QUICKLY IDENTIFYING POTENTIAL DATA RISKS

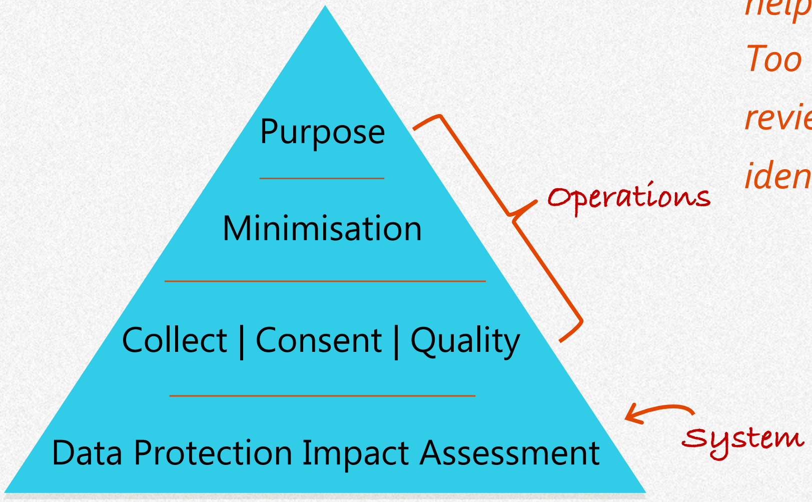
February 2022

Amos Doornbos

Introductions

Digital transformation and using data are commonplace in many of our projects. Digital and data provide significant opportunities for us to improve the effectiveness, efficiency, and engagement of our projects, which is exciting. However, while every opportunity can be used for positive impact, they also come with the potential for harm. This resource is designed to help us increase the effectiveness of digital and data, while reducing the risks and the potential for harm.

We often assume data protection and risk is the job of IT. However, it is not, IT has a role to play, but so does Operations. Operations determines what data to collect and why, while IT helps to ensure the systems we use are as secure as possible. Too often our focus is only on the system and we forget about reviewing risk in our data decisions. This resource is to help us identify the potential for risk and options for mitigation.


Purpose
Minimisation
Collect | Consent | Quality
Data Protection Impact Assessment
Operations
System

Who’s it for? When to use it?

Who’s it for?

This resource can be used by anyone involved in project design and proposal writing and submission. The summary results of this resource can be included in the project risk table.

When to use this resource?

Ideally, it is to be used in the Design phase of the project cycle. A data protection impact assessment tends to focus on our systems used to collect/store data. Broader risk assessments like this resource help us identify risks, to us as an organisation and the project participants, created by collecting and processing personal data.

The assessment of risks and harms should be done by a diverse group of stakeholders and should not only focus on digital and data risk.

Key Definitions

***Personal data** – is any piece of information that someone can use to identify, with some degree of accuracy, a living person, including:*

- A name and surname
- A home address
- An email address
- An identification card number
- Location data

***Sensitive data** -- is a specific set of "special categories" that must be treated with extra security, including:*

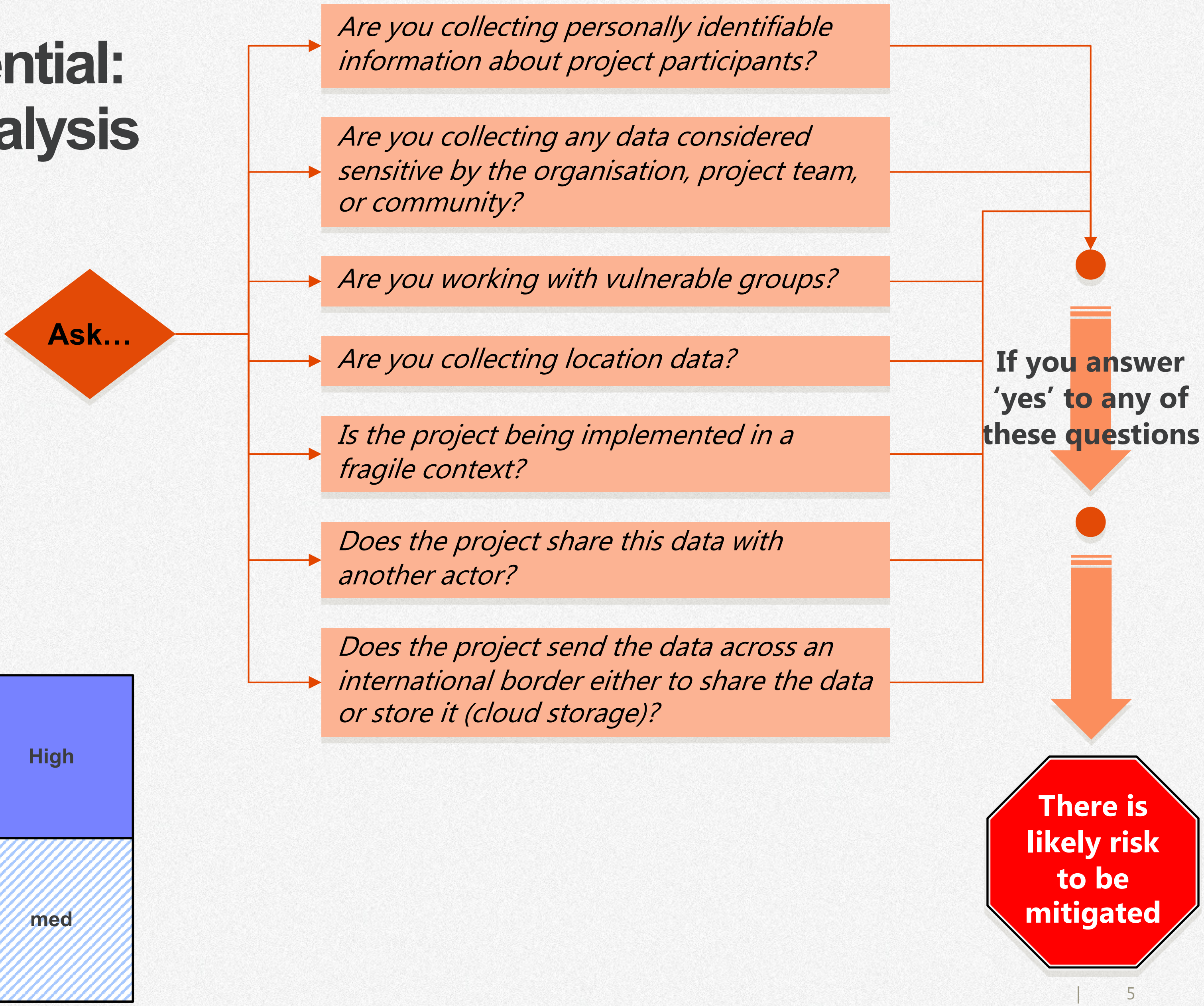
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Genetic data
- Data related to a person's sex life or sexual orientation
- Biometric data

***Risk** – in this context, we define risks as events that might happen to the data or system which have the potential to impact the organisation or individual negatively.*

***Harm** – is defined as damage to someone or undignified or discriminatory treatment, including harm that is:*

- physical (e.g., serious bodily injury)
- legal (e.g., loss of privacy, free expression, or other rights)
- economic (e.g., loss of property or livelihood)
- psychological or emotional (e.g., distress or depression)
- social (e.g., reputational damage)

Risk Potential: Quick Analysis



Ask…

Are you collecting personally identifiable information about project participants?

Are you collecting any data considered sensitive by the organisation, project team, or community?

Are you working with vulnerable groups?

Are you collecting location data?

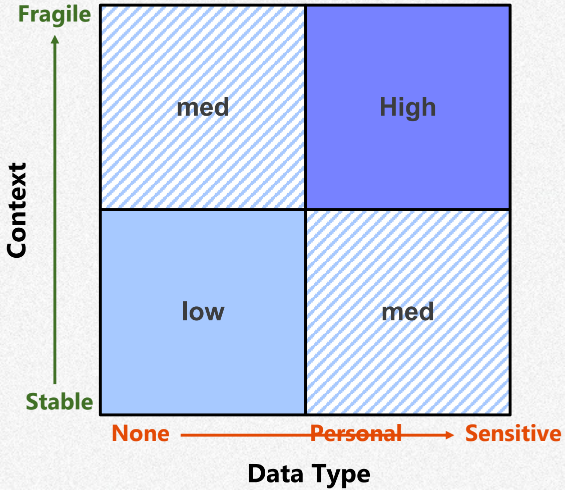
Is the project being implemented in a fragile context?

Does the project share this data with another actor?

Does the project send the data across an international border either to share the data or store it (cloud storage)?

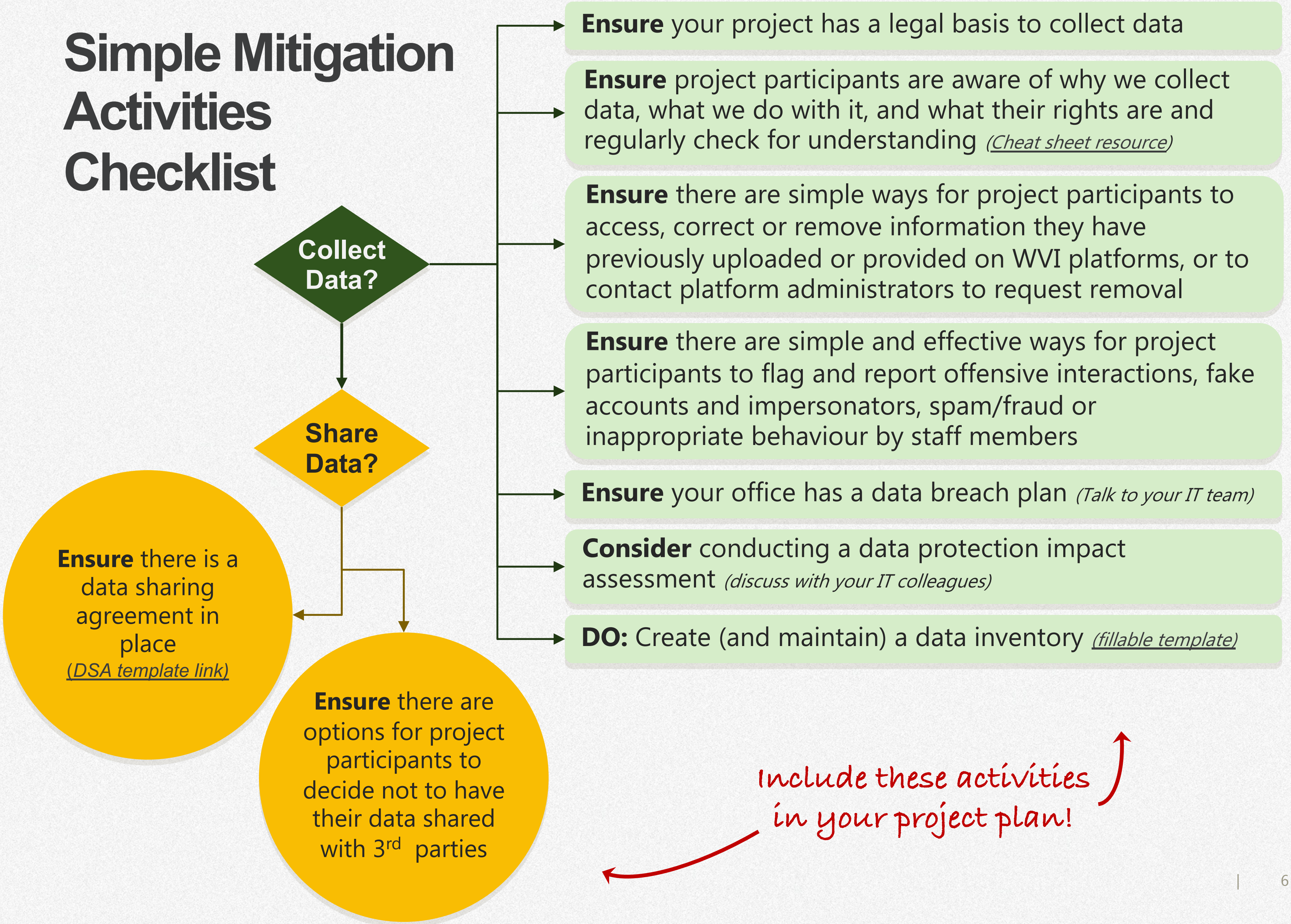
If you answer 'yes' to any of these questions

There is likely risk to be mitigated



med	High
low	med

Simple Mitigation Activities Checklist



Collect Data?

Ensure your project has a legal basis to collect data

Ensure project participants are aware of why we collect data, what we do with it, and what their rights are and regularly check for understanding *(Cheat sheet resource)*

Ensure there are simple ways for project participants to access, correct or remove information they have previously uploaded or provided on WVI platforms, or to contact platform administrators to request removal

Ensure there are simple and effective ways for project participants to flag and report offensive interactions, fake accounts and impersonators, spam/fraud or inappropriate behaviour by staff members

Ensure your office has a data breach plan *(Talk to your IT team)*

Consider conducting a data protection impact assessment *(discuss with your IT colleagues)*

DO: Create (and maintain) a data inventory *(fillable template)*

Share Data?

Ensure there is a data sharing agreement in place (DSA template link)

Ensure there are options for project participants to decide not to have their data shared with 3rd parties

Include these activities in your project plan!

Identify Potential for Harm

Fill in this column!

Risks and harms are not the same thing and need to be considered separately. And while many risks lead to harms, this is not always true. The below table lists common harms and invites you to consider from where the harm would come. Fill it in with your team.

Harms	By Whom?
1. **Physical harms** For example, death, serious bodily injury, forced movement, etc.	
2. **Legal harms** For example, loss of privacy or other fundamental rights, profiling, active persecution, violence, forced movement, repression, etc.	
3. **Economic harms** For example, loss of livelihood, loss of home, loss of other property, financial loss, etc.	
4. **Psychological or emotional harms** For example, distress, depression, emotional instability, etc.	
5. **Social harms** For example, reputational damage, etc.	
6. **Other harms** Identify additional harms not mentioned above, this should include considering harms to individuals and groups (villages)	

Detailed Risk & Mitigation Table (1)

Risks	Mitigation Options
1. Data collected but not used or needed Sometimes the data we collect is not needed for the project we are implementing or is not used. Sometimes we collect this data 'just in case' or to 'help out' a partner (*this is called speculative data collection).* Extra data comes with additional liability (potential for breach, cost of storage, etc) for both the organisation and the beneficiaries, not to mention it is a waste of time and resources for everyone involved.	▪ Create a data inventory for the project to map the data that would be collected and what it would used for. Stop collecting any data that is not being used to implement the project. ▪ Where possible reduce data collection further by exploring if the project objectives can be achieved with less data.
2. Incomplete Data Sometimes we do not collect enough data to fulfil the project objectives. Incomplete data about communities or individuals can lead to representation or selection bias. This occurs when the full target group is not captured, therefore skewing the dataset.	▪ Gather your project team together regularly and ask 'Who is being left out?' Then explore why together and take corrective action ▪ Ensure beneficiaries understand how they can see the data you have about them and how they can correct or update the dataset
3. Poor Quality Data Similar to incomplete data, inaccurate, outdated, or irrelevant data can *cause an incorrect operational decision, create a certain bias, or deprive certain groups (that were not accounted for in the dataset) of critical aid.*	▪ Work with your MEAL team to supplement and correlate your dataset with other ground truth data could also help to enhance the quality of your data and of decisions made based on the analysis of your data. ▪ Ensure beneficiaries understand how they can see the data you have about them and how they can correct or update the dataset
4. Data Scope Creep/Misuse Data used for something other than the purpose for which it was collected is illegal in most data protection regulations as this leads to data ***misuse risk*** *due to* *(a) the actions of team members,* *(b) of third parties who get access in an improper manner and* *(c) third parties who get access in a proper manner through your release, publication and authorized disclosure of your data, results or report.*	▪ Build the digital literacy of staff so they understand what the project data can and cannot be used for ▪ Limit access of project staff to only the parts of the datasets they require to fulfil their tasks ▪ Ensure personal data is held separately from other project data and is encrypted ▪ Ensure robust and detailed data sharing agreements are in place with third parties

Detailed Risk & Mitigation Table (2)

Risks	Mitigation Options
5. Beneficiary Exposure Only in exceptional circumstances for specific projects, should data about religion, ethnicity, sexual assault, or other sensitive aspects be collected. This data is high risk organisationally and for the beneficiary.	▪ Raise beneficiary awareness about what data you are collecting, why, and with whom it will be shared ▪ Discuss with beneficiaries if they have any concerns about the data being collected, how it is used, or with whom it will be shared and then take appropriate action to reduce concerns. ▪ If sensitive personal data is being collected digitally, it must be encrypted and/or pseudonymised and be stored separately from other personal data. (*Talk with your IT team for assistance)* ▪ If sensitive personal data is being collected on paper, it should be stored in a locked drawer or filing cabinet.
6. Data Leakage or Breach Unintentional leakage or unintentional disclosure of either the raw data or of the information/ knowledge resulting from your analysis of the data can occur by *(a) of a member of the project team;* *(b) of known third parties (e.g., government, research partners); who have requested or may have access, or who may be motivated to get access in order to misuse the data and information; or* *(c) by unknown third parties (e.g. due to hackers or other bad actors)*	▪ Personal data should always be stored in encrypted files and devices. ▪ Ensure a data protection impact assessment (DPIA) is conducted by your InfoSec team on any data system the project is using ▪ Ensure staff members have completed the information security awareness and data protection training training (*Talk with your IT team)* ▪ Limit access of project staff to only the parts of the datasets they require to fulfil their tasks ▪ Ensure personal data is held separately from other project data and is encrypted ▪ Ensure the office has a data breach plan that is up to date and known by project staff
7. Re-identification Anonymised datasets can be combined with other datasets to re-identify beneficiaries, which can expose them to harm.	▪ Limit access of project staff to only the parts of the datasets they require to fulfil their tasks ▪ Delete after the purpose for which it was collected has been fulfilled *(Note: it is wise to check the project audit requirements before deleting)*
8. Access Access to data opens up the possibility of harm and increased risk of inappropriate use.	▪ Limit access of project staff to only the parts of the datasets they require to fulfil their tasks ▪ Maintain an access map and monitor access ▪ Establish different levels of access to beneficiaries' personal information and data based on sensitivity of and potential risk related to the data

Detailed Risk & Mitigation Table (3)

Risks	Mitigation Options
9. Legal Basis for Collecting Beneficiary Data Informed consent is one of the most common legal basis organisations can collect data under data protection regulations. However, because of the power differential between the beneficiaries and our organisations, this rarely happens and there is a lack of awareness of why data is being collected. The lack of ***informed*** consent increases organisational risk because data subjects (beneficiaries) can claim not to understand and coercion. Legitimate interest is the other, growing, legal basis for collecting and processing beneficiary data, which comes with its own responsibilities. Regardless of which legal basis is used, ensuring the beneficiary is aware ***and understands*** why we are collecting the data, what we are doing with it, and what their rights are is ***our*** responsibility to ensure.	▪ Conduct awareness raising activities regarding what data you are collecting, why, with whom you are sharing it (and why), and what rights the beneficiaries have. Where appropriate, target vulnerable groups separately (e.g. women, girls, elderly, people living with disabilities, etc.). See here for awareness raising cheat sheet. ▪ Ensure the following (at minimum) is communicated: ○ the period for which their consent is valid ○ how they can manage any consent they have provided ○ any consequences of withdrawing or withholding consent ○ how they can withdraw consent through simple means without undue delay or cost? ▪ Ensure your project offers beneficiaries an alternative enabling them to participate without data capture
10. Location of Data Storage Depending on the digital data collection system you use, if it is using cloud servers or storage at any point, it is likely your data travels outside of the country you are working in. This may violate local data protection regulations	▪ Create a data flow map ▪ Have at least one project staff member that understands local data protection regulation or consult with your legal team ▪ Discuss with IT & legal colleagues, and project management team about the risks and options for data storage. ▪ If necessary, store personal data locally, however be aware this comes with its own risks
11. Algorithms Not understanding the algorithms your data management system or analysis tool uses exposes the organisation to risk.	▪ Identify algorithms being used ▪ Ensure at least one project staff member can explain how they work in a simple way that a 10 year old would understand

Resources & Contacts

Below are key links with more information on the above topics and from which most of the above has been taken.

- https://www.unglobalpulse.org/policy/risk-assessment/
- https://docs.google.com/spreadsheets/d/1qsbegV4uTfXdQKD-YdlpaCYyOabyZiZXn5AaTjsmXSI/edit?pref=2&pli=1#gid=773614129
- https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf
- https://docs.microsoft.com/en-us/azure/architecture/guide/responsible-innovation/harms-modeling/
- https://ethicalos.org/

Assistance:

If you would like more information or assistance with any of the above, kindly contact Amos Doornbos (www.thisisamos.com)

END