Responsible data management training cycle

cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Session 3
Responsible Data in action - part 1

Introduction to session 3

And now...

1/ The different dimensions of responsible data management

2/ Focus on data protection

3/ The concepts of responsible data management in action- part 1

4/ The concepts of responsible data management in action- part 2

5/ Discover how current stakes apply to you

Session 3 agenda

- Introduction to today's session
- Overview of the « production » steps of the data cycle
- 2 focuses on topics of high interest:
  - MDC and data protection
  - Secure your systems
- Group work on 6 themes & debrief
- Conclusion

Work on :
1. Data minimization
2. Analysis plan
3. Enumerator training
4. Unique identifiers
5. Work with local partners
6. Data register

The development of this training material is supported by the French Ministry of Europe and Foreign Affairs (MEAE-CDCS). Nevertheless, the ideas and opinions presented in this training do not necessarily represent those of MEAE-CDCS.

Questions & Answers

You can find all the questions and answers from last session, including those we didn't have time to answer live, in the constant companion.

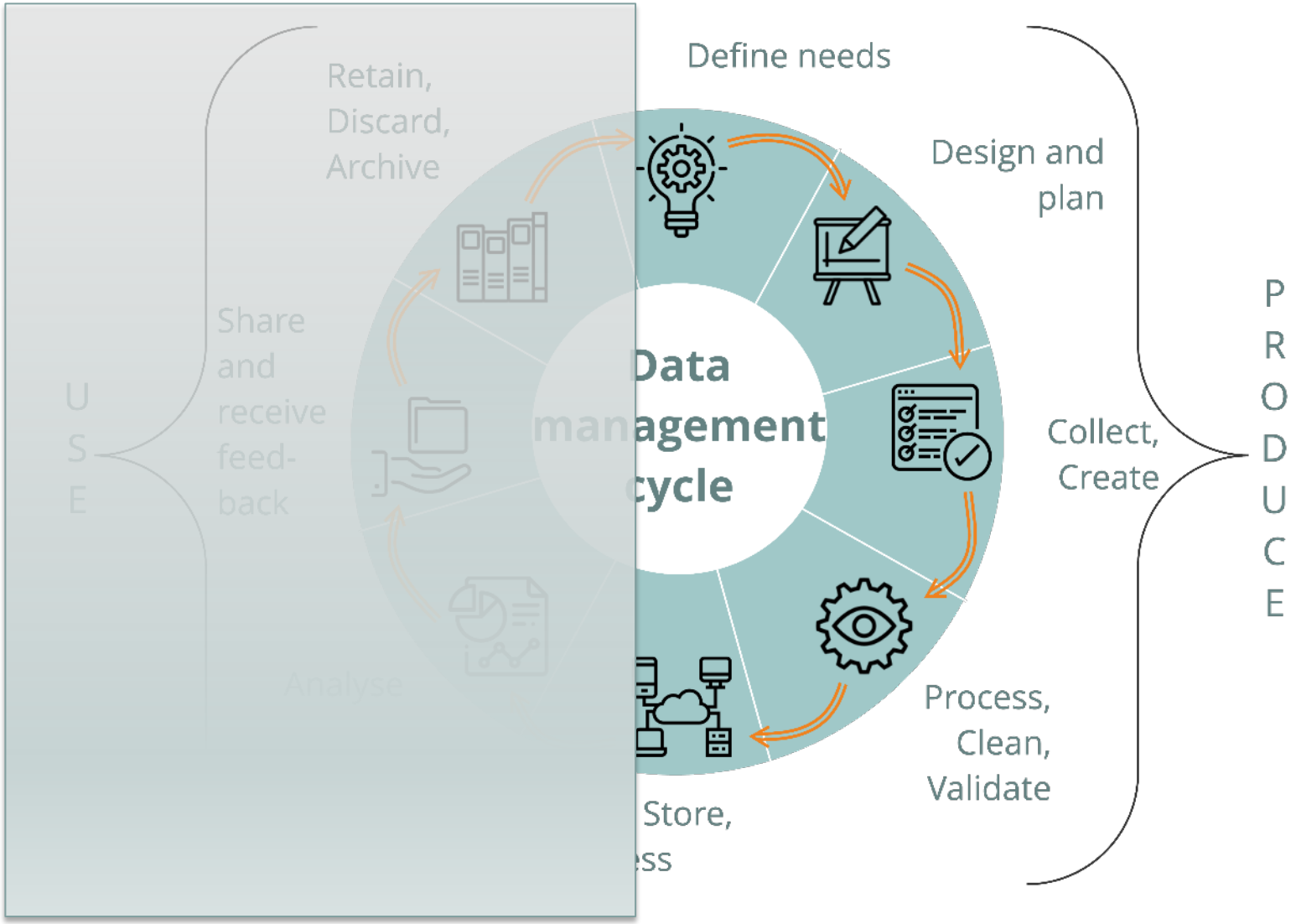
Do you have further questions on the last session?

Quiz

Feedback on the homework

Responsible data applied to data production

Data Management cycle



Source: [CartONG 2020 study]

Step 1: 

- Define the **purpose** of the data collection (& legal basis)
- Based on those needs:
  - Check **compatibility** with applicable **laws**
  - **Evaluate the risks** associated to the data collection and determine **associated mitigation measures**
  - Apply principles of **minimization & proportionality**

Cf session 2 for more information, resources etc

Quiz

Quick reminder of Akachaland and Unicorn

Remember…

In the country **Akachaland**, a major flood during the moon season has devastated around 30 villages, located in the north. You are a member of the **« Unicorn »** NGO, from Finobaka, specialized in the protection of children and women to whom you also provide food and NFI. Its members are mostly from Akachaland and some staff are from Finobaka.

Akachaland

Step 2 :

Confidentiality

- Define adequate **user / role management** for data access
- Determine means for affected populations of providing feedback / making requests related to their data
- Design **data sharing / Non-Disclosure agreements**

Security

- **Select** "privacy by design & default" **tools** to collect, store, share data (see your HQ recommendations)
- **Configure** the tools

Quality

- **Build the analysis plan**
- Inbuild **engagement with affected populations**
- Test/improve data collection tools with quality in mind (unique ID, translation, in-build calculations etc)

Literacy

- **Onboarding** of relevant staff
- Plan internal or **partner trainings**

What would it look like in Akachaland?

To start the assistance as soon as possible, you and your colleagues from Unicorn need to run the data collection in the field with the affected population. What are **the first steps to plan a data collection**? How do you choose adequate data collection tool and method? How do you ensure a data collection in line with its purpose?

Unicorn is working in **consortium with Akachaland care**. The 2 NGOs have decided to share the database to avoid collecting too much data. Unicorn is also working with an external consultant who is a researcher.
How are you going **to plan the sharing of data with your partners** in a secure way, as it contains personal and sensitive data ? How to respect confidentiality ?

Equipe du partenaire local spécialisé en assistance médicale, **« Akachaland care »**,

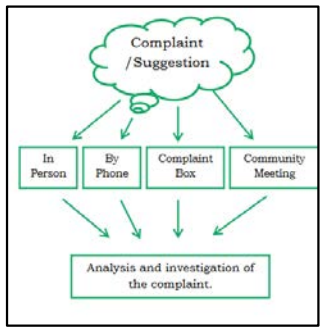
ayant accès aux données en en création/modification: XX

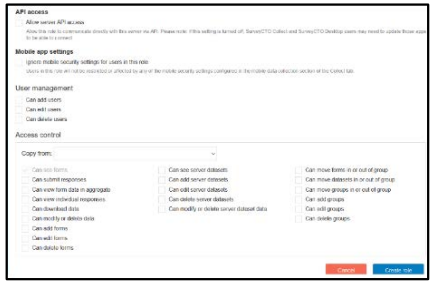
Rôles de Unicorn ayant accès aux données en lecture : XX

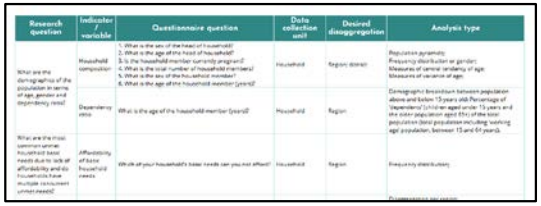
AGREEMENT
CONCERNING THE PROTECTION OF PERSONAL DATA
FOR THE SHARING OF PERSONAL DATA
OF REFUGEES AND HUMANITARIAN AID BENEFICIARIES
(DATA SHARING AGREEMENT, this "Agreement")
Between
UNICORN
And
Akachaland Care
.....

Preamble

fferent stakeholders signing this DSA, list the legal framework binding d by the present agreement and list all relevant other surrounding law. ve any implication here.

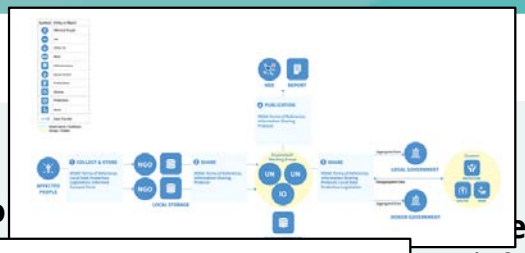


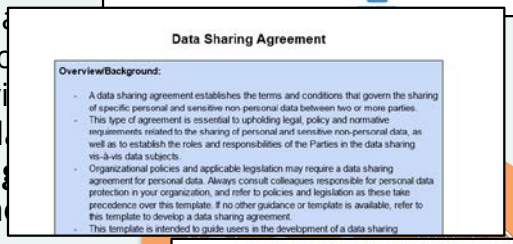


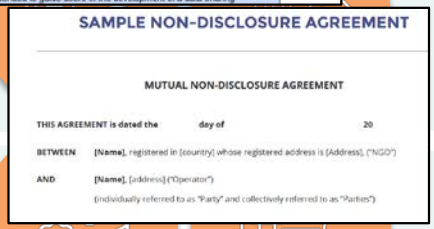


Sources: print screen from SurveyCTO, PSEA task force guidance, SI data sharing agreement, CartONG analysis plan

Ressources / templates available







Confidentiality

Define adequate **user / ro**
management for da
Determine means fo
populations of provi
making requests rel
Design **data sharing**
Disclosure agreem

Security

ect "privacy by design & default" **tools** to collect, store, share data (see your HQ recommendations)
Configure the tools

Quality

Build the analysis plan
Inbuild **engagement with affected populations**
Test/improve data collection tools with quality in mind (unique ID, translation, in-build calculations etc)

Literacy

Onboarding of relevant staff
Plan internal or **partner trainings**

Ressources / templates available

Confidentiality

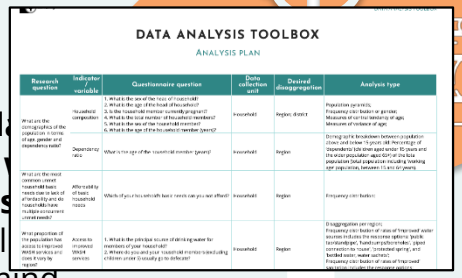
Define adequate **user / role management** for data access
Determine means for affected populations of providing feedback / making requests related to their data
Design **data sharing / Non-Disclosure agreements**

Security

Select "privacy by design & default" **tools** to collect, store, share data (see your HQ recommendations)
Configure the tools

Quality

analysis pl
Inbuild **engagement affected populations**
Test/improve data col
tools with quality in mind
(unique ID, translation, in-
calculations etc)



MDC Toolkit section & Clear Global resources on languages

CartONG Webinar (and presentation) on quality-oriented data collection

Literacy

Onboarding of relevant staff
Plan internal or **partner trainings**

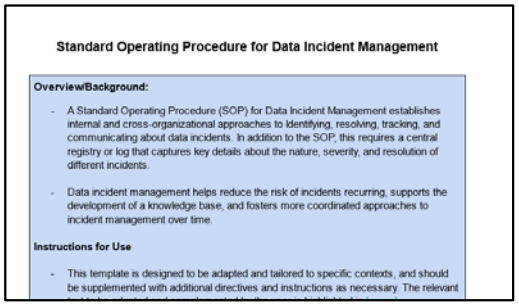
cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Step 2: Design and plan

And more transversally:

- Build **contingency plans** (in case of data breach)
- Define clear project **Standard Operation Procedures**, with roles & responsibilities,
- fill your **data register**
- Include responsible data in your **budget** (tools, trainings, field pilots, translation to local languages, external support for anonymization etc…)



Standard Operating Procedure for Data Incident Management

Overview/Background:

- A Standard Operating Procedure (SOP) for Data Incident Management establishes internal and cross-organizational approaches to identifying, resolving, tracking, and communicating about data incidents. In addition to the SOP, this requires a central registry or log that captures key details about the nature, severity, and resolution of different incidents.
- Data incident management helps reduce the risk of incidents recurring, supports the development of a knowledge base, and fosters more coordinated approaches to incident management over time.

Instructions for Use

- This template is designed to be adapted and tailored to specific contexts, and should be supplemented with additional directives and instructions as necessary. The relevant

FICHE DE REGISTRE DE L'ACTIVITÉ

Cliquez ici, Nom de l'activité

(Créer cette fiche pour chaque activité listée en page 2)

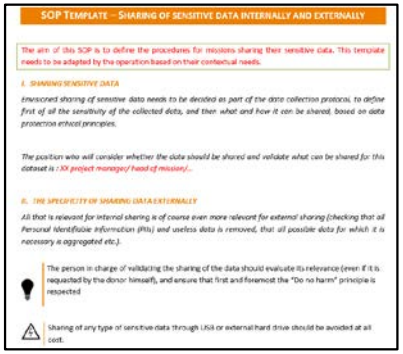
Date de création de la fiche	Cliquez ici pour entrer une date.
Date de dernière mise à jour de la fiche	Cliquez ici pour entrer une date.
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de données est partagée avec un autre organisme)*	Cliquez ici.
Nom du logiciel ou de l'application *(si pertinent)*	Cliquez ici.

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.
Cliquez ici.

Catégories de personnes concernées



SOP TEMPLATE – SHARING OF SENSITIVE DATA INTERNALLY AND EXTERNALLY

The aim of this SOP is to define the procedures for missions sharing their sensitive data. This template needs to be adapted by the operation based on their contextual needs.

I. SHARING SENSITIVE DATA

Ensconced sharing of sensitive data needs to be decided as part of the data collection protocol, to define first of all the sensitivity of the collected data, and then what and how it can be shared, based on data protection ethical principles.

The position who will consider whether the data should be shared and validate what can be shared for this dataset is : XX project manager/ head of mission/...

II. THE SPECIFICITY OF SHARING DATA EXTERNALLY

All that is relevant for internal sharing is of course even more relevant for external sharing (checking that all Personal Identifiable Information (PIIs) and useless data is removed, that all possible data for which it is necessary is aggregated etc.).

The person in charge of validating the sharing of the data should evaluate its relevance (even if it is requested by the donor himself), and ensure that first and foremost the "Do no harm" principle is respected

Sharing of any type of sensitive data through USB or external hard drive should be avoided at all cost.

Sources: IASC task force, CNIL, Tdh example SOP

Step 3 :

Confidentiality

- Use **adequate legal basis**
- Inform on the data usage

Security

- **Respect SOPs** on software and hardware

Quality

- Ensure data collection occurs in the **right language**
- Check **ongoing data** collection quality

Literacy

- Enumerator **trainings**

What would it look like in Akachaland?

Unicorn has chosen its data collection tool and method.
The enumerators will be soon deployed in the field. Unicorn has internal SOPs in place regarding data collection. The population is speaking Warazu and a majority of enumerators speak the language.

What **should you do before launching the collection?** How to choose the appropriate legal basis ?

How do you ensure the **data collection quality** ? Do the enumerators know the tool, the form and the context ?
How do you make sure the **SOPs** of Unicorn are respected during the collection?

Sources: print screen from Kobo toolbox

Ressources / templates available

Confidentiality

- Use **adequate legal basis**
- Inform on the data usage

Security

- **Respect SOPs** on software and hardware

Quality

- Ensure data collection occurs in the **right language**
- Check **ongoing data** collection quality

Literacy

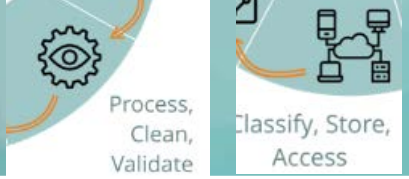
- Enumerator **trainings**

Mobile Data Collection
Learn to master Mobile Data Collection

cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Step 4 & 5 :



Confidentiality

•Ensure data is only **accessible to authorized staff (remote obsolete accesses), with specific rights regular review** of access rights
•Applying **data subject rights** (to object, to data portability, to restricting processing, rectificati erasure, access…)

Security

- Ensure **physical & IT security** of data (paper & digital) and the hardware on which it is (antivirus, firewall, latest version of tool etc)
- **Respect SOPs** on cleaning, validation, access…
- Back-up the data or ensure the software you use does it
- Prohibition of shared accounts

Quality

- Check data **relevance, accuracy, completeness**
- **triangulate** it
- Ensure **data comparability & integrity**/ coherence with related databases

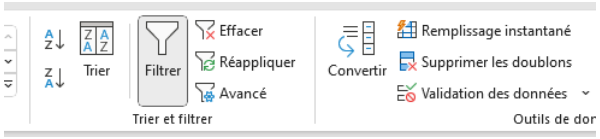
Literacy

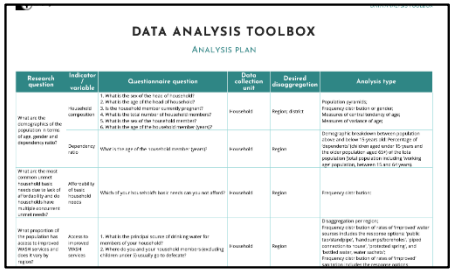
- Ensure proper understanding of data quality, bias, of the teams involved in the cleaning, as well as the limits of the data collected

What would it look like in Akachaland?

Unicorn's team of enumerators has collected data on the children and women to launch its assistance and has it stored. Only some members of Unicorn will need the data to work with the population. The office is shared with all the team and is located in the north area, where the « Akaidnappers » are actives.

Which **security measures** do you take regarding the material and the data stored? Do the children and women have access to their data ? Are their data treated with confidentiality in mind ?
How do you **implement SOPs** regarding the data cleaning? How do you ensure **the data quality** of the database?





Ressources / templates available

Confidentiality

•Ensure data is only **accessible to authorized staff (remote obsolete accesses), with specific rights regular review** of access rights
•Applying **data subject rights** (to object, to dat… restricting pr…icati… erasure, acce…

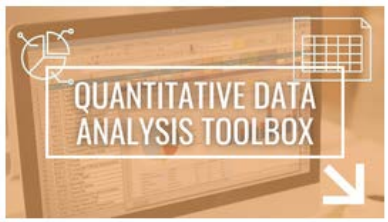
Security

- Ensure **physical & IT security** of data (paper & digital) and the hardware on which it is (antivirus, firewall, latest version of tool etc)
- **Respect SOPs** on cleaning, validation, access…
- Back-up the data or ensure the software you use does it
- Prohibition of shared accounts

Quality

- Check data **relevance, accuracy, completeness**
- **triangulate** it
- Ensure **data comparabil… & integrity**/ coherence w… related databases

On the field, I don't analyse, I Excel!
Become a fan of the fabulous tool that is Excel



Quantitative data analysis
Learn all the tricks of quantitative data analysis

Literacy

- Ensure proper understanding of data quality, bias, of the teams involved in the cleaning, as well as the limits of the data collected

cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

2 Key focus

Mobile Data Collection and data protection

Quiz

You want a secure tool?

- Encryption of forms / data
- Application encryption
- Server localisation
- Platform hosting
- Marking of sensitive datasets
- Data expiry dates
- « Cold-room computer »
- …

Advantages:

- The data that needs to be is secure (for ethical reason & compliance

Disadvantages:

- Harder to set up and use
- Distinctive features that requires a higher cost

Open Q&A around your MDC tools

Secure your systems

Why?

*"Security safeguards **appropriate to the sensitivity of the information** must be in place prior to any collection of information.»*

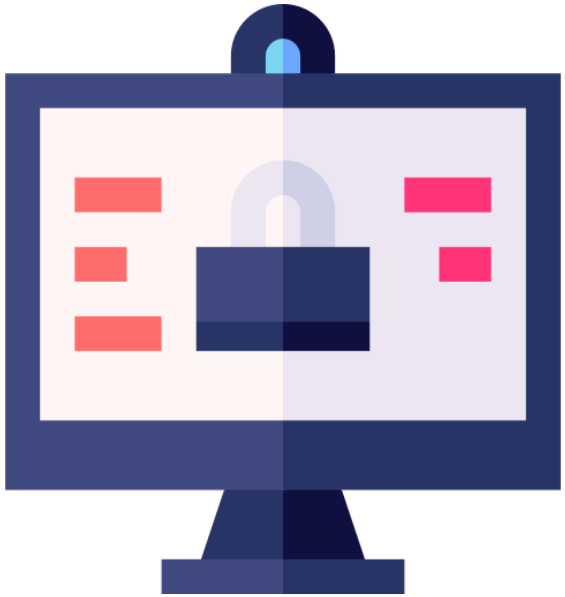
Professional Standards for Protection Work

In field offices, **basic digital security hygiene is often lacking**. Password management and encryption is weak or non-existent, and multi-factor authentication and intrusion detection are not currently common practice. Data on insufficiently protected devices can be exposed when passing through security checkpoints and borders. Unprotected devices may be confiscated, corrupted and compromised.

May 2019 – Wilton Park event - OCHA

Nota Bene

*We will try here to focus on **things that can be done at your individual/mission level**, but depending on your organisation, some of these aspects should be tackled at an organisational level*



1/ Securing your workstation

Objective: Prevent fraudulent access, virus launch or remote control, especially via the Internet.

How?

- Regular software and antivirus **updates**
- **Log off** when away from your computer
- Limit the use of **external mobile** devices
- **Do not use personal equipment** in a professional context (BYOD - "Bring your own device")
- Never connect to **public Wi-Fi**, and **use VPNs** where necessary

2/ Protecting yourself against phishing

Objective: Prevent fraudulent access through phishing

Definition: *fraudulent communication masquerading as a reliable source, designed to trick users into disclosing sensitive data or installing malware programs. These attacks often take place via e-mail, but can also occur on social networks* ***(source: CyberPeace institute)***

How?

- **Never click on a link from an unknown contact**
- **Check the sender's** e-mail address
- **If in doubt, contact the sender by another means of communication for confirmation**

3/ Secure exchanges

Objective: Secure personal & sensitive data transmissions

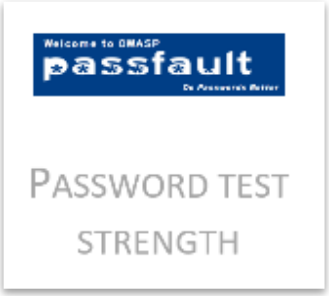
How?

- **Deidentify** data
- Use **secure sharing platforms**
- **Encrypt** data
- **Avoid emails**
- Share **passwords through secure channels**
- **Raise the awareness** of your recipient!

4/ Managing authentication

Objective: Secure access to applications
How?

- Use tools that allow **individual access,** and avoid shared accounts at all costs
- Stop writing passwords on **post-its**
- Use **unique** & **strong passwords** (12 characters, special characters, etc.)
- Use an **organization-wide password manager** (so you can easily manage all your passwords)
- Consider using **2-factor authentication for tools containing personal or sensitive data**



(Examples as food for thought)

5/ Securing mobile equipment

Objective: Anticipate potential data breaches linked to theft or loss of mobile storage media

How?

- **Encrypt** mobile equipment and storage media as far as possible (internal/external hard disks; smartphones; USB sticks)
- **Check** that **backup** and **synchronization** measures are in place
- Ensure that equipment **locking systems** are sufficiently robust
- Never connect to **public Wi-Fi**, and **use VPNs** where necessary

(Examples as food for thought)

6/ Encrypt data as required

Objective: Guarantee data integrity and confidentiality.
***Definition** : encoding of a message or information so that **only authorized persons** can access it and those who are not cannot.*

How?

- Favor tools that enable encryption for personal or sensitive data (e.g. SurveyCTO vs Kobo, Signal vs SMS…)
- Ensure that they use a **recognized and secure algorithm** (e.g. SHA-256, AES-256…)

tresorit send
ENCRYPTED SHARED FILED

ProtonMail
PGP ENCRYPTED EMAIL

SurveyCTO

VeraCrypt
ENCRYPTION SOFTWARE FOR DISK OR USB

7ZIP

SIGNAL
SECURED MESSAGING APPS

(Examples as food for thought)

7/ Ensuring continuity

Objective: Reduce the consequences of unwanted data loss.

How?

- Use your institutional tools, if you have them (or put them in place), **to make frequent data backups.**

8/ Supervise data destruction

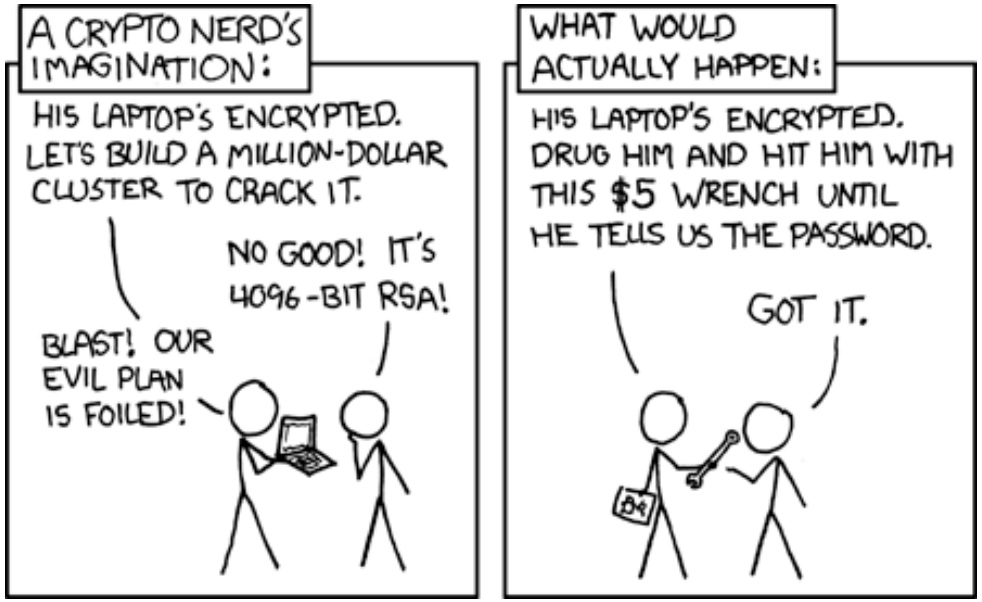
Objective: To guarantee the correct destruction of data at the end of the hardware and software lifecycle..

How?

- **Provide a deletion/archiving date for all personal/sensitive data sets**, and procedures to ensure this is respected.
- **Securely erase data from hardware** (before disposing of it or sending it for repair) and **software used**.

Conclusion on data security

- Keep in mind the **tension between operational efficiency and harmonization of data storage**
- Consider the **existing and desirable level of security of organizational tools** used for **program data management** (data collection, storage and analysis, etc.).
- Data security is a subject that requires, among other things, **the support of cybersecurity experts**.



Source: XKCD

Questions & Answers

Do you have questions on the the topic of security?

Break

Group exercise

Group discussion !

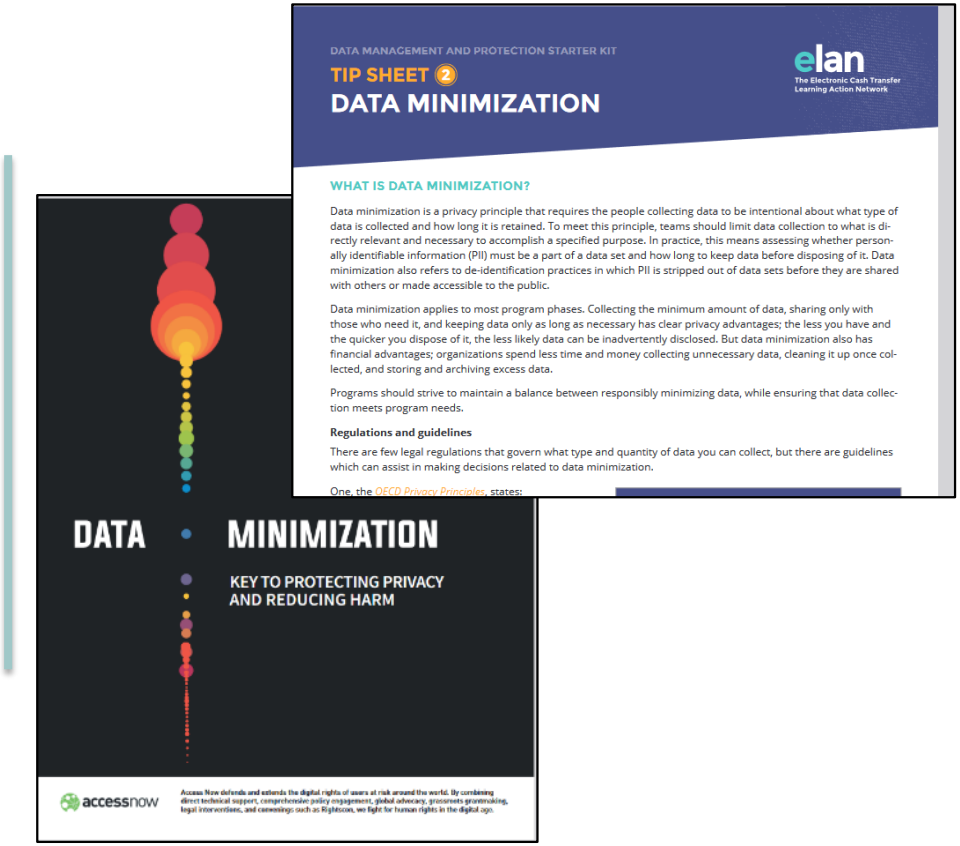
Your group will have a **topic attributed**
You are expected:
- for the topic, to **list Do's and Don'ts in terms of good practices**
- to **answer your « nut cracking » question** related to the theme

Groups :
1. Data minimisation
2. Analysis plan
3. Training enumerators
4. Unique identifiers
5. Working with local partners
6. Data registry

Correction – a few elements of reflexion & resources

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

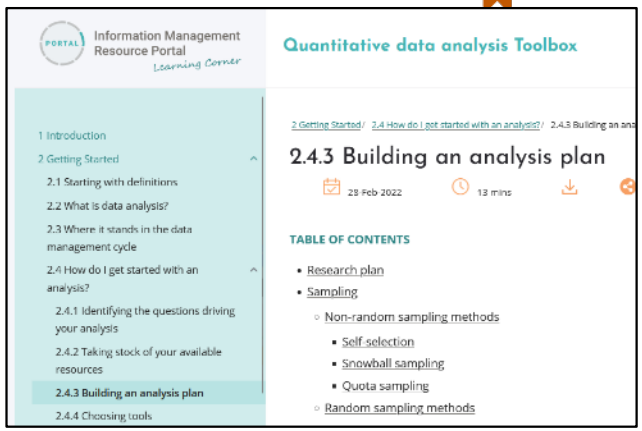
- **Be creative** about **how to minimise** data collection and sharing
- For example, once you sampling strategy defined, do you really need to collect the names of respondents?

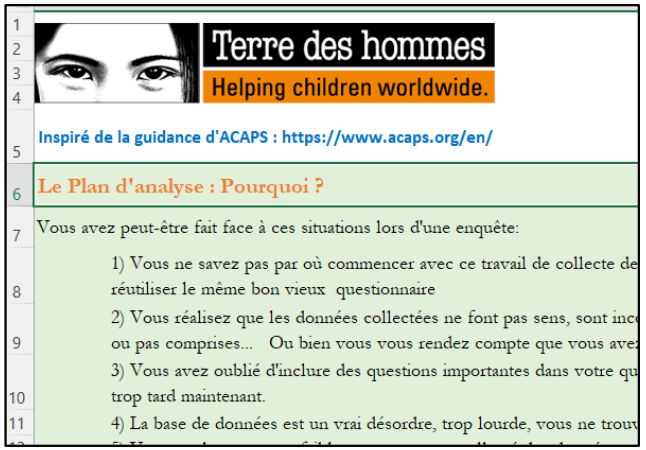


Sources: Accessnow & Calpnetwork

An analysis plan to support data quality

- An **analysis plan is your key to quality** and to document in detail your analysis to
- It is not because it is called « analysis » that you should wait until you get to that stage to prepare it
- It will make your life easier when you get to the analysis!

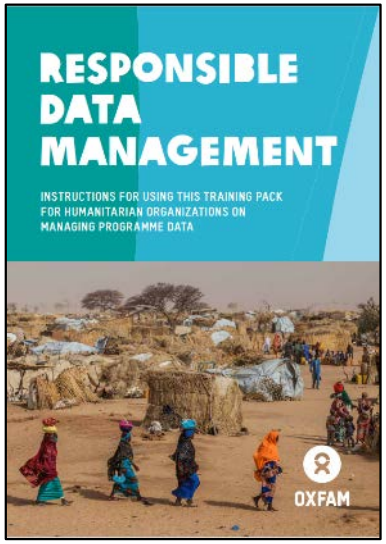




Sources: Tdh & CartONG quantitative analysis Toolbox

Training enumerators as the front-liners of responsible data practices

- **Give meaning to their work**, on why they are collecting data
- **Make them « experience » the tricky quality/responsible data situations**, through « standardisation tests », real life situations, pilot sites etc
- Give them feedback on their work during and after the data collection



Sources: CartONG MDC toolbox & Oxfam

Unique identifiers

- **Create unique identifiers that do not allow people to be directly identified** (e.g. avoid "villageParisHHFinas")
- Follow an internal procedure on this if it exists to standardise practices

Source: Enisa (EU)

Local partnerships

- **Question your practices / relation with your local partners** in terms of data for operational uses / M&E
- Think long term- signing a contract that says « you need to use the data responsibly » is not enough, you need to **give them the means** (financially, in terms of capacity building etc) to do so

In the past, we did a workshop of with a scale of « *localisation washing* »

Source: CartONG

Data register

- The data register is a tool that can help your organisation to **document the personal data processing activities**
- To be seen what procedures your organisation wants to set up, between this, an R&R diagram etc
- But it is important to know **who is in charge of a dataset** (its securisation, its RAD etc…) , have a place where the **mitigation measures are** & such

FICHE DE REGISTRE DE L'ACTIVITÉ

Cliquez ici, Nom de l'activité

(Créer cette fiche pour chaque activité listée en page 2)

Date de création de la fiche	Cliquez ici pour entrer une date.
Date de dernière mise à jour de la fiche	Cliquez ici pour entrer une date.
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de données est partagée avec un autre organisme)*	Cliquez ici.
Nom du logiciel ou de l'application *(si pertinent)*	Cliquez ici.

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : p… formation e…

Cliquez ici.

Catégor…

Source: The French CNIL

Conclusion

Key messages to remember

- Much of what is required in terms of responsible data management is defined at the **planning /designing stage**

- **There are many templates/resources available to help you** in your approach / to help your organization structure/harmonize its procedures - it's not an insurmountable mountain

- Some subjects still lack ready-to-use resources / procedures - but **follow your acquired common sense of "data responsibility"** until !

Homework for the next session

Thank you for your attention!

info@cartong.org

www.cartong.org

cartong