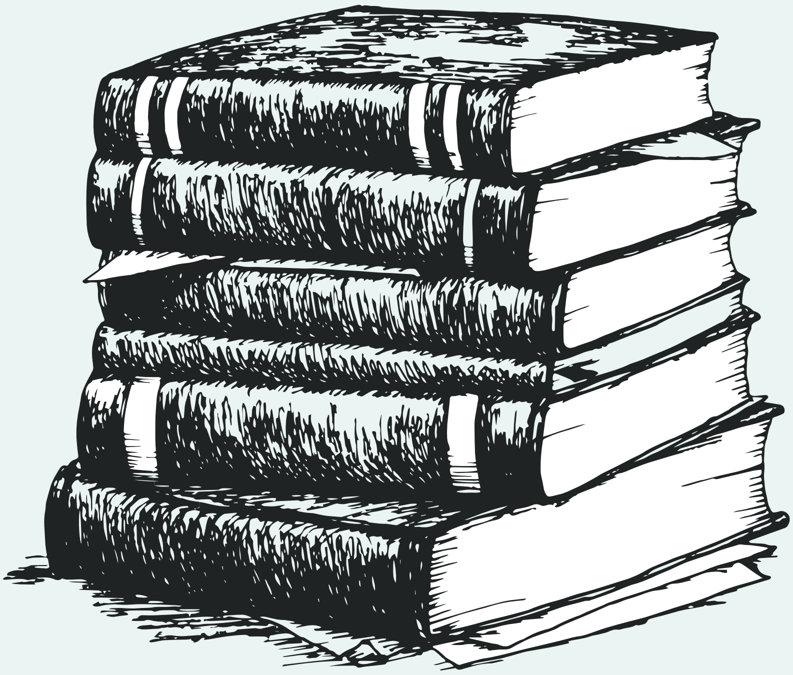
RESPONSIBLE DATA FORUM

The HAND-BOOK OF THE MODERN DEVELOPMENT SPECIALIST

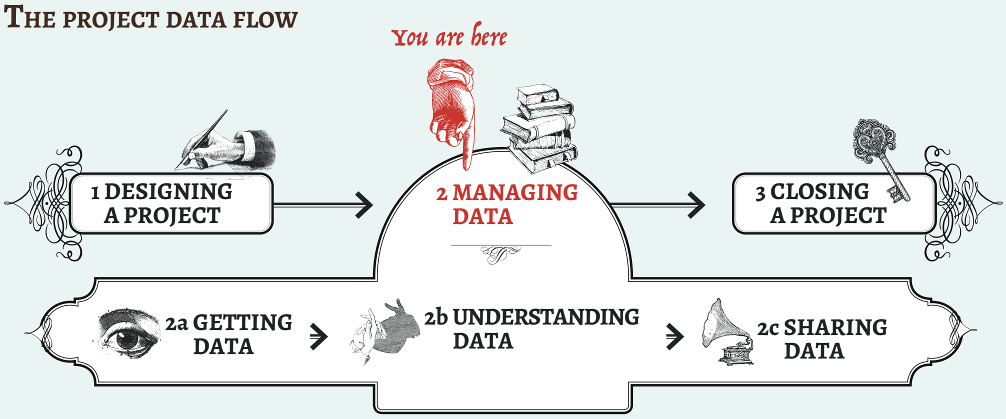
2

MANAGING DATA

SETTING UP THE ‘DATA INFRASTRUCTURE’



The project data flow



Target audience

Those who are making decisions, or advising others, on how to go about managing data; from the very basics of deciding where and how to store it, to who has access to it, how it is managed on an ongoing basis, and broad legal considerations to bear in mind.

When might this chapter be useful?

In advance of actually collecting any data, the chapter contains information that might be useful to consider when setting up the 'data infrastructure'.

Content summary

This section provides an overview of approaches you can implement to ensure your information is stored, managed and accessed in a responsible, secure and protected manner. To begin with, it's worth reviewing the general principles of data integrity, and thinking about how to manage risks surrounding data storage.

### A home for healthy data

All data occupies physical space, even if we don't think of it as such.

There are lots of decisions and processes that go into creating, storing and sharing data. Some of these are discussed under the section 'data integrity', which looks at the validity, authenticity and security of data. As a frame of analysis to understand what the given data is, and isn't, it can be very useful. Some main considerations to bear in mind when interrogating the *integrity of your data* are included here.

Other risks and harms associated specifically with *data storage*, along with appropriate mitigation strategies, are then discussed. Then, extra considerations to take into account when dealing with *sensitive data* are briefly mentioned.

The pros and cons of various responsible data storage options are then discussed, such as storing data locally, in the cloud, or within a network. Another oft-overlooked aspect of data storage, *physical data storage* is then explored in more detail.Threats to your data don't only happen online. To plan for a possible physical break into your office or headquarters, a checklist is provided of things to consider in advance.

For your eyes only looks at who has access to the data. Essentially, making sure that access to sensitive information happens on a "need-to-know" basis can reduce the risk of someone getting access to data they shouldn't. This can happen online, through setting appropriate user permissions for a certain person's role, or physically, in terms of only letting trusted or vetted individuals into an office space. Regular audits that check who has access and revisiting user permissions can help make sure these access levels remain up to date.

Many of us work often on *collaborative projects*, which require different parties having access to the data. Another checklist to consider when setting up access permissions and data infrastructure on collaborative projects is included here, like including *layered access*, or embedding secure practices into the various access points.

Despite all this, it is important not to over do the checks and security measures in place; when it comes down to it, the project and the data need to be accessible in times of need, and potentially on a longer-term basis. Some concrete steps for making sure that the data will be available for the right people at the right time and planning for disruption or technical emergencies, are then included.

In the final section within this chapter, *Legal considerations* are discussed. Given the general nature of the book, much of this is discussed on a very broad level, to provide the reader with a guide of where to look and what to look for when thinking about the legal aspects of data storage. Whether it's data protection laws, encryption technology laws, or jurisdictional issues, (or more!) this section may well be especially relevant to the non-lawyers among us who are looking for a broad overview of what they should have in mind.

Useful resources

The Frontline SMS Users' Guide to Data Integrity
http://www.frontlinesms.com/wp-content/uploads/2011/08/frontlinesms_userguide.pdf

Deflect https://deflect.ca/

Cloudflare https://www.cloudflare.com

For a listing of secure tools, see https://www.prismbreak.org

On choosing a hosting provider,
see https://learn.equalit.ie/wiki/Responsible_Data_Forum_on_Hosting

On setting up a secure hosting provider,
see https://learn.equalit.ie/wiki/Secure_hosting_guide

NGO Law Monitor - http://www.icnl.org/research/monitor/

Maps of Data Protection Laws
http://www.forrestertools.com/heatmap/
& http://www.dlapiperdataprotection.com/#handbook/world-map-section

Choosing an Open Source Licence for Code
http://choosealicense.comCreative Commons - https://creativecommons.org

This publication is part of a series found at https://responsibledata.io, produced by the engine room Responsible Data Program, 2016.