(See: Responsible Data for M&E in the African Context)

TIP SHEET 4

Consent

Regardless of the lawful basis for processing data, it is important to be transparent about the data you collect, what you will do with it, who you will share it with, and for how long you plan to keep it. You'll also need to inform people about their data subject rights (see Tip Sheet 2).

To comply with most data privacy laws and to ensure that your data collection is ethical, you must ensure that you have active, informed consent from those whose data you are collecting. When collecting data from or about children, you will need to obtain consent from a parent or guardian. It is a good practice to also obtain a child's 'assent' so that both the child and guardian are clear about the process and have had the opportunity to voice their wishes.

☑ Some key elements to include in your informed consent form are:

☐ **What data is being collected?**
Are you collecting personal or sensitive data? Explain in plain language exactly what kind of data is being collected.

☐ **Who is collecting it?**
Be transparent about who is collecting the data. Include yourself and/or your organisation and any partners involved. You may also want to include the donor that is funding the data collection.

☐ **How the data will be collected?**
Explain how data will be collected. On paper? Digitally? Via an app? Over the phone? It's also a good practice to let data subjects know approximately how long the data collection will take.

☐ **Why is the data being collected?**
Explain why data is being collected and what the anticipated benefits are for the individual or community.

☐ **How will the data be used and by whom?**
Who are the intended users of the data? How will the data be used by the M&E practitioner, the home organisation, any partners, host governments, and/or donors?

☐ **With whom will the data be shared?**
Include all parties with whom you plan to share the data. Are you contractually obligated to share data with a government department or a donor?

☐ **What are the potential negative effects of the data collection?**

Is there any potential harm for individuals or groups if they choose to provide their data? Are there risks related to loss of privacy and confidentiality? If so, these should be explained.

☐ **How long will you retain the personal or sensitive data?**

Note how long you plan to store any personal of sensitive data. Will data be aggregated and retained anonymously or will you retain the raw data?

☐ **What are the individual's or community's rights related to their data?**

Provide a clear explanation of people's data rights as outlined by relevant privacy laws (See Tip sheet 2 for an overview of common data subject rights).

☐ **How can someone contact you/your organisation with questions, concerns, or complaints?**

Provide a phone number, address, and/or an email address where people can contact you or your partners for more information.

☐ **How can someone withdraw consent?**

What is the process for revoking consent or correcting data that is held about an individual?

Other considerations

Storing consent documentation

You must ensure that consent documents are securely stored and are easily accessible for future use in case questions regarding consent are raised or if someone wishes to withdraw their consent.

Re-using data

You must obtain 're-consent' from individuals in cases where you wish to share data subjects' personal or sensitive data with additional partners, retain raw data for longer periods, use data for purposes other than those outlined in the consent form, and in cases where changes have been made to the original consent form.

Community versus individual consent

Even if a local authority or village head has authorised the collection of data in a community, it is still necessary to obtain consent from individuals before collecting their data.

Online or mobile consent

When collecting data digitally, consent is still required. Consent can be obtained via an application or on a mobile device as part of a survey or self-reporting process. Audio consent can also be recorded and stored as proof of consent.