summarizing the prevailing attitude as: "It has gone fine thus far – we don't need more expenses".

**Lack of communication with other funders**: there were few reports of organizations sharing knowledge or experiences with one another, while several people explicitly mentioned this lack of discussion as a problem. Some interviewees mentioned that this was the first time that they had discussions on these themes explicitly.

## Lack of systems, procedures and familiarity

**Data collection and management practices are typically left to an individual's discretion**: The interviews suggest that funders are putting a remarkable amount of trust in their program officers to understand, identify, and address any and all responsible data issues and concerns. Many were described as having total freedom to cultivate their preferred set of experts and advisers on issues including digital and operational security, big data and privacy.

This level of autonomy is understandable given the variability of grants, grantees, and the various issues and actors involved in the grantmaking process. Program officers (especially at private foundations) have often worked on an issue or region for at least ten years before working as a funder. This equips them to anticipate projects' political, contextual, procedural and substantive challenges. However, limited familiarity with digital media and data can lead to blind spots when considering how a project's data use could affect people's rights in a particular context.

Interviewees confirmed that their staff's familiarity with technology varied significantly, and that this made it difficult for some to stay up-to-date on emerging technologies and data-related issues.

When asked whether they had the skills to identify and address responsible data issues, the majority of interviewees did not answer "yes" with any degree of certainty, with most citing a strong dependence on informal contacts or consultants. Several funders also cited frustration with the advice they received from these sources, complaining that it did not lead to actionable recommendations that they could integrate into their workflows.

# Findings

Funders have a crucial role to play in promoting data usage practices that respect and protect their grantees, as well as the rights of the communities they aim to help. This report argues that they have an opportunity to play this role more actively, for the following reasons:

**Funders cannot avoid influencing grantees' priorities.** Many grantees, largely dependent on project-based funding, have clear incentives to design projects and activities in ways that they think align with funders' expectations. Without explicit recognition from funders that treating data responsibly is important – and help for grantees in understanding which responsible data issues are likely to affect them – many grantees may find it difficult to justify proactively improving their data usage practices.

> *"Grantees are stretched so thin, they don't have a chance to think about it. It doesn't become a priority; this can be part of the donors' role."*

**Funders collect and process information from their grantees** for reporting, putting an onus for responsible data management on the funders. Sometimes it is also helpful for funders to release data publicly, but doing so can raise the risks to the grantees and their constituents, particularly around issues of agency and security. Not all grantees may be able to identify risks involving funders' actions, know how to mitigate them, or have the expertise to de-identify data appropriately. They may also feel uncomfortable expressing concerns about funders' use of their data because of the power imbalances in the funder-grantee relationship.

> *"Grantees just never want to tell you what you're doing wrong."*

**Funders also need to be aware of issues around consent and agency.** Collecting data also creates a power imbalance: whoever collected the data now holds a commodity that relates intimately to an individual. This means that those collecting data have an even greater responsibility to treat this data with care, especially in areas where a community may be vulnerable or excluded from society.

> *"[Some organizations use data because they think it will help them] reach out to communities more easily, without actually realizing that they are collecting data sets linked to individuals."*

**Funders that actively demonstrate that they are willing to discuss responsible data issues – and work with grantees to overcome them – can significantly improve the effectiveness of their programming.** Some grantees may be aware that they cannot recognize or address threats to the security of integrity of their data, but be unwilling to disclose this to a funder for fear of damaging their relationship. As a result, difficulties may well be hidden from funders, when they could have been mitigated if tackled earlier.

> *"I usually only know about something going wrong when it is at a full-fledged crisis."*

**Funders that signal their willingness to talk openly about these issues may hear a much wider sample of the problems that grantees actually experience.** When asked about issues experienced by grantees, interviewees typically referenced data security breaches that posed a severe, immediate threat to a grantee. Important though these are, they do not take into account equally important questions about other facets of data use – particularly how a grantee's practices around data can affect the communities that they seek to help.

> *"Unless it's a long relationship, [we're] not told about something going off course unless it's a train wreck, unless they are highlighting how they avoided it. I often have a hard time getting info and organizations aren't forthcoming."*

**Much of the data collected by grantees is gathered with funders' priorities in mind**, whether to demonstrate the impact of a project or highlighting their organization's effectiveness. This means that funders have a space to discuss what data actually needs to be collected – and what could be left out.

> *"[Most grantees are not thinking about privacy and consent] in a systematic way. There is a real bias towards looking to the positive side."*

**By helping grantees to manage their own data successfully, funders can improve their own reputation as a champion of responsible data norms.** Although interviewees said that organizations' leaders, ranging from presidents and directors to board members and trustees, were very concerned about "not causing harm" and their organization's reputation, they also described an absence of concrete measures to deal with these threats.

> *"International human rights funders are losing plausible deniability that grantees are safe when executing grants in environments that are increasingly surveilled and hostile to civil society."*

# Funders' needs and suggestions for meeting them

Several interviewees suggested resources they would like to see made available or which they would themselves use during the grantmaking and communications process. Some of these would require action on the part of respondents' institutions or those institutions' peers. Others could be produced by experts or coalitions working on these issues. Respondents pointed out that some more practical resources have already been created and shared in the International Human Rights Funders Group (IHRFG) community, but it is unclear to what extent they have been used.

## From their own institutions

**In-house training**: Several respondents noted that the limited opportunities they had had to develop capacities in these areas were at conferences and events, but that "in-house" trainings catering to their specific needs would be more useful.

> *Trainings on digital security, evaluating responsible data risks in proposals and responsible data publishing practices for funders could help to strengthen the skills and confidence of individual program officers, while also supporting a culture of responsibility within funding institutions.*

**Experts on retainer**: Reliance on an expert consultant was a consistent theme in interviews, and several participants mentioned how such interactions would be more efficient and impactful if institutionalized.

> *Establishing retainer-style relationships with experts in digital security, data ethics or participatory methods could help program officers to quickly and efficiently address responsible data challenges large and small, and consistent support from known experts would likely have a positive impact on capacity development for program officers as well.*

**Internal audits**: Many respondents noted concern about responsible data practices within their organization, suggesting that the lack of policy and familiarity with the issues is likely to have led to widely variant and often irresponsible data management.

> *Internal audits of security practices can be a good way to identify risks and weak spots in responsible data practice, while also establishing a foundation for better internal discussions and capacity for addressing responsible data practices.*

## From their peers

**Shared experiences**: Interviews revealed a broad interest in how peers are addressing responsible data issues.

> *Shared experiences in trusted fora, either in written or presentation form, ideally after grants have ended, would likely help to familiarize a broad base of funders with responsible data issues, while increasing potential for collaboration across institutions.*

**Structured collaboration**: Though interaction in the IHRFG was consistently cited as the sole space where discussion and collaboration on responsible data issues takes place, there was also significant interest in more structure, and additional fora.

> *Structured collaboration between grantmakers on responsible data issues – either through the development of resources, training, joint risk assessments, or events and seminars on specific issues – can provide concrete support to program officers and increase the chances that program officers recognize challenges before things go wrong.*

**Access to peer resources**: Several respondents noted that they had heard that peers actively used specific resources for addressing responsible data challenges, but that these were not accessible.

> *Making tools, checklists and risk assessments available to peers would be allow funders to position themselves as leaders in developing norms for responsible data, while also helping to validate and improve such resources, and providing much-desired support to other funders.*

## Tools for the job

**An overview of resources**: Respondents recognized that there are likely to be a significant number of tools and resources that they don't know about. They consistently emphasized how useful it would be to have an overview that would direct them to relevant resources for specific challenges.

> *An overview would be a dynamic reference document organizing resources for dealing with digital security and privacy issues, as well as ethical questions about consent, representation and agency, and strategic issues such as data re-use and accessibility, all organized according to the situations and workflows faced by a grants manager or program officer in funder organizations.*

**A checklist for decision points**: Respondents emphasised the utility of a quick reference sheet to help identify opportunities for more responsible data practice.

> *A short, one-to-two page reference document could highlight common points in the grant-making and grant management process where program officers can take concrete steps towards responsible data management, with notes on some of the common challenges and questions at each stage.*

**Detailed 'dos and dont's'**: Respondents who had previously faced significant responsible data challenges stressed how challenging they were, and how useful detailed guidance could be.

> *In-depth resources could focus on the trade-offs and challenges of key strategies. For example, they could include helping grantees think about privacy issues among their beneficiaries, or assessing the risk involved in publishing information about grants.*

**Easy introductions**: Respondents repeatedly noted how complicated some responsible data issues are, and how useful highly accessible, introductory materials would be – both for them, and for colleagues less familiar with the issues.

> *Introductory materials could be packaged as documents or animated videos, providing staff with basic introductions to issues such as digital security, data privacy, consent and representation in a donor context – and providing a basis for further exploration on an individual basis.*

# Conclusion

If you're unsure how to use data responsibly in your programming, you're not alone. In the course of these interviews, we found that many funders were thinking about similar issues, and facing similar problems. There have been many changes since the interviews were conducted: new threats have emerged, awareness of some issues has increased, and more resources have been developed to address existing gaps. Still, we believe that many of the opportunities and constraints described by the interviewees persist to this day. We hope that discussing them openly in this report will serve as a starting point for conversations and spark the development of more useful practical resources.

Funders are in a position to improve the way in which they and their grantees collect and manage data. Using data responsibly can help funders develop and strengthen long-term relationships between with their grantees, based on respecting the rights of the people that they aim to support. This report outlines some things that can be done to help achieve this.

RESPONSIBLE

DATAFORUM