The Tdh Data Protection Starter Guide.

2017.

Terre des hommes
Helping children worldwide.

Produced by
cartong

Part I : Introduction to data protection in the field.

1. Overview.

Terre des hommes (Tdh) teams use data for many purposes: to identify needs and trends, to develop strategies, to plan the efficient and strategic use of resources and to understand whether our programmes have helped to empower and improve the lives of some of the most vulnerable people and communities in the world.

To get these valuable insights, Tdh staff collect, analyse, share and store data every day. But data can also cause harm, for example if it is lost, or if it gets into the wrong hands. Tdh staff – i.e. you – have a responsibility to protect the data that we have been entrusted with. The Terre des hommes Data Protection Starter Kit will help you collect and manage data responsibly.

01	02	03
Part I is an **introduction to data protection** and helps you **identify and understand your risks.**	Part II is filled with **practical tutorials** that demonstrate step by step how you can better protect data.	Part III contains a set of **Standard Operating Procedures** (SOPs) templates to help field offices implement structural changes that improve data management and data protection.

This document is mainly written for Tdh field staff who are involved in collecting or working with data that has been obtained directly from people or communities whom we are supporting with our programmes. This guide does not focus on other data sources, such as call data records or other meta-data, that can be obtained through third parties.

Also, since this guide is written for staff working in more than 30 countries, it cannot be a legal reference document, as more than 100 countries have their own data protection laws and regulations. However, by following the good practices and tips described in this toolkit, you will be on a good path to fulfil your legal data protection obligations and to prevent harm from those we seek to serve.

In parallel with this starter kit for the field, Tdh headquarters in Switzerland is working on a separate organisation-wide policy document to ensure that Tdh complies with the EU General Data Protection Regulation, which will come into effect in May 2018.

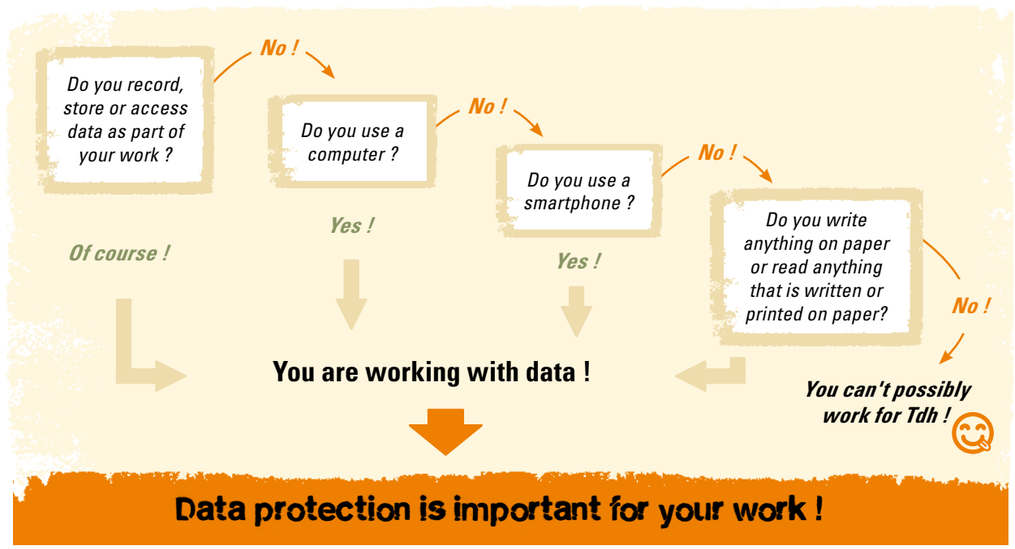


Figure 1 Adapted from "The Responsible Data Handbook".

2. Why data protection is important.

Everything that is written down on paper or saved in a digital file is data. For example: the handwritten notes from an interview with an unaccompanied girl, a digital photo of a boy on your camera, or a printed map that shows communities where Tdh is planning to build latrines.

We need and rely on data, but the loss, corruption, illegitimate use, unauthorized distribution and even the collection of data can sometimes be harmful for beneficiaries, the organisation or staff.

Three examples:

Harmful for beneficiaries: A 14-year-old girl has been raped while fleeing a conflict area. She got pregnant and delivered the child. The girl and her family have received assistance from Tdh. As part of a monitoring and evaluation mission in the programme area, a Tdh staff member visits the girl and asks her multiple questions about what has happened to her and when. The girl relives the experience and is re-traumatized.

Harmful for staff: Someone who doesn't know Tdh notices that your digital camera is full of photos of children. He has heard a rumour that children have been adopted by foreigners. He quickly organizes a group of people who threaten you and chase you out of the village.

Harmful for the organisation: While in the field, you lose a map that shows the location of villages where Tdh is planning to build latrines. You don't know the area and have to drive back to the office to print the map again. You lose a whole day of work and miss a meeting with a village elder that had been scheduled for that day. This decreases the trust that the village elder has in Tdh.

While many of these risks have been present in the humanitarian field for many years, data protection has recently become more important. This is partly due to legal obligations: more than half of all countries in the world have data protection laws. More importantly, data protection has become an issue because the likelihood of data being misused has increased.

Civil Society Organizations working with Tibetans for example report that they experience frequent attacks on their IT systems[1]. In addition, UNOCHA reported that Syrian refugees living in Lebanon were concerned that biometric registration data could be shared with the Syrian government[2]. Last but not least, data is lost every day through computer viruses or carelessness.

The best way to reduce the risk of data causing harm is by not collecting it in the first place. To protect people from being harmed, Tdh staff should therefore only collect necessary data, for which they have a concrete and specific use. In addition, robust data protection procedures can further help reduce the likelihood of incidents like the ones described above and can mitigate the impact, if an incident occurs.

3. Roles and responsibilities within the delegation.

Everyone is responsible to help protect the data that Tdh has been entrusted with, but the concrete responsibilities depend on each team member's function. The following is an outline of what these responsibilities can be in a delegation, however this will vary depending on the setup and the resources in each country.

Management.

Country office representative:

√ is accountable for the overall process, making sure that risks are analyzed and mitigation measures are taken within her/his area of operations. S/he ensures that all teams receive the adequate information and are aware of the tools, Standard Operation Procedures, etc.

√ negotiates non-disclosure agreements with partners where necessary.

√ is responsible for appointing a focal point in charge of data protection issues. Depending on the set-up of the delegation this could be:

- the information management (IM) officer / manager.
- the monitoring and evaluation (M&E) officer / manager.
- the programme coordinator.
- the IT manager.
- the deputy representative.

Programme staff.

Programme coordinator:

√ initiates, coordinates and oversees the data protection risk analysis with the support of IT / quality and accountability (Q&A) staff (IM, M&E, Q&A coordinator) and project staff.

√ ensures that partners are aware of Tdh data protection requirements.

Project managers / officers:

√ ensure that their project is analyzed for data protection risks and that mitigation measures are being defined and implemented.

√ report any questions and concerns to the relevant personnel; request assistance from support staff or programme coordinators.

√ monitors whether partners are compliant with Tdh data protection requirements.

Support departments / staff.

Quality and accountability staff:

√ contribute to the data protection risk analysis by offering technical and methodological support to programme teams.

√ ensure that any monitoring plan includes an analysis of the information management system including a reflection on data protection.

√ deliver ethical, methodological (M&E) and technical (IM) support and ensure that data protection is dealt with in the framework of the M&E plans.

√ ensure that data protection and the "Do No Harm" principle are mainstreamed in any M&E process that involves the collection, processing, use or sharing of data.

IT staff:

√ support programme teams on request and report any questions / inconsistencies.

√ alert programme teams if any risks are detected and suggest solutions.

HR staff:

√ ensure that data protection is included in the induction package for new staff.

Examples.

The following is a mix of examples related to data protection issues from the field, including suggestions on how these situations could have been avoided. Some of these examples have actually happened, others could plausibly happen.

The role you can play to ensure that data is protected adequately depends on your role in Tdh.

1

What happened?

A computer crashes that contains the files of 143 children and their families.

There is no back up.

What is the harm?

The data has to be recreated. Tdh staff spend weeks recreating the files.

In the meantime, programme activities are at on hold since it's no longer clear what should be done where and for whom.

Beneficiaries are annoyed by the questions and the delays and start to doubt whether they can trust Tdh.

A donor is annoyed because his money is not being spent as quickly as agreed.

In the end, Tdh staff are only able to find 135 of the children, the information for the remaining 8 remains lost.

What could have been done differently and by whom?

√ **Data protection focal point:** ensure that a backup plan is in place and followed.

√ **Programme manager / IT:** perform regular, incremental backups on an encrypted external hard drive that is stored in the office safe. Ensure that an appropriate password management procedure is in place for the encrypted files so that the password cannot be lost or guessed. Send copies of hard drive to the country office on a regular basis.

2

What happened?

A partner organization shares the names and locations of 50 children who are at risk of trafficking by email to a large group of people.

One of the recipients shares the information with a criminal group.

What is the harm?

The criminal group makes contact with many of the children, five of whom disappear.

What could have been done differently and by whom?

√ **Country rep / data protection focal point / programme manager:** Require partner organizations to follow responsible data sharing practices such as limiting the number of recipients of sensitive data. Discuss options to anonymize data where possible.

[1] *See: "Communities @ Risk - Targeted Digital Threats Against Civil Society"; Accessed: 13 October 2017*
[2] *UNOCHA, "Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies", p. 9; Accessed: 13 October 2017*

3.

What happened?

A programme coordinator shares a report about girls being abused by soldiers in a village with his counterparts in other organisations.

The report contains a link to a Dropbox folder with sensitive personal information that can now be accessed by anyone with the link.

What is the harm?

The report is being shared further and finally reaches a high-ranking member of the army.

Soldiers then go back to the village and intimidate the girls who have reported the abuse.

The villagers no longer want to speak with or trust Tdh.

What could have been done differently and by whom?

√ **Data protection focal point / programme coordinator:** Define clear SOPs that regulate who can have access to what kind of information and how it can be shared.

√ **Programme coordinator / programme manager / Q&A:** Restrict who has access to personal data and for which purposes. If you use a shared drive like Google Drive / One Drive, give access only to named users.

4.

What happened?

The printed and signed attendance sheet of a HIV/AIDS awareness training is accidentally left at the hotel where the training took place.

A hotel employee shares the list with a member of the government's health ministry.

What is the harm?

All male participants of the training are being detained on the suspicion of homosexuality, which is illegal in this country.

The detainees have to submit to anal exams at the hospital.

What could have been done differently and by whom?

√ **Programme manager / Q&A:** Evaluate whether an attendance sheet is necessary for this event.

5.

What happened?

Hard copies of all case management files are kept in a secure locker. However, local staff export information from the database to their personal USB drives and laptops when going to the field.

One day an employee quits. The data is still on his computer.

What is the harm?

Given that the staff were working in a cross border operation, the data, which included addresses and nationalities, could have been used to identify refugee families and put pressure on them.

What could have been done differently and by whom?

√ **Headquarters:** Provide a budget to ensure that relevant local staff have laptops.

√ **Programme coordinator / country rep / Q&A:** Define who has access to the database and for what purposes. Define a policy about the use of personal electronic devices for work and share with all staff.

√ **Field office:** Explicitly ask employees during exit interviews for any Tdh data in their possession.

6.

What happened?

A staff member receives an email with an attachment. The attachment contains the WannaCry virus that locks and encrypts the hard disk.

A message appears on the screen, saying the user has seven days to pay several hundred dollars to release the data, else the data will be deleted.

What is the harm?

Tdh does not pay the criminals and all data on the computer is lost.

What could have been done differently and by whom?

√ **IT:** Ensure that virus protection is up to date on all computers.

√ **Programme manager / IT:** perform regular, incremental backups on an encrypted external hard drive that is stored in the office safe. Ensure that an appropriate password management procedure is in place for the encrypted files so that the password cannot be lost or guessed. Send copies of hard drive to the country office on a regular basis.

4. Key terms and Concepts.

Tdh is committed to using data responsibly to uphold the rights of the individuals, groups and organizations with whom we work. This Data Protection Starter Kit provides you with many practical tools to help you live up to this commitment in your day to day work. Here are some key terms and concepts that you should know before using it:

Responsible data use is :
"the duty to ensure people's rights to consent, privacy, security and ownership around the information processes of collection, analysis, storage, presentation and reuse of data, while respecting the values of transparency and openness."[3]
This means that good data management policies and practices do not only seek to avert harm, but also try to empower the people who are at the core of the data by establishing feedback loops.

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

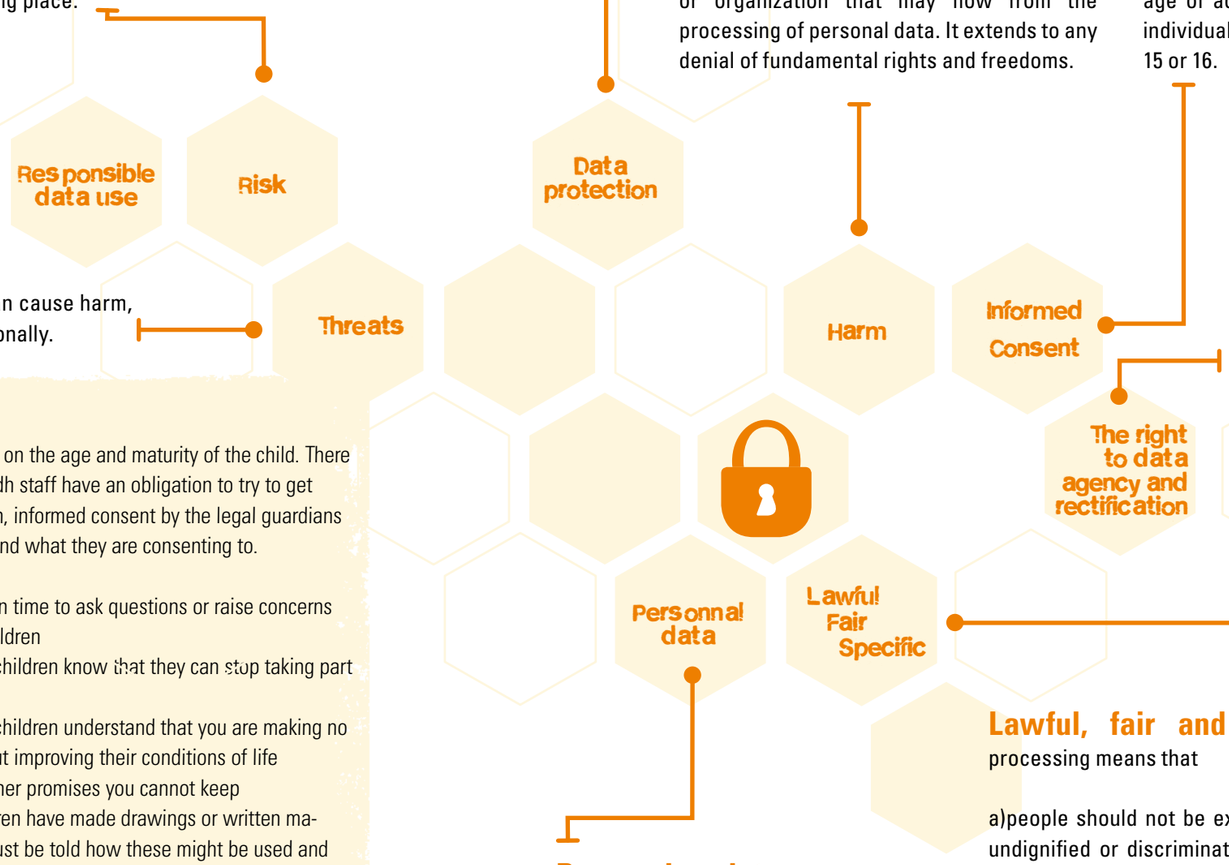
Threats are anything that can cause harm, either intentionally or unintentionally.

Data protection is all processes, practices and systems that are used to safeguard information from being lost, corrupted or accessed by unauthorized parties.

Harm signifies 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.

Informed consent must be given explicitly to collect data and must be specific for the purposes the data is used for. Consent for children must be given by the child's parent or legal guardian.

In cases where secondary uses of the data are anticipated, these need to be explained to the person giving the information. It is also advisable to check what the national age of adulthood is, since in some contexts individuals are considered adults at the age of 15 or 16.



The right to data agency and rectification describes the right of everyone to have control over the collection, use and disclosure of their information. This includes an individual's right to get access to their own information and to correct information that is inaccurate[4].

Personal data is any information relating to an individual that can help identify them either directly (e.g. first and last name or a unique registration number) or indirectly by combining different data sources.

Lawful, fair and specific data collection and processing means that

a)people should not be exposed to rights violations, harm, or undignified or discriminatory treatment as a consequence of personal data collection and processing. This includes the duty to get informed consent from the people you are collecting data from. It also means that refusing to give data should not result in negative consequences for the individual.

b)you should only collect data that is necessary for a specified purpose and delete it if no longer necessary for that purpose[5].

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

[3] *Responsible Data Forum, working definition, September 2014; https://responsibledata.io/about/ Accessed: 28 August 2017*

[4] *The Signal Code: A Human Rights Approach to Information During Crisis" by Signal Program on Human Security and Technology at the Harvard Humanitarian Initiative; Accessed: 28 August 2017*

[5] *Adapted from Conducting Mobile Surveys Responsibly: A Field Book for WFP Staff, May 2017" and "How to Do A Privacy Impact Assessment", Privacy Commissioner of New Zealand; Accessed: 28 August 2017*

Moldavie. © Tdh / François Struzik

Siège | Hauptsitz | Sede | Headquarters
Avenue de Montchoisi 15, CH-1006 Lausanne
T +41 58 611 06 66, F +41 58 611 06 77
E-Mail: info@tdh.ch, CCP / PCK: 10-11504-8

Terre des hommes
Aide à l'enfance. tdh.ch
cartong

Produced by
cartong