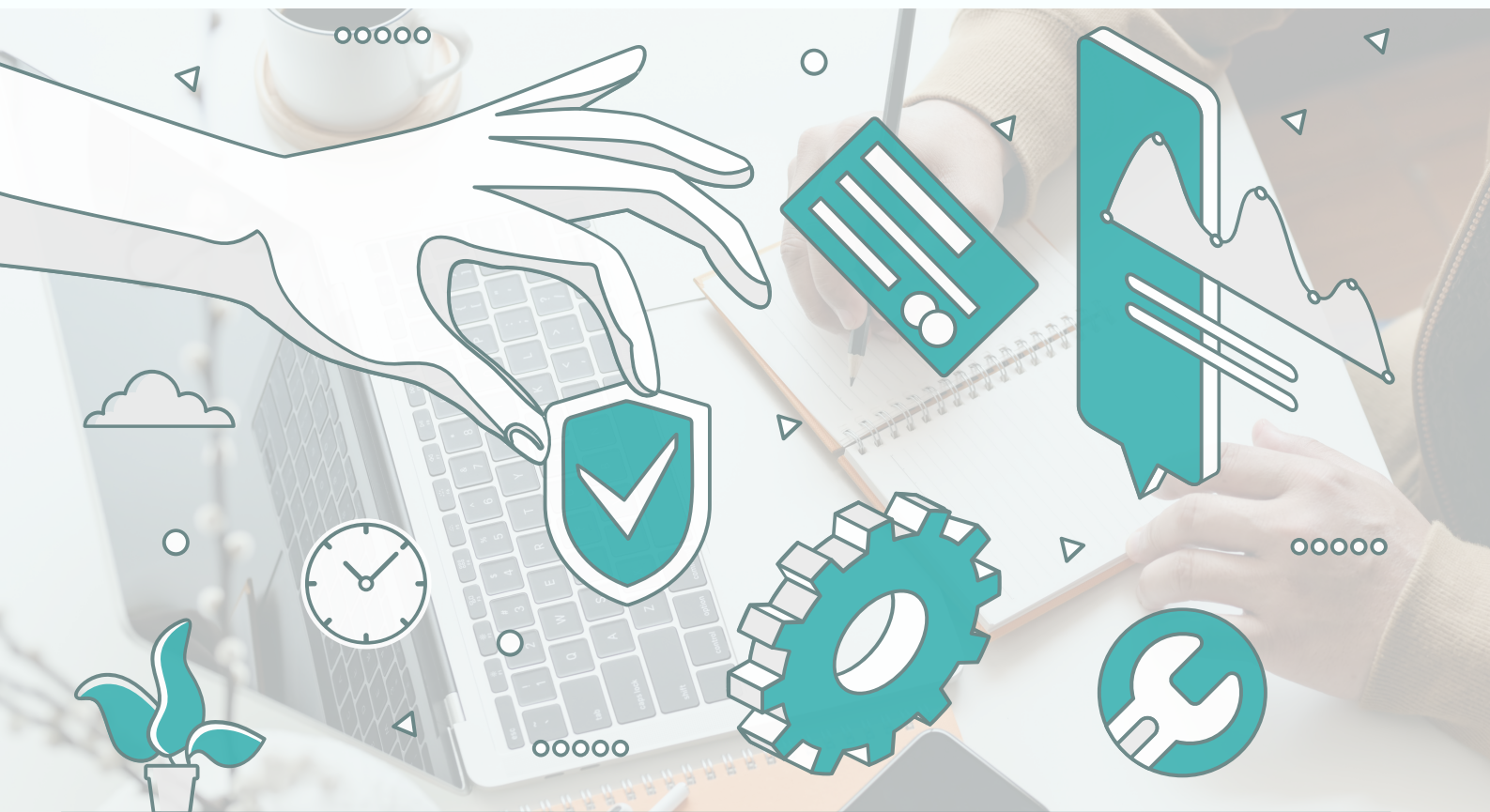


RESPONSIBLE DATA MANAGEMENT PRACTICAL SHEETS

Do's and Dont's of the data management cycle steps



These 12 sheets are the result of a training cycle on responsible data management, part of the CartONG initiative to help humanitarian actors better include responsible data management and data protection into their programs, supported by [the French Ministry of Europe and Foreign Affairs](#), [Handicap International - Humanity & Inclusion](#) and [Terre des hommes](#).

They were drawn up by participants to English - and French-speaking sessions, deployed in over 50 countries, from 12 NGOs: Alima, ACF, CRF, Care, La Chaîne de l'Espoir, HI, MdM, PUI, SI, SIF, Tdh & TGH.

Specific topics have been selected for each stage of the data management cycle, in order to identify good practices (do's) and those to be avoided (dont's). A set of guiding questions defines the scope of the topic.

TABLE OF CONTENTS



TOPIC N° 1

Data minimisation as a mantra to have less data to protect!

TOPIC N° 2

An analysis plan to support data quality

TOPIC N° 3

Training enumerators as the front-liners of responsible data practices

TOPIC N° 4

Building and using unique identifiers to pseudonymise personal data where you can

TOPIC N° 5

Make an asset of your local NGO partnerships in terms of responsible data

TOPIC N° 6

A data processing register to map out and control your personal data



TABLE OF CONTENTS



TOPIC N° 7

Anonymization - opportunity or technical challenge?

TOPIC N° 8

Data, the key to better dialogue between teams

TOPIC N° 9

Data destruction, the forgotten step

TOPIC N° 10

Community feedback to close the loop

TOPIC N° 11

Learning from project experience

TOPIC N° 12

Data sharing in questionable contexts





TOPIC N°1

DATA MINIMISATION AS A MANTRA TO HAVE LESS DATA TO PROTECT!

This is an overview of all the good practices you can have or practices you should avoid in terms of data minimisation (that are feasible with the usual field constraints).



DO'S

- Mention the practice of minimization in the analysis plan and terms of reference
- Setting up a data collection plan
- Include in the analysis plan the people with whom we will share this data
- Identify data collection requirements
- Justify the future use of each item of data collected
- Define data collection objectives and evaluation matrix
- Anticipate the risks that the data collected may represent
- Do not leave any questions open
- Use standard tools
- Clarify study variables to improve analysis
- Limit data to those relevant to survey analysis
- Incorporate minimization into best practice



DON'TS

- Vague and long questions
- Avoid collecting data on paper on specific contexts that require paper
- Collect everything and sort it out after the collection
- Collecting data without identifying a precise reason
- Collecting data "just in case"
- Working in isolation: for example, design a questionnaire without consulting the team
- Exclude certain variables, without justification
- Skip steps in the analysis plan
- Jumping too quickly into the survey without conducting a literature review
- Repeated data collection of the same indicators within short time-periods, when not necessary



TOPIC N°2

AN ANALYSIS PLAN TO SUPPORT DATA QUALITY

This is an overview of all the good practices and the ones to avoid, in terms of analysis plan (that are feasible with the usual field constraints). When should you have it ready? What balance should you take in terms of methods of data collection (between qualitative and quantitative methods)?



DO'S

- Draw up an analysis plan prior to data collection
- Templates should be adapted to the context or the project
- Systematically discuss survey objectives
- Clarify expected outcomes: what is the information and the intended use of it ?
- Involve technical, operations, and MEAL specialists in developing the analysis plan
- Formalise these discussions
- Identify the analysis tool (software) to be used
- Include preferred data visualisation in the plan
- Prioritise or organise the questions according to the indicators to determine any gaps or excess questions to generate the desired analysis
- Clarify any disaggregation required in the analysis
- Challenge questionnaire's formulations/approaches via the analysis plan to integrate the point of view of affected populations;
- Challenge the quantity of information collected to minimise them
- Train teams on the data analysis plan



DON'TS

- Copy and paste the analysis plan from past surveys / tools or questionnaires to reuse past practices without questioning them
- Start the analysis without relying on the plan

**TOPIC
N°3****TRAINING ENUMERATORS AS THE
FRONT-LINERS OF RESPONSIBLE
DATA PRACTICES**

This is an overview of all the good practices and the ones to avoid related to the question of how to help enumerators master aspects related to responsible data management (that are feasible with the usual field constraints), such as informing on data processing aims, legal basis for data collection & consent, and anything related to better data quality.

**DO'S**

- To have a proper training on the global context, to facilitate the data collection process and improve better data quality (rephrasing question if needed, based on the whole context)
- Training on methodological aspects such as bias control
- Training on how to approach the community and adapt the communication: e.g. in the context of beneficiaries affected by a mental health problem, to adapt the manner of speaking
- Training on data security, e.g.: not to divulge passwords, not to write them on post-it notes
- Training on data protection related to data collection, e.g.: code of conduct, policies, importance of consent, confidentiality
- Training on sensitive data, such as health-related data, and in this context, collecting consent even for satisfaction surveys
- Testing data collection tools and processes with enumerators, as an onboarding session about the tool, its specificities, and the data collection process itself

**DON'TS**

- Using personal phones and tablets for project data collection
- Transferring forms links via Whatsapp or other social networks, or taking a photo of a form in order to complete it later
- Allowing enumerators to access data, modify it, after it has been submitted as this can often lead to errors. If a correction is necessary, it is essential to validate the changes and ensure traceability
- Train that, for responsible data management
- Allowing the use of mobile phones/tablets after working hours
- Rushing to start and deploy surveys
- Sharing passwords between enumerators



**TOPIC
N°3****TRAINING ENUMERATORS AS THE
FRONT-LINERS OF RESPONSIBLE
DATA PRACTICES****DO'S**

- Conducting daily (end-of-day) session with enumerators, to reflect on the challenges, the questions, the clarifications and the inputs on data they have collected
- Trainings can be provided by peers or through role-playing, combining the roles of enumerator and MEAL Officer focused on data quality

**DON'TS**



TOPIC N°4

BUILDING AND USING UNIQUE IDENTIFIERS TO PSEUDONYMISE PERSONAL DATA WHERE YOU CAN

It is an overview of all the good practices and the ones to avoid related to building and using unique identifiers for personal data (that are feasible with the usual field constraints).



DO'S

- Use sequential numbers at the end of the code, or use random identifiers, as techniques to pseudonymise data
- Use a platform that automatically generates the unique identifiers
- Implement appropriate security measures to secure the database
- Restrict access of the staff to the unique identifiers document
- Ensure that within different database tables it's necessary to use foreign data for reconstitution
- Take into consideration the relationships between different coding methods that could take place within the same intervention/project, E.g.: Generating a code that represents the household, alongside generating a code that represents each individual within the household
- Provide proper training to the data enumerators, project teams on how to effectively use the unique identifiers to avoid as possible the duplication



DON'TS

- Associate photos or first and last names of beneficiaries with unique identifiers
- Establish a pseudonymisation code based on personal identifiers such as date of birth, city, gender, etc.
- Using personally identifiable information to build a unique identifier

**TOPIC
N°5****MAKE AN ASSET OF YOUR LOCAL NGO
PARTNERSHIPS IN TERMS OF
RESPONSIBLE DATA**

It's an overview of all the good practices an NGO can have with its local partners (that are feasible with the usual field constraints). This presents the different dimensions you should be looking into (administrative, capacity building, technically etc).

**DO'S**

- Include the responsible data management approach in the discussion when starting the partnership and in the MoU/agreement
- Codifying data is a good practice that the local partner should be encouraged to adopt.
- Raise awareness of data protection practices, e.g. how to share data
- Define a chain of communication and clarify roles and responsibilities within the partnership framework
- Identify actions to be taken around the responsible data management especially regarding data collection and data sharing processes, e.g. through a roadmap
- To have a harmonised tool rather than a unique database and identify the roles in data collection to avoid duplication efforts and beneficiary fatigue
- List the type of data to be collected and all elements of personal and/or sensitive data
- Describe potential risks and threats of all data processing activities of the project such as sharing, with the partner

**DON'TS**

- Data sharing outside of the MoU framework
- Internal/external database shared by the partner without security measures
- Offering local NGOs tools that are unsuitable or difficult to use, which can lead to misuse and data protection issues
- Reduce the importance of data sharing in the partnership and its associated risks



TOPIC N°6

A DATA PROCESSING REGISTER TO MAP OUT AND CONTROL YOUR PERSONAL DATA

It's an overview of all the good practices and the ones to avoid an INGO can have in terms of mapping out its data processing through a data processing register (that are feasible with the usual field constraints). Make sure you clarify when and how it can function, what type of generic profile should fill it, what you could have in it, how it can be maintained, without it being a burden on the organisation.



DO'S

- Define roles and responsibilities / persons in charge of the data processings register
- Define access to the register accordingly
- Identify a clear purpose of the data register to know what data to collect and what not to collect
- Define retention/archiving/destruction periods for each type of data
- Include the DPIA (Data protection Impact Assessment) outcomes in the register: the level of risk, the measures in place to secure the data
- Structure the register tool in a clear and easy to understand way: e.g., by project, then within each project, the different areas of intervention of the project
- Include links must to enable access to the data, and access must be restricted to clearly identified persons
- Secure the register storage space
- Review the register on a regular basis to add new entrants and move out the ones that are redundant



DON'TS

- Putting the data itself in the register, where only the metadata should be written down in it
- Put people in responsibility of the register and datasets who haven't the right skill set

**TOPIC
N°7****ANONYMIZATION - OPPORTUNITY OR
TECHNICAL CHALLENGE?**

Guiding questions: Anonymization is a technically difficult subject requiring advanced specialist skills. What can an NGO - which generally lacks these skills - do to properly anonymize its data?

**DO'S****Upstream:**

- Check that anonymization is essential, as the process is irreversible
- Reduce the amount of sensitive information available
- Check that you have the technical skills in-house or, if not, call in external consultants
- Carry out a risk assessment
- The decision to anonymize must be taken before the data is collected
- Train staff in anonymization procedures

During anonymization:

- Use data masking software to hide personal data when necessary (e.g. Tonic.ai, Delphix, Imperva, etc.)
- Ensure that global data is not altered by anonymization
- Inform stakeholders about anonymization processes

**DON'TS**

- Anonymization without checking that you have the necessary technical skills to avoid deleting too much information
- Share data externally if you are unsure of the quality of anonymization
- Do not keep backups during the anonymization process
- Partially hide personal data and consider it anonymized

**TOPIC
N°8****DATA, THE KEY TO BETTER DIALOGUE
BETWEEN TEAMS**

Guiding questions: Data is collected, but how do you ensure that it is actually used to initiate discussions on quality within your organization, and that it is also used by decision-makers?

**DO'S****Dialogue preparation:**

- Define the purpose of the conversation and who needs to be involved (level of expertise, strategic level)
- Set a clear agenda, so that participants have clear expectations and can prepare before the session

Conditions for quality dialogue :

- Encourage open dialogue and trust, and make sure people feel at ease
- Encourage decision-makers to share their views and needs
- Set clear objectives for data collection and use
- Ensure that roles are clearly defined at each stage of the cycle
- Check data source, validate and control quality
- De-identify personal data not required for decision-making or reporting purposes
- Setting up a framework for testimonials
- Present data as simply and clearly as possible
- Use data visualization tools to highlight trends
- Present the right level of narrative to trigger reflection and enrich analysis
- Establish a feedback mechanism to find out whether data is being used by decision-makers, and whether it is of adequate quality

**DON'TS**

- Sharing sensitive data / personal data
- Include unwanted or unnecessary data to create "infobesity"
- Measuring/tracking everything
- Make do with poor-quality data
- Jump to conclusions based on data
- Neglecting training/briefing of the team and decision-makers, which would slow down the improvement of the understanding and importance of data by all staff

TOPIC
N°9DATA DESTRUCTION,
THE FORGOTTEN STEP

Guiding questions: What can you do and what should you avoid to ensure that the destruction of your data at the end of the retention period is effective?



DO'S

Upstream:

- Drafting and disseminating procedures for data retention, archiving and destruction
- Indicate the retention period for data collected throughout the project
- Ensure that beneficiaries are informed of data retention periods in the data collection protocol
- Ask whether it is relevant and useful to store anonymous, aggregated data for future use
- Keep track of all sources and copies, including paper copies, so that they can be completely deleted
- Promote single-read access to avoid copying and uncontrolled dissemination of data

During destruction:

- Include all copies of data, including intermediate data and all other sources, in the deletion process
- Include an automatic destruction system with predefined deadlines (automatic data purging)
- When destroying external hard drives, call in a professional service; or use appropriate processes and tools to ensure complete erasure of data before re-using the devices
- Inform beneficiaries about the destruction of their data



DON'TS

- Keep non-anonymized data after the end of the data retention period
- Don't check if there are paper copies when deleting data
- Keep backup data after the retention period
- Share personal data with the community
- Share sensitive outcomes that run counter to the community's interests
- Share specific cases or personal data or other data in the community
- Multiply data storage sources

TOPIC
N°10COMMUNITY FEEDBACK
TO CLOSE THE LOOP

Guiding questions: What should you communicate to communities about the outcomes of your data collection, how should you communicate them, and what should you avoid doing?



DO'S

Before setting up the returns mechanism:

- Discuss with communities to identify the best discussion channel to share data collection
- Examine the outcomes in terms of the "Do no Harm" principle, and assess the risks of sharing information (e.g.: could the information to be shared lead to tensions within the community?)

When collecting feedback:

- Use accessible language
- Present a clear objective to the community
- Communicate comprehensive, understandable and usable information to the community
- Recontextualize the subject so that the community can contribute its points of view, providing a space for feedback and involvement
- Sharing positives and areas for improvement
- Find out what will be done with the outcomes and how the information will be shared
- Adopt an empathetic posture to be more in tune with community expectations
- Use of communication channels adapted to the community
- Thanking the community for its contributions



DON'TS

- Use jargon or complex language
- Making false statements or promises
- Communicating sensitive outcomes or personal data
- Share details of specific complaints that have gone through a complaints, feedback and response mechanism (CFRM)
- Ignoring community concerns and feedback
- Withhold important or relevant information that could have an impact on the community's understanding or interpretation of the outcomes
- Not being transparent about outcomes
- Sharing feedback that is too detailed and abstract in its analysis, which can lead to distancing from the realities of the population

**TOPIC**
N°11**LEARNING FROM PROJECT EXPERIENCE**

Guiding questions: You're at the end of the project and you've faced many data responsibility challenges and overcome them as best you could. What do you need to do to ensure that your organization learns from your project?

**DO'S**

- Openly acknowledge difficulties
- Include community feedback and recommendations in the process
- Use inclusive and accessible language in project evaluation
- Document all failures and analyze them to find the root causes
- Document the best practices and solutions we have found to overcome these difficulties
- Check whether the difficulty is due to standard operating procedures (SOPs) that do not correspond to the context, and update them accordingly
- Train staff in new or updated SOPs

**DON'TS**

- Minimize or conceal the problems encountered
- Document lessons learned without sharing them
- Don't implement changes based on lessons learned
- Include a lessons-learned action plan without tracking its progress
- Don't inform decision-makers to take action

TOPIC
N°12DATA SHARING IN
QUESTIONABLE CONTEXTS

Guiding questions: You are sharing data with a donor/institution. Outline everything you need to/could do and should bear in mind to ensure that this is done in a way that respects responsible data management.



DO'S

Upstream:

- Obtain consent from data subjects for data collection and sharing
- Have a data-sharing agreement in place
- Set up a public policy for data sharing, or even have joint NGO advocacy on the subject
- Minimize shared data
- Choose the method used to de-identify data before sharing

When sharing:

- De-identify individuals who need access to data
- Protect shared data with encryption
- Use password generation tools or strong passwords



DON'TS

- Share passwords in the same email as data sharing
- Share unnecessary or incomplete data
- Share metadata
- Share data on a laptop that isn't yours