USING THE DATA LIFECYCLE TO MANAGE DATA RESPONSIBLY

OXFAM

WHAT IS RESPONSIBLE DATA MANAGEMENT?

This leaflet will help anyone handling, sharing or accessing programme data to properly consider responsible data issues throughout the **data lifecycle**.

It focuses mainly on the responsible management of data in humanitarian crises, from the perspective of data collection. However, the principles, tools and approaches are also more widely applicable.

Responsible data management is about treating the data that we collect with respect, and upholding the rights of respondents – people whose data we collect. 'Data' includes: survey responses, registration information, photos, stories, etc.

Managing data responsibly need not be restrictive. Instead, it can strengthen and facilitate the contribution that data makes to high-quality work. It should be seen as a framework for ensuring that data collectors are responsive, uphold accountability and raise voices.

The regulatory framework (laws and other standards) for data management is rapidly changing, and so are technologies for collecting and managing data. So responsible data management is a constantly evolving process about deciding when and how to collect data, and how to manage risks.

1 MAKE A PLAN

Clearly **define the purpose** of collecting the data.

The benefits you expect from the data should be proportional to the risks. You should be guided by the interests and wellbeing of the affected population.

Evaluate the methods and tools available to find those most appropriate to the context and your purpose.

Minimize the questions you ask, and rigorously check if you really need to ask them. Check that the information has not been collected already from a trusted source.

Do you need to do a data protection/**privacy impact assessment**?

Personal data is highly sensitive and needs additional safeguarding, such as storing separately from respondents' answers, or taking measures to **anonymize** data.

Plan from the start how you will ensure genuinely **informed consent**. Make clear what consent means, and inform communities about the purpose of the data you collect.

Check for risk of bias in your targeting and methodology. How will you check the accuracy of your data?

2 DO A RISK ASSESSMENT

Collecting data can put people at risk.
Assess risks and take action to avoid negative consequences for respondents, e.g. by ensuring data security and confidentiality.

Use technical experts to understand specific risks, and think through what you will do if a problem or **data breach** occurs.

3 TRAIN ENUMERATORS

When training data collectors:

- Cover responsible data considerations.
- Cover the consent process. What should respondents know about what is going to happen to their data?
- Use real-life scenarios to bring training on systems and protocols to life.

4 GET INFORMED CONSENT

Consent is not just a box-ticking exercise – it's about treating respondents with dignity and respect as well as upholding legal requirements on personal data.

Tell respondents how you will use their data and why you need it. How will you store it? Who will you share it with? How will you ensure these groups don't share it further? What if respondents change their mind about consent? How can they contact you?

Ask respondents if/how they want feedback on what you do with their information.

Give respondents a chance to opt out, and devise a 'plan B' in case they do.

5 MANAGE THE DATA

TRANSFER

Take care when using portable devices and sharing technology. **Encrypt** where appropriate and set up systems that allow phones to be remotely wiped of data.

For paper-based processes, take extra care when moving hard copies in the field. Encrypt digital files at the point of data input.

ACCESS

For access rights to digital data sources, set up individual accounts with user passwords. Prioritize who needs to access what.

Each person who collects or uses data is accountable for responsible data management. One approach is to give one team member responsibility for data protection, and ensure everyone else understands their roles and accountability.

STORE

Carefully research the data security and location of cloud storage and database options.

For paper-based collection, reflect on safe storage options. If possible, store in a safe or locked cupboard.

SHARE

Set up a **data-sharing agreement** with organizations that you share the data with, including data-handling guidance. Seek legal advice if necessary.

These principles apply no matter who the third party is: a government, another NGO, a private company, a bank, etc.

Don't share data without getting consent from respondents.

Some organizations 'open' (i.e. publish) data. Seek specialist advice and check for risks and sensitivities before opening any **data set**. Simply removing names is not enough to hide identities.

6 USE DATA TO DO SOMETHING

This might be lobbying, advocacy, or making adjustments to programmes.

Think about who is being represented in the data. Have you considered the gender balance?

Is there any bias in the decision made, based on the data?

7 OWNERSHIP AND FEEDBACK

How can you promote ownership by respondents?

Meet respondents to validate results and ensure they represent their views where possible. Give them feedback on what happened with their data.

8 RETAIN/DISPOSE

Always plan for how long you need to keep data – remember, data loses relevance very quickly.

Deleting a digital document isn't the same as burning or shredding a physical one, because digital records can often be left on your computer. (E.g. download folders, archives, etc. This is known as data afterlife.)

JARGON BUSTER

Anonymization In theory, this means making it difficult or impossible to identify an individual from a data set. In reality, pieces of data can often be reassembled to reveal identities.

Data breach The release of information, which may or may not be intentional, to an untrusted environment.

Data lifecycle The flow of information through a system, from creation and storage to deletion.

Data set A collection of related data.

Data-sharing agreement A framework for the sharing of data which sets out how data will be transmitted, stored and used.

Encrypt Convert data into a format that cannot be easily understood by unauthorized people.

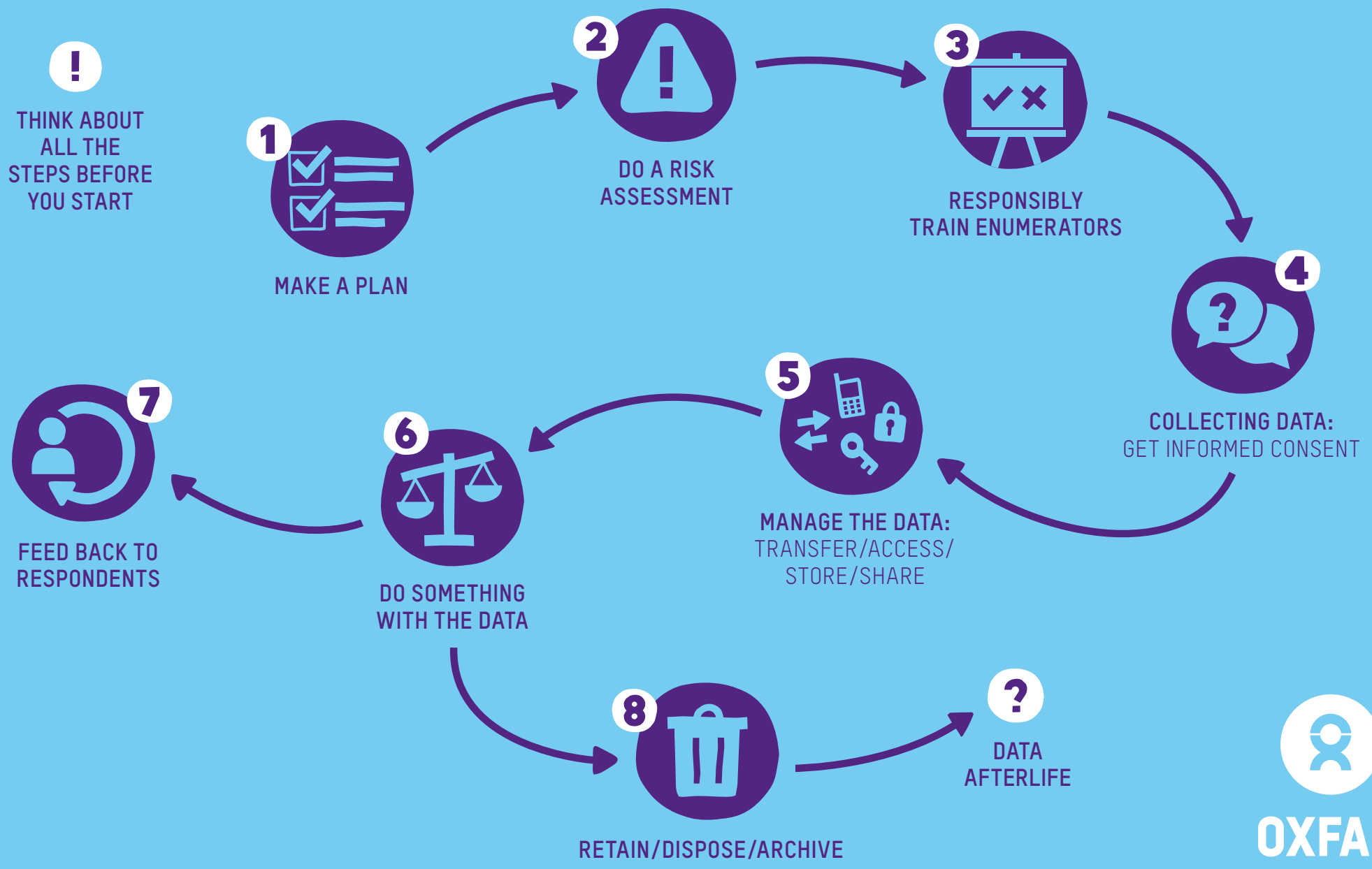
Informed consent A voluntarily and freely given agreement, based upon a clear appreciation and understanding of the facts, implications and future consequences of an action. Individuals must be aware of their right to refuse consent, and able to exercise it. There are situations where consent might not be possible, e.g. with children, or people with disabilities.

Personal data Information that can be used, on its own or with other information, to identify an individual.

Privacy impact assessment A tool to identify and reduce privacy risks.

For more information, see...
www.oxfam.org.uk/responsibledata

THE RESPONSIBLE DATA LIFECYCLE



OXFAM