Responsible data management training cycle

cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Session 2
Focus on data protection principles

Introduction to session 2

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 2 agenda

- Introduction to today's session
- Understanding the main data protection principles
  - First overview of the case study
  - Overview of the main data protection principles
- 5 focus areas
  - Which legal basis to choose for a data collection ?
  - And now, what about consent?
  - How to manage and to mitigate the risks ?
  - How to tackle various legal and contractual contexts?
  - What to do in case of data breach ?
- Conclusion

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.

The aim of this session: demystifying this!

Turning this into something you understand and can act upon!

Source: The Guardian

Questions & Answers

Do you have questions from the 1st session?

Quiz

Understanding the main data protection principles

First overview of the case study

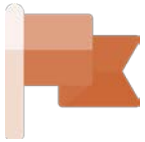
Presentation of Akachaland and Unicorn

Imagine…

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 Non Food Items. Its members are mostly from Akachaland and some staff are from Finobaka.

Your « Unicorn » NGO has had different projects in place in other areas of Akachaland for a decade. It has personal data collected and stored.

You are wondering how can you responsibly manage the data ? And how to apply **data protection principles** in the field ?



Akachaland

Overview of the main data protection principles

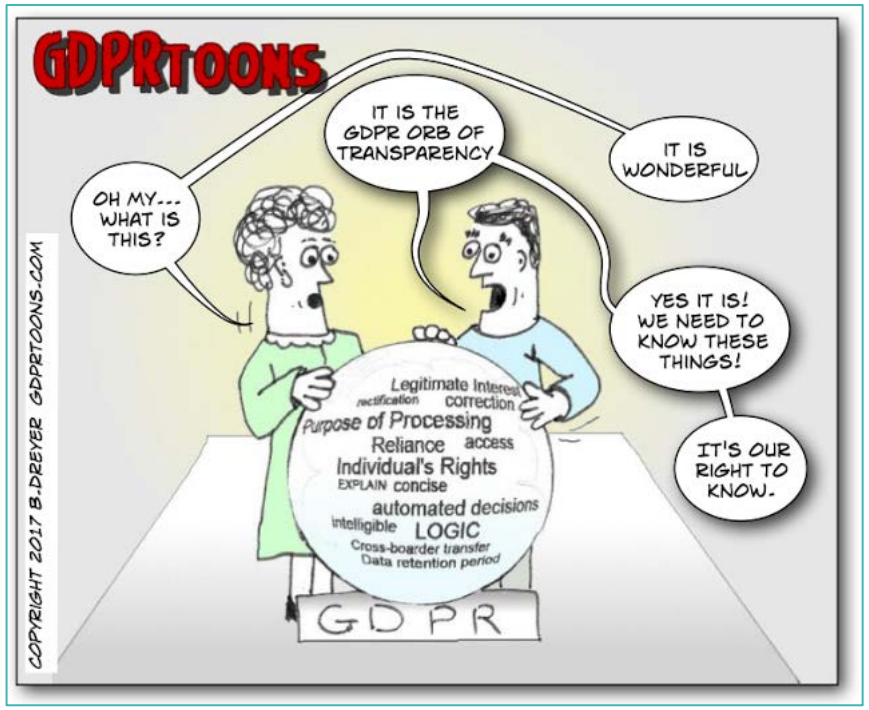
Overview of the GDPR principles

In “complying with GDPR”, we must not lose sight of **what ultimately matters** – ensuring that we never use anyone’s personal information **in a way that they do not want or in a way that could cause them harm** (source: OXFAM).

- Legitimacy & transparency
- Purpose limitation
- Proportionality, relevance & minimization
- Quality
- Limitation of data retention period
- Confidentiality
- Accountability & documentation

Legitimacy & transparency

- Ensure that the data collection processes **do not violate the law ("legal basis")**.
- Be **clear, open and honest** with people about **how you will use their personal data**.
- Record the purposes and **share them in your information**



Source: gdprtoons.com

Purpose limitation

Source: teachprivacy

- Personal data should be collected for a **specific, legal** and **legitimate purpose**
- Be clear about **what the purposes for data processing** are **from the start**.
- The purpose of the data collection & use **should be limited**

Proportionality, relevance & minimisation

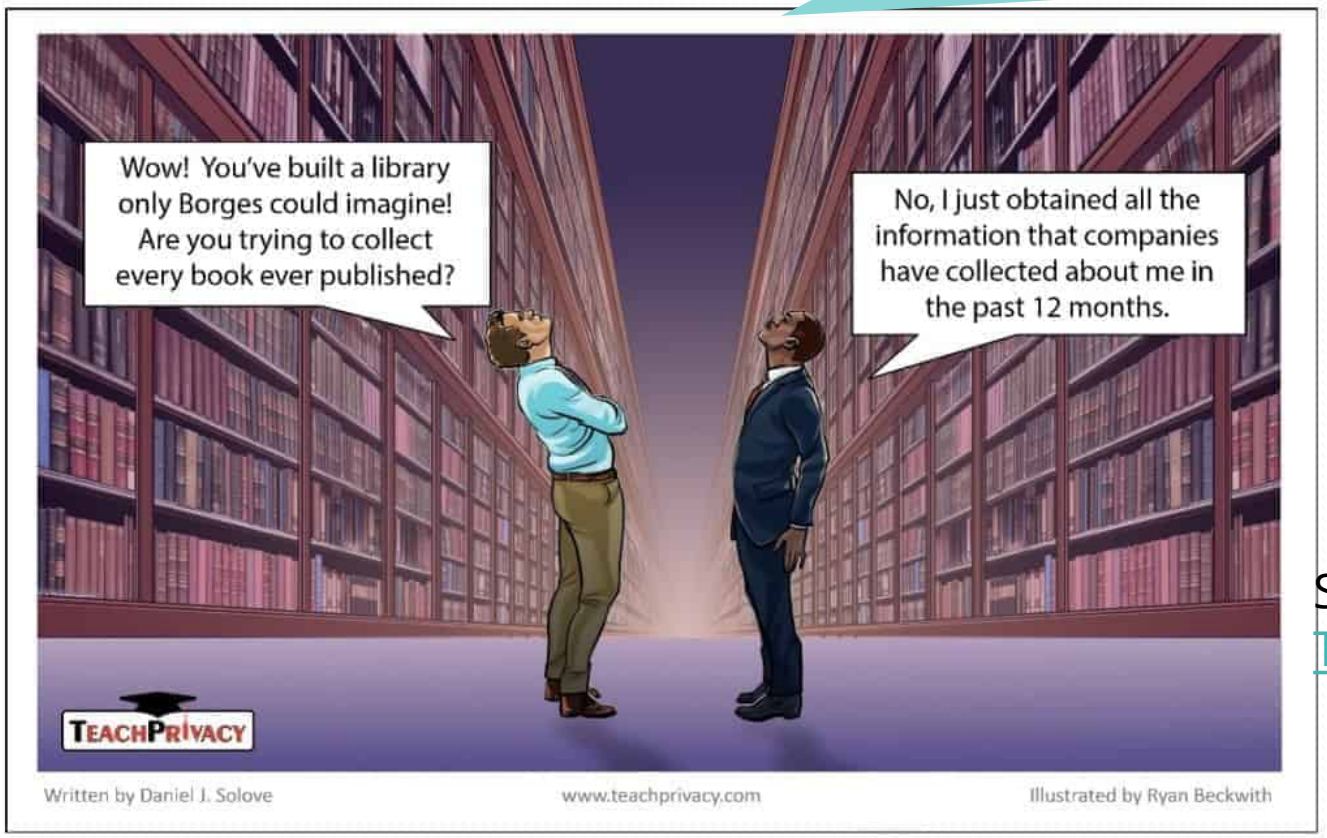
Source: cartoonstock

- The data managed by humanitarian actors should be **adequate, relevant and not excessive** for the purposes for which they are collected and processed
- The principle is applicable throughout the data management cycle.

Focus on data minimization

"**The less data** you process, **the less risk you run of causing harm** with this data." **Key principle** in the humanitarian sector

Examples: remove elements from a database which aren't necessary or categorizing date of birth as age or age group



Source: Teachprivacy

Quality

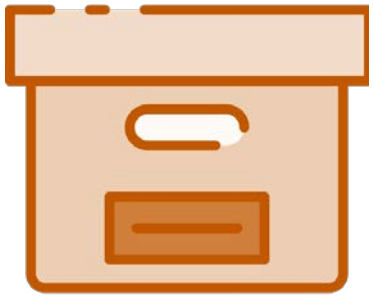
Data quality includes components such as **accuracy, relevance, accessibility and comparability and timeliness, including up to date nature of the data**.

All reasonable steps should be taken to minimize the possibility of making a decision that could be detrimental to an individual, such as excluding an individual from a humanitarian programme **based on potentially incorrect data**.

Limitation of the data retention period

The limitation of the retention period means **keeping the data as short a time as possible**.

Make sure you plan and **are able to justify** how long you keep personal data (for example: for audits, operational needs etc) and ensure you keep as little data as you can during the retention phases (intermediary archiving, anonymization…)

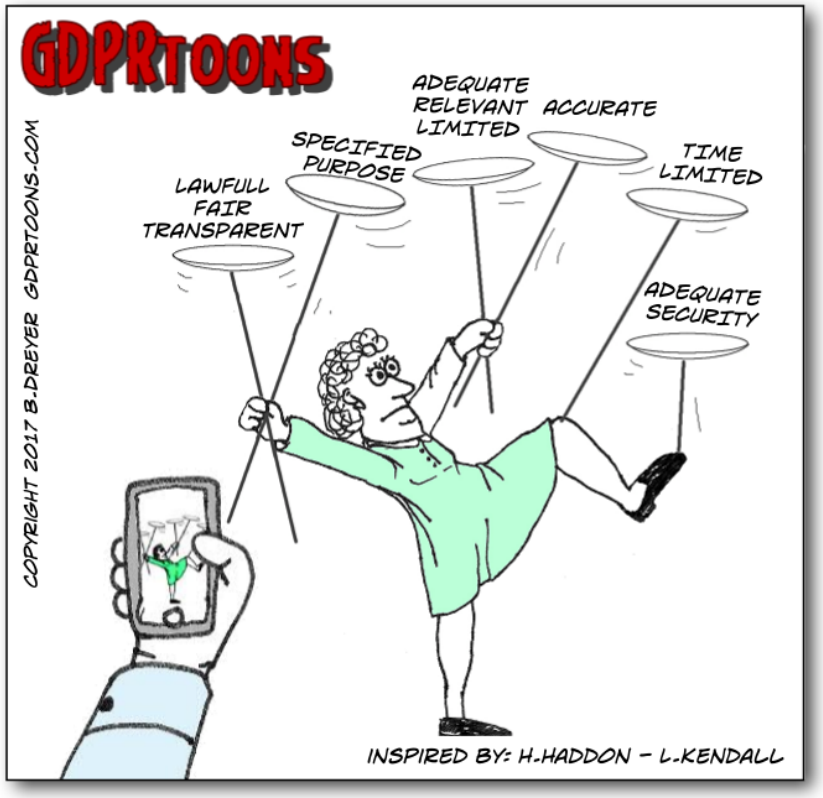


Confidentiality

Confidentiality entails :

- To have **appropriate security measures** to protect the personal data you hold
- To ensure that only **authorized individuals** have access to those data and manage **access rights**
- To have appropriate processes to **test the effectiveness of your measures**, and undertake any improvements
- To make possible the **restoration of data** in case of a physical or technical incident.

Accountability & documentation



Source: gdprtoons

Take responsibility for what you do with personal data and how you comply with the other principles:

- Be able to **demonstrate your compliance**.
- Maintain **records** (in writing) on several aspects of the processing such as **purposes, data sharing and retention**.

Controllers and processors both have documentation obligations.

Associated difficulties

- Applying those principles in some countries can be problematic legally speaking when for example **encryption or VPNs are prohibited**

- It can lead to sometimes **not collecting the data** that you need

Source: All things secured

"In the most severe cases, if the **level of risk is too high** to collect any personal information, the only options are to **collect limited, anonymous information, or rely on alternative data sources**" (Oxfam)

One last detail

All these apply to both:

Paper

Digital

Image source: Tdh

Questions & Answers

Do you have questions?

5 focus areas

Which legal basis to choose for data collection ?

Akachaland and Unicorn

Back to Akachaland…

The access to the communities in the north is quite restricted. You are part of the first convoy with a team of enumerators : amongst the survivors, you need to know how many children and women there are and what are their urgent needs in terms of protection, food and NFI. To do so, you will probably **need to collect their personal data** and determine the exact use for them.

How can you **make sure to collect the children and women's personal data in a legitimate and transparent way**?

Quiz

A few questions on the topic to start off !

The 6 legal basis for data processing

There are 6 different legal basis for data processing under the GDPR:

Source: Teachprivacy

- **Contractual** obligation
- **Legal** obligation
- **Public** tasks
- **Vital** interests
- **Legitimate** interests
- **Consent**

Contractual obligation

The processing can be **necessary for a contract you have** with the individual, or because you have been asked to take specific steps before entering into a contract (e.g. a quotation).

It applies for the following purposes:

- the management of **human resources files**, including recruitment
- the management of relations with **suppliers of goods/services**
- relationships with **donors**

Legal obligation

The processing can be necessary for you to **comply with the law** - identify the specific legal provisions or an appropriate source of advice or guidance that clearly states your obligations

It applies for the following purposes : **employment law**, **financial law**...

If this could put populations at risk of repression, you should **consider not engaging in data collection** in the first place.

Public interest

The processing is necessary for you to perform a task in the **public interest or for your official functions** with a clear mention in the law.

- Activity in question should be part of a **humanitarian mandate established under national or international law**

- This does **not** apply to the majority of NGOs

Vital interests

The processing is **necessary to protect someone's life** (the data subject or another person)

It applies for :

- **monitoring epidemics**
- cases of **sought persons**
- where there is a natural or man-made disaster causing a **humanitarian emergency**
- to process a parent's personal data to **protect the life of a child**
- for **emergency medical care**

Restrictions to “vital interests”

However, it can’t be used for health data or other special category data if the individual **is capable of giving consent, even** if they refuse to give their consent the processing is then limited to **proper emergency phases** (and limited to this assistance) and without further processing

Keep in mind that it should not make you forget data subjects’ **other rights** (such as information or objection)

Legitimate interest

The processing is **necessary for your legitimate interests,** unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

It applies for the following purposes :

- you use people's data in **ways they would reasonably expect**
- the processing has a **minimal privacy impact**
- there is a **compelling justification** for the processing

This is **the most flexible legal basis for processing.** Using this basis **makes you take on extra responsibility** for **considering and protecting people's rights and interests**

Examples of legitimate interest for NGOs

- **collecting data necessary to run the project**
- **scanning its IT systems** for viruses and other IT security purposes;
- verifying the identity of affected population for **anti-fraud** purposes;
- use of employee data for **time tracking**;
- **defending** oneself in a legal proceeding brought by an ex-employee

The key elements about legal basis

Most legal basis require that processing is **'necessary' for a specific purpose**. If you can reasonably achieve the same purpose without the processing, the legal basis will not be valid.

Make sure to get it right first time - you should **not change to a different legal basis at a later date** without good reason. In particular, you cannot usually change from **consent** to a different basis.

Whatever legal basis is used to collect personal data, **accountability to the affected population implies to always inform them**. The population should be informed about the reasons and the use of their data before you collect it.

And now, what about consent?

Akachaland and Unicorn

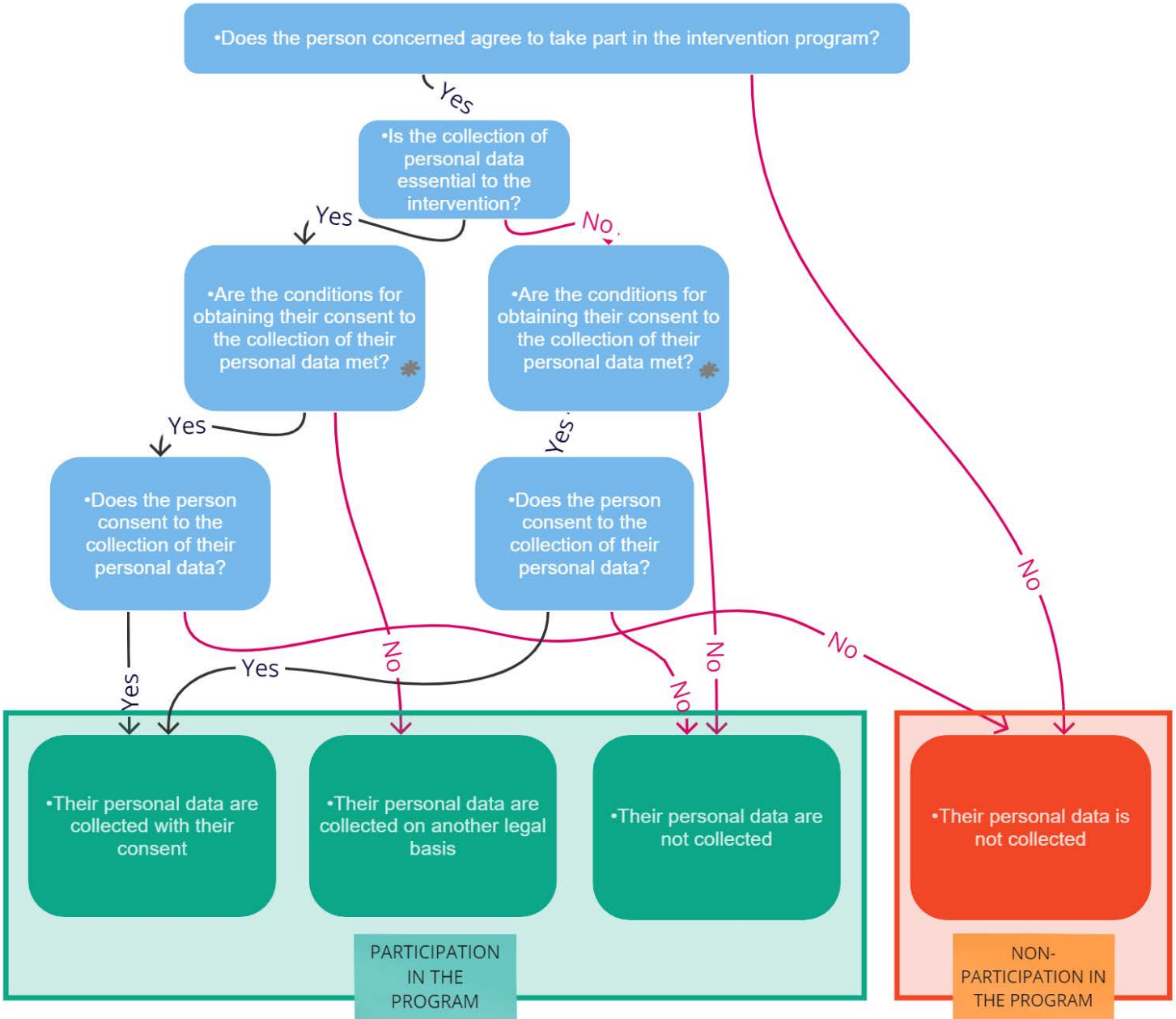
Back to Akachaland…

There are more than 300 children and 500 women amongst the survivors. They don't know the team and the NGO's activities. The population is traumatised after this natural disaster and is in a very vulnerable situation. Some of them lost their homes and members of their family: they have no place to go to.

To start the assistance as soon as possible, in order to respond to the needs, you and your colleagues from the Unicorn team, need to run the data collection in the field with the affected population. You have determined **the purpose** and the use **of the data collection** and **its limitations.**

How do you **inform the population** that it is necessary to collect their data? How do you build trust amongst the population ?

Informed consent to data collection



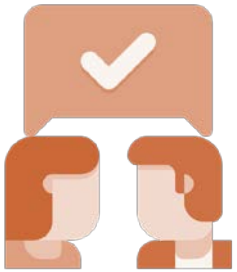
Source: CartONG

Conditions of informed consent

🍟 **Consent = FRIES**

Freely given (consent is clear, there are no tricks!)
Reversible (people should be able to remove their data at any time)
Informed (takes context into consideration! It's on you to inform people appropriately)
Enthusiastic (people need to be able to actively express consent!)
Specific (consentful data collection processes include being clear and explaining that consent given to a specific goal should be limited to that goal alone)

Source: The Engine room



The stakes around informed consent

Consent is supposed to **uphold the dignity for individuals and communities involved**, but it has been proven that:

- people may not be truly giving meaningful consent due to **cultural differences** or knowledge gaps
- informed consent is not effective in an environment with vast **power imbalances**. If there is no way to refuse, then consent is not valid
- to refuse or withdraw consent often impacts the **ability to receive assistance** and services
- "consent messages are in fact **regularly not asked**" (Oxfam)

To keep in mind

This means that the organisation providing assistance holds such power over them that the idea of informed consent is meaningless: **it's like "dangling a lollipop"** , as a humanitarian worker in Somalia noted. (Human rights watch)

Source: Teachprivacy

So what should we do ?

Our recommandations, when possible:

- To **exclude consent** used as a legal basis for data collection, **in most situations**, as its validity is not often solid

- To use other legal basis to collect data such as **legitimate interest** or **vital interests**

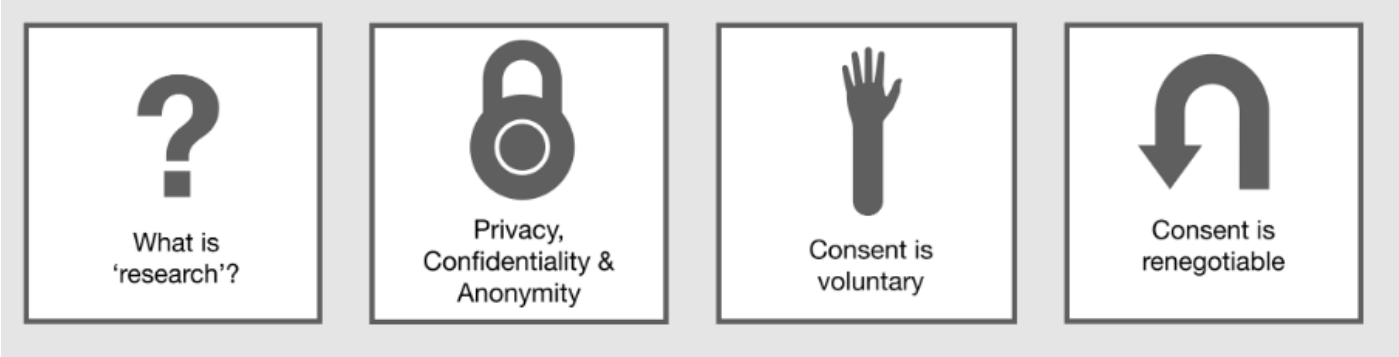
- To **use consent when collecting sensitive data**, such as photo, testimonies or biometrics – it is best suited as the risks associated are stronger

- In any case, to **inform affected people of the reasons behind the data processing**, whichever the legal basis used to collect their data

Field and HQ testimony

From Tdh regarding specific conditions on how to inform children

- **CONSENT or ASSENT** by Children and Consent by caregivers -> WHICH adults to involve ?
- **INFORMATION - method** according to emotional and cognitive maturity,
- **TRUST building** process vs one-off event – **ETHICS vs COMPLIANCE**



International Charter for Ethical Research Involving Children (childethics.com)

From Tdh in Lebanon regarding their practices and processes about children consent

Key elements when obtaining informed consent from children

Obtaining Informed Consent from Children – a Difficult Task

Obtaining informed consent from children can be difficult and partly depends on the age and maturity of the child. There is no easy solution for all countries, demographics and ages. Nevertheless Tdh staff have an obligation to try to get informed consent from the children if their data is being collected. In addition, informed consent by the legal guardians is mandatory. The following is a list of suggestions, to help children understand what they are consenting to.

- Introduce yourself as a person rather than with your status
- Explain the purpose of the data collection
- Inform children about the importance of the data
- Inform children how they will be involved, how much of their time will be required, and how confidentiality will be ensured
- Inform children what kind of information would be collected, how it will be collected, and how it will be used
- Make sure children really do understand what you have told them by asking them to repeat back what you have told them
- Give children time to ask questions or raise concerns
- Listen to children
- Make sure children know that they can stop taking part at any time
- Make sure children understand that you are making no promises about improving their conditions of life
- Make no other promises you cannot keep
- When children have made drawings or written materials they must be told how these might be used and asked afterwards if they wish to be identified as artist/author.

In situations where staff encounter unaccompanied minors who do not have a legally responsible adult to look after their interest, special consideration must be given as to whether approaching a child is in his/her best interest.

Adapted from: "Handbook for action-oriented research on the worst forms of child labour including trafficking in children", p. 115 ff, Regional Working Group on Child Labour in Asia (RWG-CL), December 2002

Source: Terre des hommes

Which data do we need to protect ?

Akachaland and Unicorn

Back to Akachaland…

You **were able to collect data** from the children and women amongst the survivors and target their prior needs. You and your colleagues from Unicorn have access to their data now.

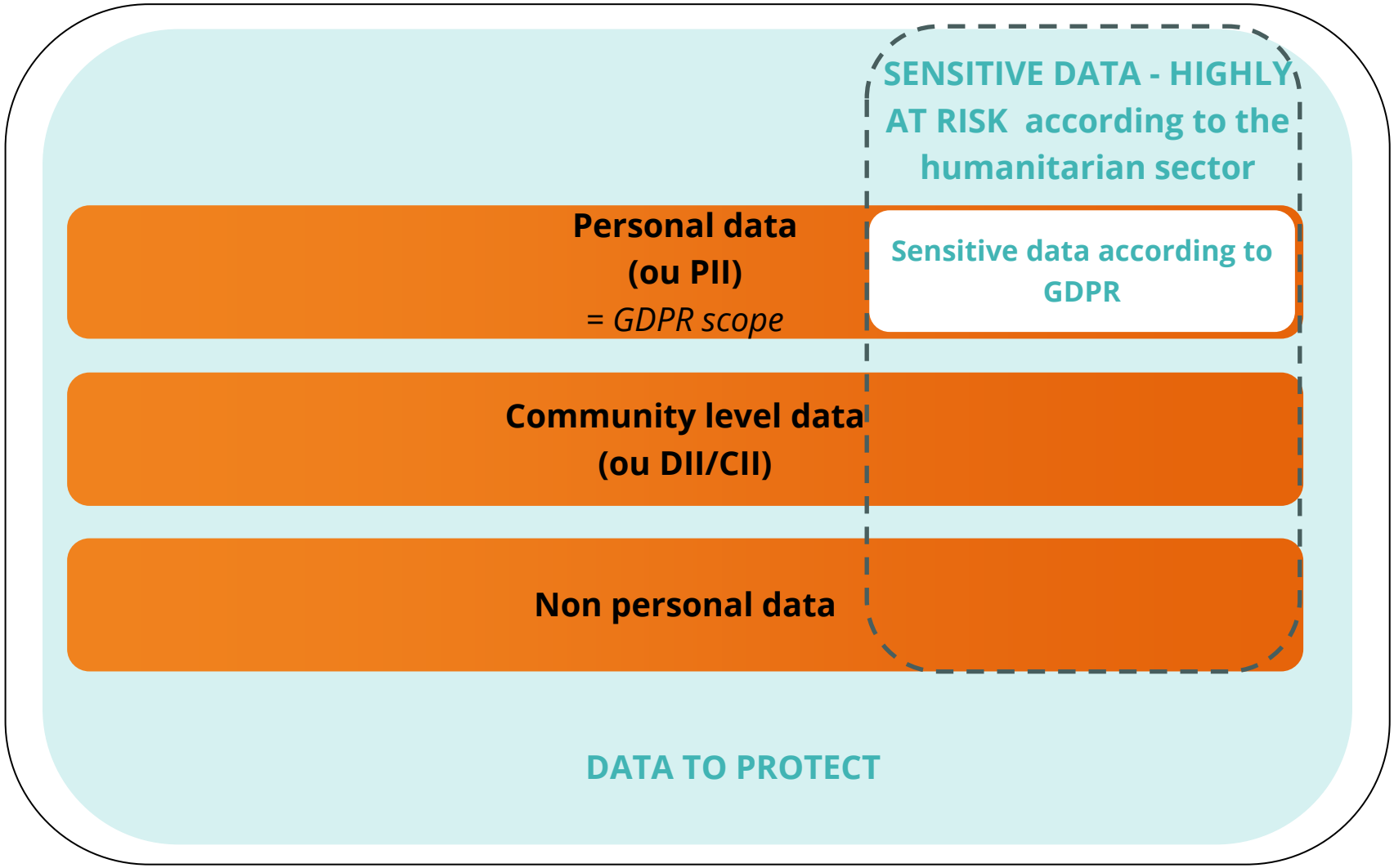
Are you going to process all the data the same way ? How do you **identify the sensitive data** from all the collected data in this context?

Sensitive personal data…

They require a **higher level of protection** because the consequences of their misuse would be **more serious, potentially harming** fundamental rights of the people.

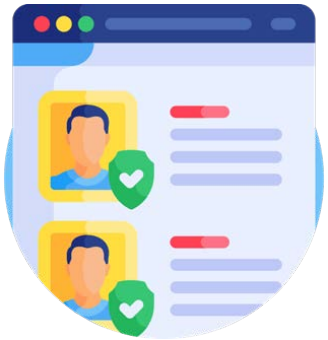
ICRC states :
"**Protecting individuals' personal data** is an integral part of protecting their life, integrity, and dignity"

… and non personal sensitive data



Source: CartONG

Another classification



Information and Data Sensitivity Classification		
Sensitivity	Definition	Information and Data Sensitivity Classification
Low or No	Information or data that, if disclosed or accessed without proper authorization, are unlikely to cause any harm or negative impacts to affected people and/or humanitarian actors.[5]	**Public**
Moderate	Information or data that, if disclosed or accessed without proper authorization, are likely to cause minor harm or negative impacts and/or be disadvantageous for affected people and/or humanitarian actors.	**Restricted**
High	Information or data that, if disclosed or accessed without proper authorization, are likely to cause serious harm or negative impacts to affected people and/or humanitarian actors and/or damage to a response.[6]	**Confidential**
Severe	Information or data that, if disclosed or accessed without proper authorization, are likely to cause severe harm or negative impacts and/or damage to affected people and/or humanitarian actors and/or impede the conduct of the work of a response.[7]	**Strictly Confidential**

Source: Centre for humanitarian data

Another classification of data sensitivity

Information and Data Sensitivity Classification		
Sensitivity	Definition	Information and Data Sensitivity Classification
Low or No	Information or data that, if disclosed or accessed without proper authorization, are unlikely to cause any harm or negative impacts to affected people and/or humanitarian actors.[5]	**Public**
Moderate	Information or data that, if disclosed or accessed without proper authorization, are likely to cause serious harm or negative impacts to affected people and/or humanitarian actors and/or damage to a response.[6]	**Restricted**
Severe	Information or data that, if disclosed or accessed without proper authorization, are likely to cause severe harm or negative impacts and/or damage to affected people and/or humanitarian actors and/or impede the conduct of the work of a response.[7]	**Strictly Confidential**

Yet, **there is no official classification of sensitive data**, as data can be sensitive in a specific context and might not be in another or can change over time. Assessing whether data is sensitive requires a **risk assessment**. (ACF)

Source: Centre for humanitarian data

Group discussion !

Your group is working for « Unicorn » in Akachaland. Some situations from the field are involving data protection issues.

Take some time to reflect on them and answer the associated questions

Debrief of the exercice

How to manage and to mitigate the risks ?

Akachaland and Unicorn

Back to Akachaland…

Few years ago, **the armed group « AKaidnappers »** developped their influence in the countries of the region. This group is known to specialise in kidnapping children and use cyberattacks to gain access to data to localise them.
They target the communities in the north, as this was a landlocked arae before the flood and its access is quite restricted now: they control a small part of the area. They mainly recruit children amongst the community.

The access to the collected data of the 300 children and 500 women is only authorized to some of the members of Unicorn.

What are the **major risks for the community regarding the access of the database,** including personal data ? What measures can you take to prevent those risks from happening ?

Quiz

A quiz to start off on the topic of risks and mitigation measures !

Reminder of must-know definitions

What's a threat ?

Threats are anything that can **cause harm**, either **intentionally or unintentionally**.

E.g. : Unreasonable use: for instance: using data to target assistance by marital status rather than by needs

What's a harm ?

Any damage, injury or **negative impact**- whether tangible or intangible or economic- to an individual or organization that may flow from the processing of personal data. It extends to **any denial of fundamental rights** and freedoms.

E.g. : Tangible harm: bodily injury, loss of freedom of movement, harm to a person or property, and other material or bodily harm.

What's a risk ?

Risks are the intersection of harm and threat and describe **the likelihood and impact of a harmful event** taking place.

E.g. : In a training on HIV/AIDS, the risk of indicting men participating will be much more likely in a country hostile to homosexuality.

Source: CartONG/Tdh

How to identify the risks in data protection ?

It is **common practise to run risks analysis** in the humanitarian sector (e.g.: security)

It is the **same mechanism** that should be applied to the data protection risks of a project (often neglected)

And, even better, **on a regular basis,** they can be **reviewed and updated**

Data Protection Impact Assessment

DPIA - This tool helps to:

- **Identify the risks** and **mitigation measures** of a project/data collection
- **Assess sensitivity of data**

OCHA centre for humdata

THE CENTRE FOR HUMANITARIAN DATA

DATA RESPONSIBILITY IN HUMANITARIAN ACTION

NOTE #5: DATA IMPACT ASSESSMENTS

KEY TAKEAWAYS:

- Data impact assessments determine the potential benefits and risks associated with data management. They are a critical component of responsible data management, but are often overlooked.
- There are a wide variety of approaches to data impact assessments. Selecting the right assessment for a given data management activity can minimise the risk and maximise the benefit to affected people, humanitarians and other stakeholders.
- Applicable laws and regulations, internal policies, the context in which data management will take place and other factors determine which assessment(s) should be applied to a data management activity.
- Data impact assessments should be conducted before and during data management activities in order to inform project planning and design. Activities should be redesigned or cancelled if the foreseeable risks of data management outweigh the intended benefits.

Source: The centre for humanitarian data

When should you conduct a DPIA ?

If a processing is likely to result in a **high risk to individuals**, in particular when 1 of these elements is met :

- Data from people in **vulnerable situations**
- **Innovative use** of data
- **Sensitive data** or highly personal
- Data processed on a **large scale**
- Matching or **combining datasets**
- **Evaluation** or scoring
- **Automated-decision making** with a legal effect
- When the processing in itself "**prevents data subjects from exercising a right** or using a service or a contract"
- **Systematic monitoring**

What are the DPIA contents ?

Your DPIA should:

- **describe** the nature, scope, context and purposes of the processing;
- **assess necessity**, **proportionality** and **compliance** measures;
- identify and assess **risks to individuals**
- identify any additional measures to **mitigate** those risks

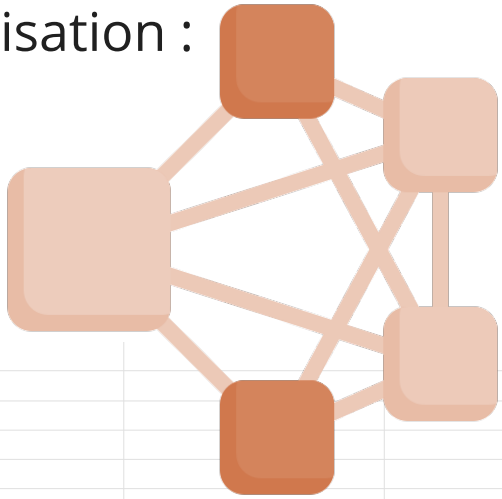
Its **form may vary** depending on your organisation

It's a key step to **raise awareness** inside the team

To document them, a data register?

The data register is a tool that can help your organisation :

- to **document the data processing activities**
- to **map** personal data



Here is an example (from the ICO):

Controller					
Name and contact details		Data Protection Officer (if applicable)		Representative (if applicable)	
Name		Name		Name	
Address		Address		Address	
Email		Email		Email	
Telephone		Telephone		Telephone	

Article 30 Record of Processing Activities									
Business function	Purpose of processing	Name and contact details of joint controller (if applicable)	Categories of individuals	Categories of personal data	Categories of recipients	Link to contract with processor	Names of third countries or international organisations that personal data are transferred to (if applicable)	Safeguards for exceptional transfers of personal data to third countries or international organisations (if applicable)	Retention schedule (i possible)
Finance	payroll	N/A	employees	contact details	HMRC	N/A	N/A	N/A	5 years post employment

Source : The ICO

Field testimony

From HI – on its mission in the Philippines, an illustration of the use of their DPIA tool in the field

How to tackle various legal and contractual situations?

Akachaland and Unicorn

Back to Akachaland…

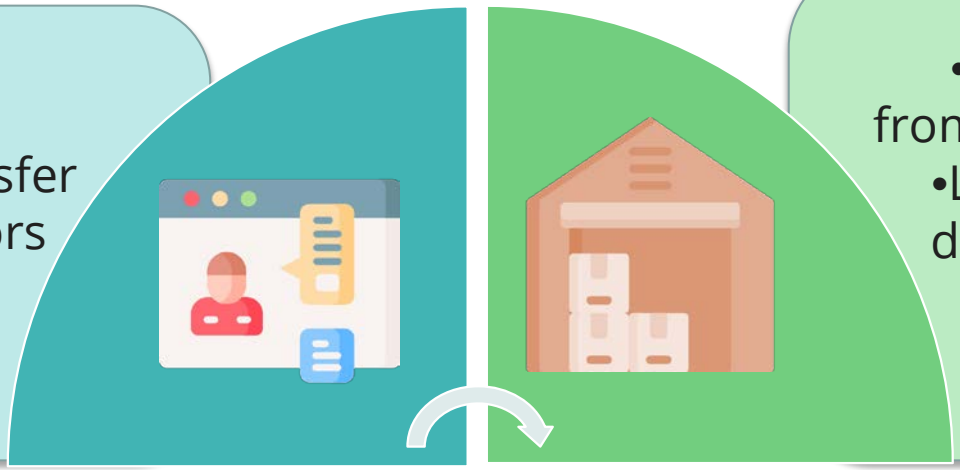
In 2020, **the government of Akachaland** passed a law allowing **mass surveillance** towards the population, as « Akaidnappers » had started to recruit amongst the Akachaland communities. This law requires all NGOs working with the population, especially in the northern area, where your Unicorn team is active, to share their data.
In addition, **your major donor from Brajoki,** is asking for all the information details about the members of Unicorn, to check if they appear in their list of people under international sanctions.
Moreover, **your local partner specialised in medical assistance**, **« Akachaland care »**, wants to use your database to identify the most urgent needs and provide medical assistance to the communities.

How do you manage all the requests, when the collected data is personal and sensitive ? How do you share « safely » the data ?

An example of the various legal and contractual contexts

- Supplementary measure to transfer data to the donors

Brajoki



•National legislation from the country of HQ
•Legislation from the data storage country

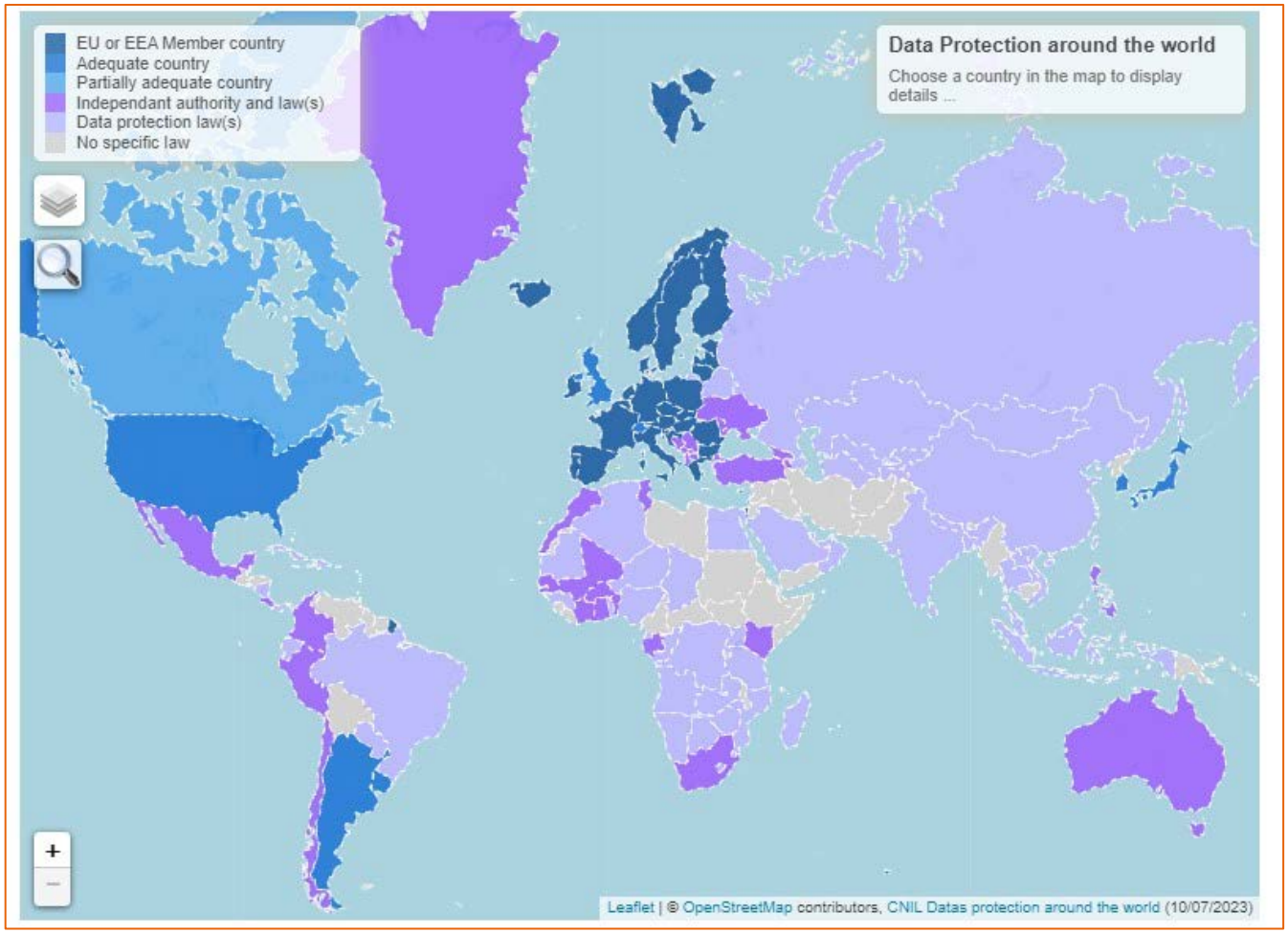
Finobaka

•Local legislation
•Contracts with local partners

Akachaland

World map of data protection legislations

Data protection legislations are developing around the world, though their contents and **level of protection vary**



Source: The French CNIL

What do you need to know about the GDPR ?

The GDPR principles and rules are known as respectful of the right of privacy **legislation**, among the humanitarian sector

As an organization, we fundamentally believe in **the right to privacy**, regardless of the letter of the law. We see GDPR as **complementary to our work and our principles** (OXFAM).

The European legislation applies to :

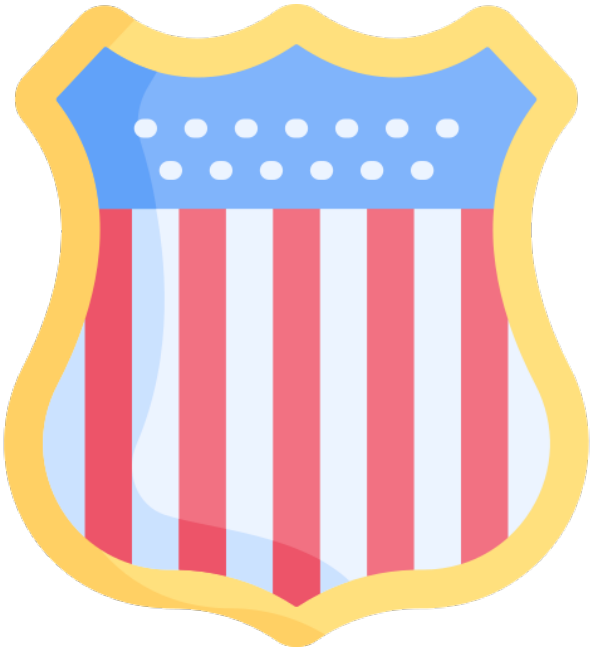
- **Establishments in the EU** regardless the place of the processing
- Organizations established outside the EU which **target data from EU residents**

- "The protection afforded by **this regulation should apply to natural persons, whatever their nationality or place of residence**, in relation to the processing of their personal data" (GDPR)

What do you need to know about U.S.A. Cloud Act?

The USA legislation "Cloud Act" adopted in 2018 broadened conditions for the US government to **request personal data, regardless of the data location**, for example if the data is owned by an NGO funded by US Aid

If such a request is made, you should assess the conditions of the transfer to judge if this is necessary and implement measures ensuring the data is protected, as the transfer to the USA **doesn't comply with basic data protection principles**

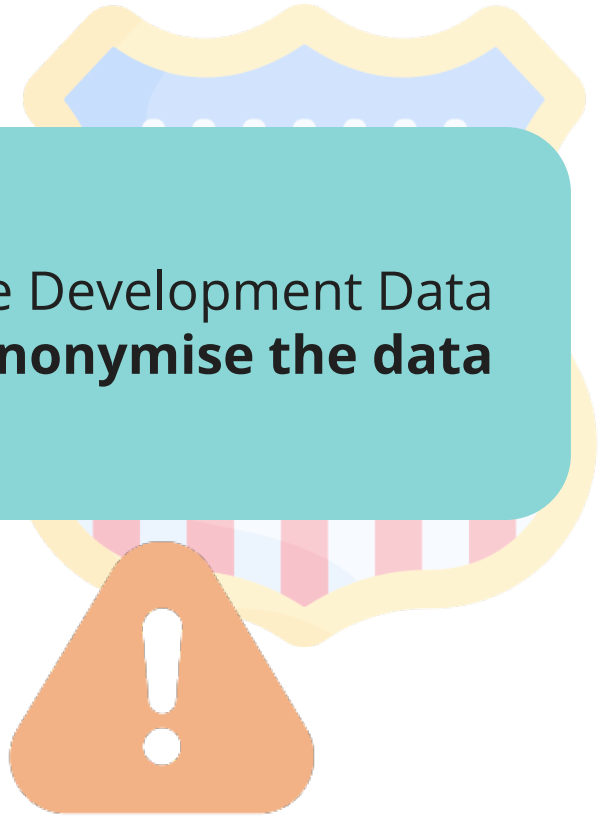


What do you need to know about U.S.A. Cloud Act?

The USA legislation "Cloud Act" adopted in 2018 broadened conditions for the US government to **requ**
of th
the
fund

If su
should assess the s of the transfer to judge if this is necessary and implement measures ensuring the data is protected, as the transfer to the USA **doesn't comply with basic data protection principles**

In case of data transfer request to the Development Data Library of US Aid, it is acceptable to **anonymise the data**



What do you need to know about UN system ?

The UN have **their own data protection legal framework -** it is supposed to apply the same level of data protection as the GDPR

A majority of UN agencies have guidelines and policies for their implementing partners, but **various practises** are observed, **sometimes problematic**

Recommandations:

- **Check with your HQ** what the organisation's policy is
- Be careful about the clauses **before signing a contract**
- **Refer** them to **their own policy** if contracts are problematic
- Take **extra protection mesures** when transferring data

United Nations

What to do in case of data breach ?

Akachaland and Unicorn

Back to Akachaland…

The armed group « AKaidnappers » was able to **hack your system** and access some data collected in the field, from a database shared with « Akachaland care ». It contains names, location, age, family members and health records.

You are only discovering the attack because one of your colleagues realised 2 days ago that they couldn't access the concerned database. You don't know yet the exact circumstances of the incident, nor the volume and the nature of data hacked.

What are the **first measures you take in this situation** ? What do you do towards the population ? How do you report the breach ?

What is a data breach?

The loss, destruction, alteration, acquisition, or disclosure of information caused by accidental or intentional, unlawful or otherwise unauthorized purposes, which **compromise the confidentiality, integrity and/or availability of information.** (OCHA)

E.g. : You find confidential information in a place where it is not supposed to be stored; Your laptop, mobile phone or a paper file with personal data has been lost or stolen (510)

What to do in case of a data breach ?

In 2022, a massive cyber attack on ICRC – we can use its reaction as a model :

- **communicate about the breach,** including to the population concerned
- assess the **severity** of the incident, its context and scope
- **take the adequate measures** to mitigate the risks
- **reflect on the lessons learn** to take preventive steps

Cyber-attack on ICRC: What we know

The ICRC determined on 18 January that servers hosting the personal information of more than 500,000 people receiving services from the Red Cross and Red Crescent Movement were compromised in a sophisticated cyber security attack. We take this cyber-attack extremely seriously and have been working with our humanitarian partners around the world to understand the scope of the attack and take the appropriate measures to safeguard our data.

Source: The ICRC

How to report a data breach ?

In case of a data breach, it is ethically encouraged (and often legally binding) to:

- Report the incident internally based on your procedures
- Report certain types of **personal data breach** to the relevant supervisory authority within **72 hours** after becoming aware of the breach
- If there is a high risk, inform the **data subjects**
- Have a robust **breach detection, investigation and internal reporting procedures** in place
- **Keep a record** of any personal data breaches, regardless of whether you are required to notify

Questions & Answers

Do you have questions?

Conclusion

Key messages

- **Rationalising your data needs** as per the principles of 'data minimization' and 'data proportionality' can go a long way to simplify your data practices, processes and procedures

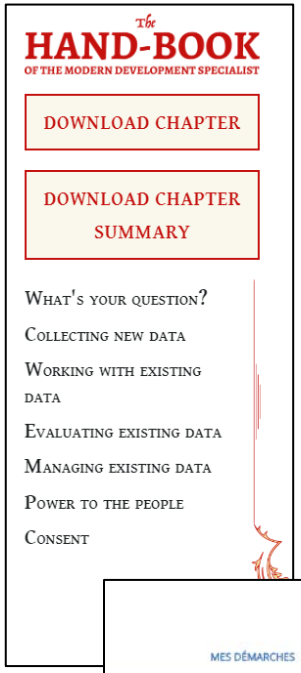
- **Assessing the risks** of data collection is essential to fully respect the « Do no harm » principle, in order to identify risks and take preventive measures

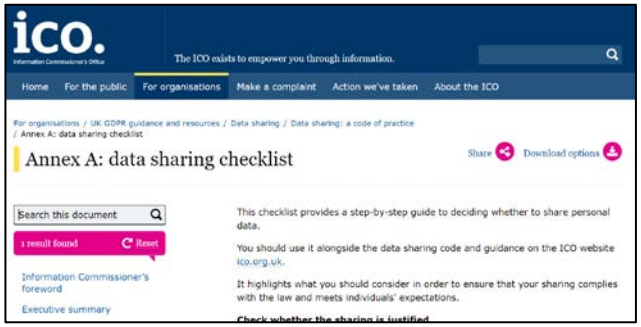
- **Question your legal basis** for data collection

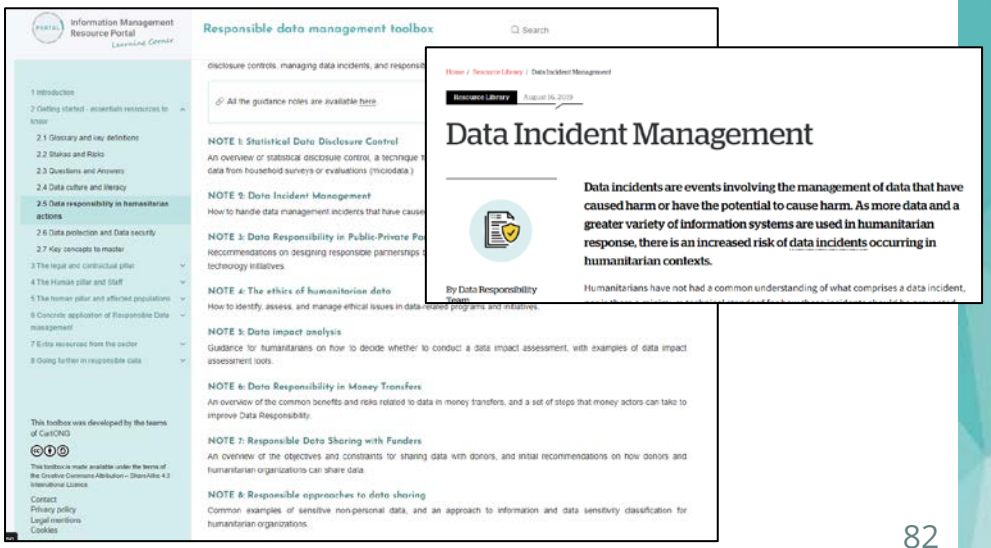
- Accountability towards affected populations: **inform on the reasons behind personal data collection**, even when the consent is not the legal basis for the data collection (and even better, share some results!) .

The go-to resources

If we had to select 5 key references





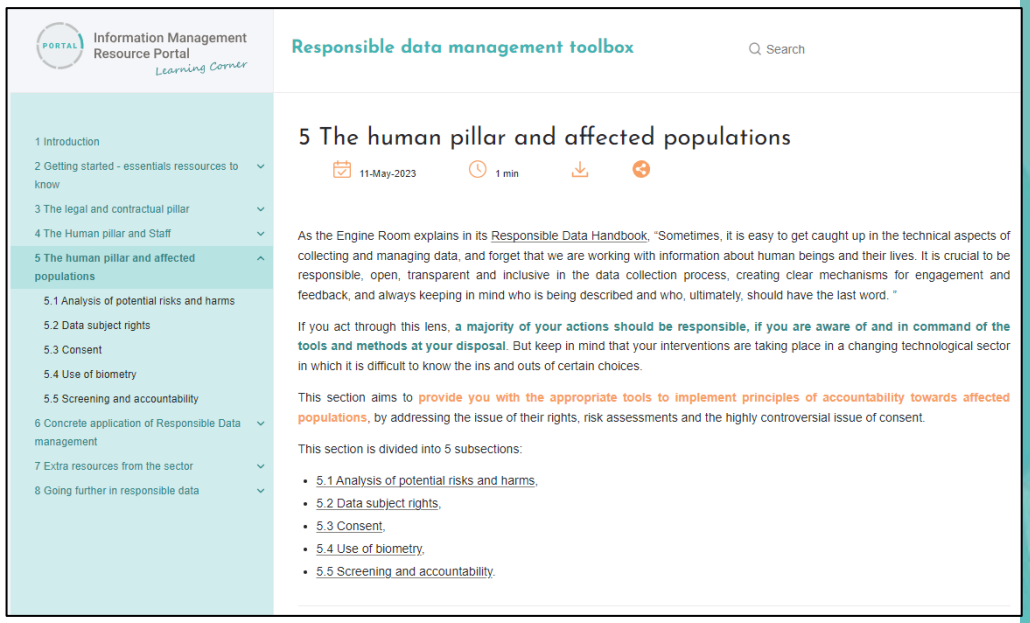


cartong

And the latest CartONG toolkit

Available on https://www.im-portal.org/learning-corner

The sections 3 & 5 for data protection



Available on https://cartong.pages.gitlab.cartong.org/learning-corner/en/3_legal_contract_RD_page

Homework for the next session

Thank you for your attention!

info@cartong.org

www.cartong.org