Sharing data responsibly

—

A CONVERSATION GUIDE FOR FUNDERS

October 2018

With contributions from

THE ENGINE ROOM
Accelerating Social Change

ARIADNE
European Funders for Social Change and Human Rights

360 GIVING

Supported by

Stanford PACS
Center on Philanthropy and Civil Society
—
Digital Civil Society Lab

This guide is based on research conducted by The Engine Room and Ariadne, with contributions from 360Giving, between March-October 2018. The project was supported by Digital Impact (part of the Digital Civil Society Lab at Stanford University).

Project lead: Tom Walker
Content: Fieke Jansen and Paola Verhaert
Editing, review and additional content: Julie Broome, Katherine Duerden, Lori Klos and Rachel Rank.
Report design: Jonas Voigt

With thanks to the staff within funding organisations who generously contributed their time and expertise to this research and the production of this guide.

Ariadne and The Engine Room request due acknowledgement and quotes from this publication to be referenced as: Sharing Data Responsibly: A Conversation Guide for Human Rights Funders, October 2018. This report is available at *https://theengineroom.org* and *http://www.ariadne-network.eu/*.

Introduction

Human rights funders collect a lot of data about their grantees - as well as the people that their grantees help.

Sharing this data openly can help funders be transparent about their activities and highlight the impact of their grantees' work. However, it can also increase risks to human rights work if data isn't collected and managed responsibly.

How can funders be transparent about the work they support, while making sure that they aren't harming grantees or others?

What is a conversation guide?

We believe funders need to start with clear, open conversations with grantees and other funders about how they collect and share data. This guide, based on inputs from more than 40 human rights funders, aims to help funders have these conversations.

It lists common questions that grantees and funders might ask, combined with advice and resources to help answer them.

There is no one-size-fits-all solution to managing grants data responsibly: contexts and grantmaking systems vary dramatically and change constantly. Instead, this guide aims to give practical advice that helps funders strengthen their relationships with grantees - thereby leading to more effective grantmaking.

Who is this for?

Funders or grantmakers worldwide who want to treat data about their grantees responsibly, but don't always know where to start. It's also useful for funders who want to improve their data management practices and are looking for resources to help.

What will you find in the conversation guide?

There are no shortcuts to handling data responsibly, and this guide won't give you any. Instead, it offers prompts that are designed to help you talk more openly to grantees or other funders about data-related risks and ways of dealing with them. The guide is organised around three elements of the grantmaking lifecycle: data **collection**, data **storage**, and data **sharing**.

→ *Collecting*: how to start a conversation about what data is being collected from grant applications, monitoring and reporting.

→ *Storing*: how to talk to grantees, peer funders or donors that fund other funders about how data will be managed once it's collected.

→ *Sharing*: how to discuss sharing information about grants, including publishing data, and any new risks this might create.

This guide is not intended to provide guidance specifically related to the EU's General Data Protection Regulation (GDPR), which was implemented in May 2018. However, if you are looking for guidance on the GDPR, the resources under the 'Data Storage' chapter will set you on the right path.

What is a responsible data approach?

Responsible data is the collective duty to account for the unintended consequences of working with data. Here, it means taking a step back to think about how you're using and managing data from or about grantees, in a way that takes into account power dynamics, security concerns and the context of the grantee.

Why sharing data responsibly matters

02

For funders, sharing data about the grants you make can help you be more transparent, highlight ways of using resources more effectively, and highlight important work by the organisations you support. The Advancing Human Rights Initiative and GrantNav are just two examples of the advantages of sharing some grants data openly.

However, if data on grants and grantees is not collected and managed carefully, it can also endanger human rights work. How?

Data on grants can put individuals at risk. In 2016, the Swedish human rights defender Peter Dahlin was arrested and interrogated in China. Chinese state security officers reportedly had access to a document prepared by a US-based foundation that described the activities of his organisation in detail, including names of employees and information on grants. Dahlin was later deported.

Data that appears innocuous when first published can become dangerous when political contexts change. Once this data is publishing, it's hard to delete it. For example, as one foundation noted, 2010 data on grants to LGBT organizations in Uganda had the power to endanger lives when the Ugandan government passed laws against 'aggravated homosexuality'.

Governments and hackers are using technology to target human rights defenders and the organisations that support them. For example, hackers leaked confidential documents on the Open Society Foundations' strategies and funding requests to the public in 2016, while governments are increasingly seeking to digitally surveil and target members of civil society, with attempts to target Mexican journalists and UAE human rights defenders using malware just some of those documented in recent years.

Even with strong digital security practices, just collecting data can increase risks because of human error: one simple mistake could mean that sensitive information about a grantee or beneficiary is shared more widely than it should be. In 2011, one foundation mistakenly published internal descriptions of grants instead of versions prepared for public audiences, provoking criticism from a blogger that the descriptions were "ambiguous and inflammatory."

During our research, we heard frequent references to other, smaller incidents. All funders we spoke to believed that that we should take every opportunity to minimise these risks. But how?

Assessing the risks

Have a discussion with staff and board members on circumstances when you wouldn't disclose a grant. People may have different ideas on how to find the right balance. To help you consider all the risks that might affect a grant, review the following questions:

- → What do you know about the authorities' surveillance capabilities where the grant is being implemented? Are they suspected to have used data to target civil society groups?
- → Is the grantee or topic of the grant controversial: do any people or groups oppose it?
- → Has the organisation been under physical or digital surveillance by state or independent actors?
- → Has the organisation or its staff been placed being placed under any government restrictions, such as a travel ban?
- → Has the staff/board/office/IT systems been under attack, physically or otherwise, by state or private actors? How have the threats been dealt with?
- → Have any staff or board members been arrested?
- → Has the organisation faced administrative harassment (tax audits, restrictions or authorisations required to access bank accounts or individual funds as they are received?)
- → Have there been any detrimental stories in the media about the organisation?
- → Are the beneficiaries of the grant a community at risk?
- → Do you know of any incidents where data was used to target similar organisations? If yes, who was behind it, or who might have been?

Then think about how the answers to your questions relate to these risks:

! Risks to the project's beneficiaries

Ask yourself what could happen to a project's beneficiaries if project data is published publicly, or if a group with malicious intentions gains access to it. For example, if a project is on a sensitive topic such as LGBTQI rights, and data about the location of project activities is published, could people attending those activities be targeted?

! Risks to the project

Consider how the project could be affected if data about the project or its activities is published publicly. For example, could beneficiaries be targeted or logistical arrangements become more difficult if details of the project activities become publicly available?

! Risk to the grantee and its staff

How might publishing data increase risks to the grantee organisation itself? For example, could a government impose restrictions on a grantee if the fact that they are receiving funding from your organisation becomes public? Could staff face security threats?

! Risk to the funder

Think about whether publishing data on the activities you fund could make it harder for you to continue your work. For example, do some of the projects you fund rely on cooperation from the authorities, while others are focused on issues that the government in Country X does not support?

Finally, think about any red lines in the way that you manage data.

Would you ever pull out of a project because a grantee, partner or back donor (a funder that provides you with funding) was mishandling or misusing data? What are the minimum standards you would need them to adhere to? Setting out these red lines in advance will help you make decisions later on in the process.

Tips for a good conversation

03

Define your core values for how you collect and manage data by thinking about how you balance these principles:

- → **Autonomy:** respect grantees' ability to decide how data about them (or data they collect) is used.
- → **Transparency:** use data to make funders more accountable to grantees and the public, and better allocate resources.
- → **Open communication:** balance between autonomy, security, privacy and transparency.

Deciding which principles resonate most strongly with your organisation's mission will help you work out what to prioritise in conversations with grantees and funders. This will help you to go beyond organisational processes and ticking checkboxes, and means you will need to regularly reflect on and improve your own practices. You will also need to balance this with your organisation's commitment to grantees' and beneficiaries' privacy and security: maintaining strong organisational security processes takes time and resources.

During the conversation, be open about your constraints as a funding organisation. Organisational culture, commitments to transparency, compliance, and allocation of resources will limit what you can commit to. However, by communicating about these limitations clearly, grantees will be able to make a more informed decision about what data they decide to share - thereby helping to improve the overall relationship.

Collecting data

04

As a funder, you will collect data about grantees during the grant application process, and during monitoring and reporting. This section helps you think through what to consider.

Before the conversation

Start by looking at your own practices. Check what data you **have** to collect, such as information for tax authorities or details for other funders. Make sure you understand how long you need to keep it, and any other conditions.

THINGS TO CONSIDER

Think about

- **Any personal and organisational data that you will need to create a grant agreement.**
- **Financial details like bank account numbers, and salaries in the budgets.**
- **Any data that you will need to collect about activities and the grant's beneficiaries for reporting purposes or to make grant award decisions.**
- **Requirements from regulatory bodies to disclose a certain percentage of grants that you make.**

RESOURCES

- See Digital Impact's template data management plan for some of the categories that might be included here.
- The Digital Security & Grantcraft guide has a useful guide to assessing risks to grantees: https://www.fordfoundation.org/library/reports-and-studies/digital-security-grantcraft-guide/

Before the conversation

Check if your organisation has a process for asking grantees if they consent to having their data collected, stored and (if appropriate) shared. If not, consider introducing one, ideally in a way that allows you to document grantees' responses in your grant management system.

If you will need to share data with another funder or back-donor after you have collected it, review how they manage data first. See **Sharing data**, below. Think about which parts of your grants portfolio could see grantees put at risk if data about them was shared.

THINGS TO CONSIDER

Some funders allow grantees to check a box stating that they would like the name and content of their project to be kept confidential. This is usually accompanied by a policy on the process for handling sensitive grants, that states who approves changes to a grantee's status, and what actions must be taken once this has been done. Other funders use grant agreements stipulating that all data must be shared unless grantees can demonstrate reasons for exemption: if you choose this route, be aware that grantees may not always have a full overview of risks that they face. Review the Risks section, above, to help you identify questions to ask.

RESOURCES

- It can be useful to conduct a threat modelling exercise:see the Electronic Frontier Foundation's introduction to threat modeling, Integrated Security's written exercise to assessing threats, as well as guidance on holistic security context and threat analysis.
- Funders have been discussing these issues for some time: see this summary of the PEAK Grantmaking conference, for example: https://www.hrfn.org/community-voices/are-you-over-or-under-protecting-your-grants-data/.
- For more on how civil society can strengthen their digital security, what and who is out there to support them, read The Engine Room's 2018 report.
- For guidance on consent processes, check the Responsible Data handbook.

How can you ask for consent?

Think about how consent fits into your grant-making processes. Do you tell grantees how data from proposals they send you will be stored? Can they consent to (or opt out of) sharing some types of data with you?

Ask yourself if a grantee could feel they have to agree to your data-sharing approach in order to receive funds. Be clear with grantees about non-negotiable requirements, but for non-essential data, explain that decisions should be guided by their security considerations.

Try to agree data management practices with the grantee before they commit to the project. This will give them a clear sense of what they are committing to. If this isn't possible, allow time and space during reporting and monitoring stages to discuss any new data collection.

CONVERSATION TIPS

In your initial call for proposals, include a section that clearly explains what data you will need to collect and what you will use it for. Use the rest of this guide to help you write that section. Make sure that grantees have an opportunity to state their reasons for asking that their data be treated differently to your standard policies.

To make managing consent easier, consider incorporating the consent statements into your grantmaking processes.

RESOURCES

↳ For more information on consent, see the Responsible Data Handbook chapter on Getting Data or 360Giving's guidance on what to consider when publishing grant data and comply with the UK Data Protection Act.

What questions might a grantee ask me?

"Do we have to share all of this data with you? Can we leave some out?"

CONVERSATION TIPS

Remember to consider what data you actually do need. Can you explain why you need it? For example, does it help you to make funding decisions in future, or help you support grantees better? If you can't give a strong and legitimate reason, do you definitely need to collect it? Think about why the grantee might be asking you the question: is there a worry they're not telling you about? Take this as an opportunity to think about potential threats they might need to consider in their context.

You may disagree with a grantee's assessment of risks and threats - they might not be aware of all the risks they face, or be overly cautious. There is no simple way of dealing with this, but it can help to talk to grantees about what threats they face, which threats are a priority, and what information adversaries might need to harm them. Breaking down threats into smaller pieces can help to identify ways of mitigating them.

RESOURCES

↳ For more information on the data minimisation approach, see the ELAN tipsheet on data minimisation.

"We are happy for you to collect the name of the project and a summary of its activities, but will you need to collect our names or the names of the people with whom we work?"

CONVERSATION TIPS

Think about whether you will you be collecting personal data about the grantee's staff or the grantee's beneficiaries. Think more broadly than the legal requirements - are there other elements in the data that could allow a person to be identified?

For example, if there are only two organisations working with a particular marginalised group in a country, simply adding background information about the location of work could allow someone to be identified.

RESOURCES

↳ Check 360Giving's guidance for useful tips and resources on legal aspects around data protection.

"Could you share more information about us? We want to raise our profile!"

CONVERSATION TIPS

Depending on the risks that the grantee is facing, there could be several responses to this:

1. If you think publishing more information about the grant will not substantially increase risks (see threats section, above), work together with the grantee to consider ways that you can publish information in a helpful way.

2. The grantee is currently at risk, but increasing their public profile may raise awareness of their existence and thus help to protect them. Here, it is worth talking with them about the best way to publish information so that it can be most useful to them.

3. You believe that publishing the information will increase risks to the grantee. Explain that you're concerned about risks to them because of how data might be used once it's published. For example, you might be sharing data with another funder that has different practices for storing data, or need to publish data openly so that more can see it. Ask them about any other threats they have experienced in the last couple of years, or anyone who might oppose the project and want to target them.

RESOURCES

↳ The Indigo Trust publish all their grants both on their blog and in an open data format (through 360Giving). In the past, they withheld information about a grant that concerned anti-corruption activists in a developing country where transparency could have jeopardised their lives. They handled this by publishing the fact that a grant of 'x' amount had been made, while noting that detail wasn't being published for security reasons.

Storing data

05

This part of the conversation focuses on how to discuss how you will store data and manage access to it.

Before the conversation

Reviewing your requirements
This section walks you through some of the questions you might be asked about the storing and management of the data you collect.

Check if your foundation has any organisation-wide protocols on storing (sensitive) information. If it does, review them and check that they meet your organisation's needs.

What to prepare
Consider the following four elements of data storing before your conversation.

THINGS TO CONSIDER

Check if your foundation has any organisation-wide protocols on storing (sensitive) information. If your foundation operates from or in the European Union, it is likely that there is a protocol in place to help the foundation comply with the General Data Protection Regulation (GDPR). The GDPR was implemented in May 2018, and was designed to give control over personal data back to citizens and residents, and to create a uniform data protection law across member countries.

If your organisation has an organisation-wide protocol on storing (sensitive) information, review them and check that they meet your organisation's needs.

1. Where is the data stored?

Think about who has ultimate ownership of the data: do you keep copies of all data on your local computer, is all information centralised in one platform or is it scattered across both? How does your data storage practice influence who owns data? Where is the digital data stored and where are you keeping hard copies of your data? If you or your organisation are unsure, consider running a data mapping exercise.

THINGS TO CONSIDER

When thinking about the location of your data, think about which country it is stored in and what implications this has for potentially sensitive data.

RESOURCES

Additional resources that might help you think about data storing challenges you are facing:

- The Engine Room's blog post on preparing for the GDPR, including a 101 document sheet and a data audit template, as well as the Holistic Security Manual's chapter on Information at rest.
- DataKind's 'GDPR I'll Show You Mine If You Show Me Yours'.

2. What kind of data are we storing?

Once you can locate your data, you'll be able to review what kind of data you are storing. Depending on your and your organisation's needs, you might want to think about revising:

- If you really need the level of detail of data you are storing.
- If you want to anonymise or de-identify a chunk of the data you store.

THINGS TO CONSIDER

- **If you want to move particularly sensitive data to a secure storage space. Check out the Responsible Data Handbook for more guidance on separate storage for sensitive data.**

RESOURCES

- See the Holistic Security guide's section on Understanding and cataloguing information for more.

3. Who has access to the data?

THINGS TO CONSIDER

Don't forget about your emails. Have dedicated moments in your year where you revisit information that is in your inbox to decide what information should be stored with the rest of the grantee data, what can be deleted and what should remain in your inbox.

RESOURCES

↳ The Responsible Data Handbook, particularly the chapter on managing data. This chapter also includes information on assessing risks and best practices for access permissions.

4. How long is data being stored for?

Ask yourself who has access to the data and check if your organisation has a practice around setting viewing/editing/adding permissions.

Find out what happens when there is no longer use for any type of data. Is it being deleted? If so, by whom? If not, why not? Is your organisation's data deletion practice influenced by any legal or fiscal requirements?

THINGS TO CONSIDER

A general security principle is to limit user access to the minimum amount of data that they need to be able to do their work - and only give them access for as long as they need it. For example, in one case, a project involved sensitive human rights work, but two of the donors involved insisted on collecting a huge amount of data on operations, including names of people involved and receipts for all activities. Within three months of the project, however, both of those donors discovered inside threats. In each case, some of their employees had become disgruntled with their working conditions and subsequently left the organisations, taking with them a large amount of data – not only on one project, but all the NGOs and individuals the donor had been working with and/or had funded.

What might you want to discuss with a grantee?

Who can access or view data about my organisation or grant?

CONVERSATION TIPS

There are several ways to approach this question, depending on the nature of the question. The grantee might be curious about where data they shared with their program officer in confidence goes, who else has access to it and who takes this decision. Keep in mind that this question might also be about data sharing, in which case, the section below on data sharing will guide you. Depending on the grantee's context, they might be anxious about surveillance risks, particularly if your organisation is using third-party tools. Consider this possibility when talking to them about their concerns.

RESOURCES

- The Human Rights Funders Network's security plan for their *Advancing Human Rights* project explains to funders who will have access to data that is submitted: http://humanrightsfunding.org/wp-content/uploads/sites/20/2017/10/Security-plan_Update.pdf

Where is data about my organisation or grant stored?

CONVERSATION TIPS

Give an overview of systems that hold data on the grantee. If possible, try to highlight where you are storing data on local systems or where you are using storage provided by a third party tool, like a cloud-based storing tool. Consider that non-digital data is also data, and include mentions of physical hard copies in your overview.

Explain the different security measures your organizations takes to keep the data safe.

Keep in mind during this conversation that not all grantees share the same threat model, and that they will have different concerns depending on context or timing.

Do you keep sensitive data about my organisation or grant?

CONVERSATION TIPS

The answer to this question should be tailored to the grantee's definition of 'sensitive data.' One grantee might be unconcerned with the idea of a donor storing address details, while another might find this a source of worry. Try to use this conversation to establish a mutual understanding of what the grantee considers to be sensitive data.

RESOURCES

- Responsible Data basic de-identification solution matrix and the Responsible Data Handbook's section on anonymising data.
- If you are not sure about the level of sensitivity of certain types of data, conduct some risk assessment exercises, possibly together with your grantee. Check out the UN Global Pulse's Privacy Assessment Tool and Girl Effect's GEM risk assessment sheet.

How long do you keep my data?

CONVERSATION TIPS

Secondly, be honest with your grantee about legal and fiscal restrictions that you might be operating under; if you need to keep certain details about your grantee on file for tax purposes, legal reasons or otherwise, communicate upfront about this.

RESOURCES

- For information on RAD policies, look at the ELAN tipsheet on retention, archival and disposal.
- If you're curious to learn more about what goes into deleting data, check out the UK National Archives data disposal checklist.

Can you delete my data?
In what circumstances will you delete my data?

CONVERSATION TIPS

If you are an EU-based organisation or collect data on EU citizens, you may already have created privacy notices outlining how you process personal data. Consider drawing on these to help you answer the next set of questions.

Be open and clear with your grantee about your practices, as well as legal or fiscal requirements to retain data, and ask them about their preferences for retention of non-essential data.
In some cases, organisations will have a data deletion or a retention, archiving and deletion (RAD) policy in place. However, most organisations hadn't considered deleting or archiving data on a systematic basis prior to the implementation of the GDPR.

It's important to be clear about what you can and can't delete. As mentioned above, some organisations will need to keep certain data for fiscal or legal reasons.
The other side of this coin is about what technically goes into data deletion.

The process of data deletion consists of:

- **Taking/assigning responsibilities**
- **Locating data**
- **Systematically scrubbing data**

Communicate with your grantee about the process and provide them with a clear timeline for when you will have been able to delete the data. Keep in mind that if your organisation processes data in the EU or collects data on EU citizens, under the GDPR individuals have the right to ask you to delete their data (the right to erasure), in which case, you will have to respond to their request within one month.

We are subgranting through you because we would like to remain anonymous in country X.

How you store our data, contact details and contract information?

CONVERSATION TIPS

Walk them through how you are storing data, what your constraints are, and how you store personal data (see sections above for guidance). Let them know that you are open to talk about their concerns periodically.

What questions might a back donor or their representative ask me?

How do you store information securely to prevent risks to us or your grantee?

CONVERSATION TIPS

Besides giving an overview of your data storage practices, tools and (potential) policy, highlight that Programme Officers can collaboratively detect sensitive data with the grantee, using this conversation guide. If applicable, you can mention specific data storing practices for particularly sensitive grants.

What might I want to raise with a back donor?

If the back donor is responsible for finances and contracting, you will need to share data with them in order for the programme to operate. However, it can be a good idea to ask about how long they will retain that data, and when and how they will delete it.

CONVERSATION TIPS

Talk to your back donor about exceptions for particularly sensitive grants and how this might affect the way you report about these grants. Additionally, you can proactively present them with an overview of your data storing practices if and whenever these change. Depending on your relation with them, ask the back donor about their practices.

Data sharing

06

This section focuses on conversations you might have around sharing data publicly or with peer funders.

Before the conversation

Reviewing your knowledge
Remember that, once data is shared publicly, it may be possible for others to access it indefinitely. Even after data is removed from your website or the sites of groups like the Foundation Center, it may still be accessible through web-based archives. Think back to your assessment of risks and consider whether anything has changed in the countries where your grantees are working (see **Collecting data**, above).

THINGS TO CONSIDER

What are your organisation's policies on sharing data publicly? Do you publish it on your website as an online database or spreadsheet? Do you publish grant data according to open data standards such as IATI or 360Giving?

If you issue public calls for applications, do you state how data will be published?

RESOURCES, TIPS AND EXAMPLES

↳ Remember that data published at an earlier date can still cause harm in the present. For example, as a former director of Ariadne pointed out, "data published in 2010 on grants to LGBT organizations in Uganda had the power to endanger lives when the Ugandan government [later] passed laws against 'aggravated homosexuality'."

What might you want to discuss with a grantee?

If you have already agreed how you will collect data with a grantee, talk about how you will tell them when data-sharing will happen in advance, and any opportunities to input into the process. Develop a system for documenting how data has been shared, and whom it will be shared with (see **Collecting data** section, above).

For example, the Oak Foundation states that before grant descriptions are published publicly, they are reviewed and approved by the partner themselves. In 2011, the foundation shared that it had mistakenly published descriptions of grants that staff used internally in their grants database, provoking criticism online.

If you are sharing data about a grant for the first time and haven't discussed it with the grantee yet, allow more time to talk about the process and give them time to decide whether they need more information.

Think about any new risks that sharing data with others or publishing it (such as a case study on your website) could create. Who might be able to see it or share it, and could they link that information with any other sources to find out more about the grantee, its staff or its beneficiaries?

EXAMPLES & RESOURCES

↳ For example: When the Indigo Trust decided not to publish details of a grant to anti-corruption activists because doing so could have affected their security, they reviewed the situations later and found that it had changed. According to them, "with the permission of the grantee we published the full information, and were encouraged to blog about the project by the grantee." See the Indigo Trust's blog for more information about the process.

Sharing data with other funders

Bear in mind that back donors (funders that give funding to other funders) may be less aware of risks than you. By talking to them about the data management systems they use and their approach to using data, you may be able to identify knowledge gaps and establish areas where you can both learn and improve.

RESOURCES

- The Responsible Data handbook discusses risks to consider when publishing data to open standards such as IATI.
- Mimi Onuoha wrote about the challenges of deleting data in FiveThirtyEight.

THINGS TO CONSIDER

Think about how much you know about the back donor. How do they manage information? How well do they know the political and security context in the area where you work? Are there areas where your knowledge of a particular context could be useful to them? If possible, ask them to share details of their policies with you.

What kind of relationship do you have with the back donor? Is it formal or more informal? If the relationship is formal, try to discuss these questions and agree on common standards before signing a contract or memorandum of understanding.
If the relationship is more informal, try discussing it on a call or (ideally) in person, and come to a common understanding that you can document in writing.

What phase of the project are you in currently? Are you still in the contracting or inception phase, or are you already implementing it? The earlier you can start this conversation, the better.

What might you need to discuss with another funder or back donor?

Common questions that other funders may ask you:

- → Could you share details of the programs you are supporting? This could include details on who you are funding, where, for how much, for which activities, and who the beneficiaries are.
- → Please send us data that we need for reporting. This could include what activities have taken place, who was involved, and who were the beneficiaries, and might involve information such as attendance sheets, pictures and other forms of documentation.
- → We understand that you are supporting Grantee X and are thinking about of funding them for a different programme - could you give us some more information about them?
- → We are travelling to Country X/ writing an analysis of the context in Country X. We know that you have a programme in that country: could you give us any contacts in your network or in the programme?

EXAMPLES & RESOURCES

- ↳ DataKind UK has two template non-disclosure agreements.
- ↳ One UK-based funder said that they do not share information with other funders, apart from anonymised data included in public reports on insights from their work. They don't share anything in writing with other funders, but do talk to them over the phone to give a verbal opinion on work that grantees are doing, or give positive references. If a funder asks them for more detail, or to share more information, the funder checks with the funded organisation before they share anything.

HOW TO APPROACH THESE QUESTIONS

Talk directly to the back donor about any concerns you have, explaining any potential risks to the grantee that you can think of.

Share only the required data, rather than entire data sets. Likely, this will mean creating different, redacted versions of data sets for different uses and partners.

Explain the different security measures your organizations takes to keep the data safe.

Use the assessment of risks you conducted earlier to help. Ask them if there is the potential to exclude data in certain cases, and explain how other funders deal with the same questions.

If the back donor is responsible for finances and contracting, you will need to share data with them in order for the programme to operate. However, you can mitigate the worst risks by being very clear to your grantees about your limited ability to manage risks yourself, and by talking openly with the back donor about the risks using the information in this guide.

RESOURCES, TIPS AND EXAMPLES

↳ Finally, consider how partners need to access the data. Do they need to edit it or simply view it? Depending on the software or technical method used to share the data, you may be able to set access permissions to control data use.

If you are publishing data that contains information about people, how will you de-identify it?

HOW TO APPROACH THESE QUESTIONS

If you are only providing reporting information to a back donor, start a conversation about their data management practices.

- **1. Ask them to talk about what data is essential, and which data is less important. At this point, you can explain how you have assessed the risks in this context, and what the concerns are.**
- **2. Discuss whether data can be de-identified or pseudonymised and still meet their needs. Ask if it is possible to only share top-level data.**
- **3. Discuss sharing grant descriptions or other data while imagining that members of the public might view it - and consider how this would change the information.**
- **4. When sharing data, indicate to the back donor which data is sensitive and why. If the back donor is a governmental donor, this will be useful for them when they get a freedom of information request**

RESOURCES, TIPS AND EXAMPLES

- For challenges in de-identifying data, read this guidance from the Me And My Shadow project. For guidance on de-identifying data, read the UK Anonymisation Network's resources, the ICO's guide to anonymisation, the chapter on anonymising data in the Responsible Data Handbook, and summaries and recordings of a discussion mini-series on the Responsible Data Forum.

How will you release data publicly?

HOW TO APPROACH THESE QUESTIONS

Things to consider when de-identifying data:

- **What people or groups may have an interest in trying to re-identify your data? (Intelligence agencies, hackers, curious data scientists, local groups that oppose the issue that the grantee works on.**
- **What other data sets are available that may result in re-identifying the data you are publishing?**

What is your release strategy for your data? (For example, how is it being released to media? Is it possible that they may accidentally/ deliberately add identifiable data?)

What technical and version control methods are you going to use? (For example, to ensure you release the correct anonymised version of your data)

Afterwards
review + repeat

07

When you or your organisation introduce new data storing policies, systems or a new programme officer, contact your grantee to discuss any consequences for them. Does this alter the risks that affect the project?

Build in regular check-ins about data storing practices with your grantee. These check-ins will allow you to gauge any changes in their context soon after they have occurred. Talk to your grantee about how they monitor the risks and what information they share about themselves.

October 2018

With contributions from

THE ENGINE ROOM
Accelerating Social Change

ARIADNE
European Funders for Social Change and Human Rights

360 GIVING

Supported by

Stanford PACS
Center on Philanthropy and Civil Society

Digital Civil Society Lab