Data Protection Self-Assessment: Understanding Threats, Harms and Risks.

As part of the data protection self-assessment tool, we ask you to describe the threats, harms and risks that can potentially occur when you collect, use or process data. In everyday speech we often use these terms interchangeably, which is why we have created this little handout.

➡ *A **risk** describes the **likelihood** and the **impact** of a **harmful threat** occurring.*

Threats.

Threats are anything that can potentially cause harm, either intentionally or unintentionally. This includes losing data, sharing data with unauthorized parties or collecting/using data without permission. Below you find a list of potential data protection threats that are also used in the self-assessment tool.

- **Unjustifiable or excessive collection of data.** *Example: data about marital status of parents is collected in a project that focuses on child nutrition.*
- **Inappropriate use of data:**
    - Unreasonable use. *Example: Data is used to target aid by marriage status instead of need.*
    - Unauthorised use. *Example: Beneficiaries allowed photos to be taken when TdH registered their children. These photos are now used for a marketing campaign without explicit consent of the parents or the child.*
    - Inaccurate or outdated data is stored or used. *Example: Age is entered wrong, making some children ineligible for assistance.*
- **Security issues.**
    - Data is lost. *Examples: A USB stick with data is lost in a taxi or the hard drive of a computer crashes.*
    - Data is stolen. Where lost data gets into the wrong hands by accident, stolen data is intentionally copied or removed by someone with criminal intent.
    - Data is unjustifiably accessed, transferred, shared or published. Data gets into the hands of unauthorized persons. However, unlike with stolen data, there is no criminal intent in this case. *Example: Data is emailed to people who should not have access to it or a password is shared too widely.*

Example:

Over the last year, armed groups have repeatedly taken laptops from NGO workers in our area of operation. This will probably continue to happen. Some of the data that we record includes mentions of abuses through these armed groups. Since our laptops are not encrypted, our data could be used to target individuals based on their names. This could have deadly consequences for them. This is a high risk.

Threat = Security Issue; data is stolen by armed groups.
Harm = Individuals mentioned in the data could be targeted and killed.
Likelihood = Likely, since it has occurred several times in the past and the situation has not changed.
Impact = Critical, since it can result in someone's death.
Seriousness = High, because it is likely and the impact is critical.

Harm.

Harm signifies any damage, injury or negative impact - whether tangible, intangible or economic - that can be a result of the processing of data. It includes any denial of fundamental rights and freedoms. Harm can affect individuals, groups of people or organizations. More than one harm may be caused by a single threat. Common forms of harm:

- **Tangible** harm may include: Bodily harm, loss of liberty or freedom of movement, damage to persons or property, other tangible harm.
- **Psychological** harm may include: Embarrassment/anxiety, (re)traumatisation, other psychological harm.
- **Social** harm may include: Discrimination/stigma, loss of trust, legal persecution, other social harm.
- **Economic** harm may include: Financial loss, loss of economic opportunities, other economic harm.

Examples: Being stigmatised by neighbours is a form of social harm. Being beaten up is tangible harm. For someone living in a village, being chased from that village is tangible (loss of shelter), economic (loss of assets and probably loss of economic opportunities) as well as social.

Risks.

Risks are the intersection of harm and threat and describe the likelihood and impact of a harmful event (threat) occurring. In the self-assessment tool we ask you to estimate the likelihood and impact of potential risks on a scale of 1 to 5. Below are some criteria that can help you choose values. Based on the rating, you can then calculate the seriousness of a risk (from low to high) by multiplying these two values. The online version does that automatically for you, in the paper version, you will have to multiply the values manually.

Depending on whether a risk is low, medium or high, you will find suggestions below at which level within the organization the risk should be addressed.

Likelihood.

Very unlikely = 1.
Remote chance of happening. Up to 20% within the next year and/or has occurred very infrequently, if ever, in the past.

Unlikely = 2.
Low chance of taking place; between 20% and 40% within the next year.

Moderately likely = 3.
Moderate chance of happening. 40%-60% chance of occurring within the next year or has occurred a few times in the past.

Likely = 4.
Will probably happen in the next year with a likelihood of 60% to 80%. Has occurred several times in the past.

Very likely = 5.
Will happen with a likelihood of 80% or more over the next year or has occurred frequently in the past.

Impact.

Negligible = 1.
Harm can easily and quickly be repaired by the affected without significant efforts.

Minor = 2.
Up to 5% of tangible assets are lost. In case of physical or social harm, the affected will be able to recover fully within a short time.

Moderate = 3.
Damage or loss of up to 20% of assets or physical harm that will require professional treatment. Self-recovery is possible but challenging over time.

Severe = 4.
Up to 50% loss of tangible assets, major injuries or damage to social standing that will take several years to recover from. Full recovery might not be possible without assistance.

Critical = 5.
Catastrophic effect on the life of the affected, such as death or long-term loss of liberty. Loss of more than 50% of tangible assets or other damage that the affected cannot recover from.

Seriousness *(calculated automatically).*

The online version of the tool calculates the seriousness automatically. To calculate the seriousness of the risk in the paper version, multiply the value for likelihood with the value for impact. *For example: "Unlikely" (2) x "Severe" (4) = 8 (medium risk).*

Low risks = 1-6.
Can be addressed with routine procedures by individual team members and programme managers.

Medium risks = 8-12.
Concrete and comprehensive measures to mitigate risks need to be implemented within a specified time period. Implementation has to be monitored by line-managers.

High risks = 15-25.
Immediate action is required. Senior country office leadership and/or HQ need to be informed of risks and mitigation measures.