**Basic rules of data protection**

1. **Introduction**

Ethical considerations are essential to any form of data collection in a humanitarian operation, mainly in conflict settings and complex emergencies. Collecting and sharing information for any purpose, including monitoring, reporting, assessments or surveys, can put people at risk not only because of the sensitive nature of the information collected - also because simply participating in the process may cause people to be targeted. The risks can range from physical violence to social marginalisation and are often unknown to the individual soliciting the information. Humanitarian organisations involved in information collection and sharing are obligated to protect the rights of individuals and groups involved in this process as participants.

Data protection and its proper implementation are complex matters that always also depend very much on the working context. Increasing digitalisation of processes creates new challenges that all organisations are facing during implementation. The GRC *CTP Checklist* refers to some technical resources that might be helpful while setting up individual data protection policies for your programme.

The following summerises basic principles of data protection and gives easy to apply recommendations for basic measures of data protection. One very essential thought should guide your implementation design and your considerations in regard to data protection: “***What if it was me? How do I want my own data and information to be handled?”***

1. **Principles of data protection[[1]](#footnote-1)**

### Respect

Organisations should respect the privacy of beneficiaries and recognize that obtaining and processing their personal data represents a potential threat to that privacy.

### Protect by design

Organisations should ‘protect by design’ the personal data they obtain from beneficiaries either for their own use, or for use by third parties, for each cash or e-transfer programme they initiate or implement.

### Understand data flows and risks

Organisations should analyse, document and understand the flow of beneficiary data for each cash or e-transfer programme they initiate or implement within their own organizations and between their organizations and others and develop risk mitigation strategies which might be required to address any risks arising from these flows.

### Quality and accuracy

Organisations should ensure the accuracy of the personal data they collect, store and use, including by keeping information up to date, relevant and not excessive in relation to the purpose for which they are processed, and by not keeping data for longer than is necessary.

### Obtain consent or inform beneficiaries about the use of their data

At the point of data capture, beneficiaries should be informed as to the nature of the data being collected, with whom it will be shared and who is responsible for the secure use of their data, and be provided with the opportunity to question the use made of the data and withdraw from the programme should they wish that their personal data is not used for the purposes described.

### Security

Organisations should implement appropriate technical and operational security standards for each stage of the collection, transfer and use of beneficiary data to prevent unauthorized access, disclosure or loss, and, in particular, any external threats should be identified, and actions taken to mitigate any risks arising.

### Disposal

Organisations should not hold beneficiary data for longer than is required unless they have clear, justifiable and documented reasons for doing so; otherwise, data held by the organization and any relevant third parties should be destroyed.

### Accountability

Organisations should establish mechanisms whereby a beneficiary can request information about what personal data an organisation holds about them and mechanisms to receive and respond to any complaints or concerns beneficiaries may have about the use of their personal data.

1. **Basic rules for better data protection[[2]](#footnote-2)**

**3.1 The purpose of data protection**

In general two terms have to be differentiated - although their impact is overlapping: **data protection** considers information about an individual directly. **Data security** refers to all hard- and software (and other IT) that holds information about individuals and organisations. Therefore, the purpose of data protection is to fulfill the basic right of informational self-determination and privacy. Data security protects basically the IT holding private and organisational information.

The measures to reach both go hand in hand; nevertheless, it is important to differentiate to understand the danger of wrong practice. To protect our beneficiaries’ and eventually our organisational privacy and data we must apply thoughtful data protection **AND** data security measures according to outlined principles above.

**Important Note: As soon as data is transmitted to GRC HQ German data protection law (Bundesdatenschutzgesetz BDSG) applies!**

* 1. **Data Security**
* measures to be considered include maintaining in first **physical security** by having servers and computer hardware and other peripherals in a secure location with strict access control. Offices and other work spaces shall be locked once left unattended, mobile devices like laptops and tablets locked in safely after working hours. All assets should be clearly tagged as part of GRC inventory (or HNS if applicable). Your general office security (guards, alarm systems, etc.) is part of your data security!
* **reduce your computer’s vulnerability** to hackers and malware, such as viruses, Trojans and spyware by installing anti-virus / cybersecurity software. Update it regularly!
* Always secure your technical devices with **passwords** (including data carriers, mobile phones)! Passwords are often the first, and sometimes the only, barrier between information and anyone or anything that might want to read, modify, or destroy it without permission. Change your password frequently.
* Never leave your mobile phone (and other relevant devices) **unattended**
* **avoid exchanging sensitive information** via messengers like Whats App and Skype.
* **limit the staff with full access** to administration profiles, soft- and hardware. Establish clear responsibilities and protocols (e.g. handover of hard drives after End of Mission, etc.).
* **data carriers** (USB, CDs, Laptops, PAPER!) holding sensitive information need to be stored in lockable drawers/shelves. Access to this location should be limited. During handovers etc. the receipts of data carriers shall be protocolled (similar to e.g.cash boxes). In case data carriers shall be disposed make sure to contact either local IT or GRC HQ for instructions.
* **Paper** – make sure to avoid unnecessary copies and scans! Sensitive data needs to be locked! Old paper files holding sensitive data (even if only remotely) **need to be shredded without exception**.
* If you receive data carriers from third parties always **run a virus-check**.
	1. **Data Protection / Data Sharing**
* Make sure to collect **only the beneficiary information actually needed**! Assess whether personally identifiable information (PII) must be part of the data set and when/how they can be disposed.
* If in depth assessments etc. result in aggregated data collection make sure that you plan IN ADVANCE how and where you want to store them. Plan in detail who has access, where and with whom you want to share etc.
* In case beneficiary information is shared make sure a ***data sharing protocol*** (who will share what, when, why and how?) is not only in place but also understood and applied by your team.
* Ensure **encryption of sensitive information** on your device (usually built-in operating system), for individual files (7-Zip, WinZip) or “virtual” disks (VeryCrypt)
* **Be aware of governmental policies or similar** (formally and informally) in place that might contradict your data protection set up. Seek legal advice when needed.
* If the **collection of biometric data** (fingerprint, iris scan, face recognition) is considered it is mandatory that this data set is handled with the utmost thoughtfulness and professionalism. Don’t jump on seemingly more efficient technologies when you cannot **ensure that the right to privacy and protection (mainly in conflict zones and refugee/IDP settings) of your programmes’ beneficiaries and partners!**
* **Avoid using public networks and hotspots** with your working devices in particular for data sharing
* Ensure your office **WLAN/LAN connection is secured sufficiently** and update passwords and access permissions regularly
* **Conduct a PIA** (Privacy Impact Assessment, **see 3.5. CaLP model**) for your programme design. Ensure that your counterparts at HNS/partners are involved.

* [ELAN (Electronic Cash Transfer Learning and Action Network)](http://www.cashlearning.org/news-and-events/news-and-events/post/399-introducing-the-elan-data-starter-kit) launched a **Data Starter Kit** which will help you drafting your individual data protection policy for your programme. The seven tip sheets build on CaLP’s *Protecting Beneficiary Privacy* and give practical advice regarding Privacy Impact Assessments (PIA), Data Minimisation, Know Your Customer Regulations (KYC), Registration, Encryption, Data Sharing and Data Retention/Archiving/Disposal.
	1. **Beneficiary Note and Consent**

It is our responsibility that all beneficiaries know exactly about the purpose of potential data collection and usage. Make sure the following explanations[[3]](#footnote-3) are given in local and easily understandable language:

* Why is the data collected and what is it being used for?
* How long will the data be kept for (consider also storage outside the country, e.g. HQ Finance?
* Whom the data will be shared with and the circumstances thereof?
* Explanation of how GRC (and HNS) protect the data
* Rights of the beneficiaries regarding their data
	1. **Privacy Impact Assessment (PIA) / CaLP model[[4]](#footnote-4)**

In the heat of setting up a new project/programme doing an additional assessment on a rather abstract topic seems little appealing in general. But - once familiar with the tool as such, a PIA will not only be an eye opener but also help you to improve GRC’S programming for the sake of our beneficiaries’ basic rights and dignity.

A Privacy Impact Assessment looks into an organisation’s procedures and technologies to analyse how personal information is collected, used, disseminated, and maintained. It is designed to ensure an organisation incorporates privacy into the development, design and deployment of a technology or policy.Rather than merely being an assessment and report of whether an organisation has adhered to principles, the PIA is in itself part of a process that enables organisations to consider the likely implications of new technologies, techniques, and policies so that it can foresee the risks, determine likely problems, and initiate the process of negotiating solutions before they become too complex.[[5]](#footnote-5)

**Example: PIA for humanitarian interventions (can be adapted based on context)**

**1 Information**

* What information is collected, used, disseminated, or maintained in the system?
* What are the sources of the information?
* Why is the information being collected, used, disseminated, or maintained?
* How is the information collected?
* How will the information be checked for accuracy?
* What specific legal authorities, arrangements, and/or agreements defined the collection of information?

***Privacy Impact Analysis****: Given the amount and type of data collected, discuss the privacy risks identified and how they have been mitigated.*

**2 Uses**

* Describe all uses of the information.
* What types of tools are used to analyse the data and what type of data may be produced?
* If the system uses commercial or publicly available data, please explain why and how it is used.

***Privacy Impact Analysis:*** *Describe any types of controls that may be in place to ensure that information is handled in accordance with the above-described uses.*

**3 Retention**

* How long is information retained?
* Has the retention period been approved?

***Privacy Impact Analysis:*** *Discuss the risks associated with the length of time data is retained and how those risks have been mitigated.*

**4 Internal Sharing and Disclosure**

* With which internal organisation(s) is the information shared, what information is shared and for what purpose?
* How is the information transmitted or disclosed?

***Privacy Impact Analysis****: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they have been mitigated.*

**5 External Sharing and Disclosure**

* With which external organisation(s) is the information shared, what information is shared, and for what purpose?
* Is the sharing of personally identifiable information outside the organisation compatible with the original collection?
* If so, is it covered by an appropriate policy and notice statement?
* How is the information shared outside the organisation and what security measures safeguard its transmission?

***Privacy Impact Analysis****: Given the external sharing, explain the privacy risks identified and describe how they have been mitigated.*

1. **Notice**
* Was notice provided to the individual prior to the collection of information?
* Do individuals have the opportunity and/or right to decline to provide information?
* Do individuals have the right to consent to particular uses of the information? If so, how does an individual exercise that right?

***Privacy Impact Analysis:*** *Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.*

1. **Access, Redress and Correction**
* What are the procedures that allow individuals to gain access to their own information?
* What are the procedures for correcting inaccurate or erroneous information?
* How are individuals notified of the procedures for correcting their information?
* If no formal redress is provided, what alternatives are available to the individual?

***Privacy Impact Analysis****: Discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.*

**8 Technical Access and Security**

* What procedures are in place to determine which users may access the system and are they documented?
* Will organisational contractors have access to the system?
* Describe what privacy training is provided to users either generally or specifically relevant to the programme or system?
* What auditing measures and technical safeguards are in place to prevent misuse of data?

***Privacy Impact Analysis:*** *Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?*

**9 Technology**

* Does the project employ technology which may raise privacy concerns? If so please discuss its risks and mitigations. Consult IT experts/service providers if needed.

***Privacy Impact Analysis:*** *What risks result from the use of applied technologies? How can they be addressed and mitigated? Can specific expertise be mobilised in case of problems?*

**A little storytelling at the end: Did you know that the death of Osama bin Laden in 2011 was linked to the work of an aid agency?**

What sounds like a Hollywood blockbuster became bitter reality for Save the Children in Pakistan in 2011. The organisation was confronted with an unbelievable accusation: DNA and data collected during a putative vaccination campaign in Pakistan was compared with a sample from bin Laden’s sister, who died in Boston in 2010, to provide evidence that the family was present in a small city 50 km northeast of Islamabad. The Pakistani Doctor Shakil Afridi, who liaised with the CIA on that matter, claimed to work for Save the Children after his activities were linked to the military “*Operation Neptune’s Spear*” by the Pakistani Secret Service. Although Save the Children could proof that neither Dr. Afridi ever worked for them, nor they did run a vaccination campaign in that area, the organisation’s set up in Pakistan was shaken up tremendously. International staff was evacuated immediately, all operations were temporarily suspended – leave alone the damaged reputation.

For sure, the example is extreme and bin Laden not an “average” beneficiary; still it shows that collected data and information can be used in any unintended way.

1. CaLP (2013): Protecting Beneficiary Privacy: Principles and operational standards for the secure use of
personal data in cash and e-transfer programmes [↑](#footnote-ref-1)
2. German Red Cross (2009): Datenschutz und Datensicherheit; Datenschutzhandbuch Version 05 [↑](#footnote-ref-2)
3. http://www.cashlearning.org/resources/library/389-protecting-beneficiary-privacy-principles-and-operational-standards-for-the-secure-use-of-personal-data-in-cash-and-e-transfer-programmes [↑](#footnote-ref-3)
4. This Model PIA is adapted from the PIA developed by the U.S. Department of Homeland Security (DHS). For many years, the DHS has conducted PIAs for all new technologies and rules. In fact, this process is considered to be inherently necessary for all U.S. Federal Government programmes since 2002, as required by the E-Government Act of 2002. [↑](#footnote-ref-4)
5. http://www.cashlearning.org/resources/library/389-protecting-beneficiary-privacy-principles-and-operational-standards-for-the-secure-use-of-personal-data-in-cash-and-e-transfer-programmes [↑](#footnote-ref-5)