TIP SHEET 2
DATA MINIMIZATION

elan
The Electronic Cash Transfer Learning Action Network

WHAT IS DATA MINIMIZATION?

Data minimization is a privacy principle that requires the people collecting data to be intentional about what type of data is collected and how long it is retained. To meet this principle, teams should limit data collection to what is directly relevant and necessary to accomplish a specified purpose. In practice, this means assessing whether personally identifiable information (PII) must be a part of a data set and how long to keep data before disposing of it. Data minimization also refers to de-identification practices in which PII is stripped out of data sets before they are shared with others or made accessible to the public.

Data minimization applies to most program phases. Collecting the minimum amount of data, sharing only with those who need it, and keeping data only as long as necessary has clear privacy advantages; the less you have and the quicker you dispose of it, the less likely data can be inadvertently disclosed. But data minimization also has financial advantages; organizations spend less time and money collecting unnecessary data, cleaning it up once collected, and storing and archiving excess data.

Programs should strive to maintain a balance between responsibly minimizing data, while ensuring that data collection meets program needs.

Regulations and guidelines

There are few legal regulations that govern what type and quantity of data you can collect, but there are guidelines which can assist in making decisions related to data minimization.

One, the *OECD Privacy Principles*, states:

> *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*

Another, the *Fair Information Practices Principles*, (FIPPS) states that:

> *Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).*

Data minimization is also addressed under the Cash Learning Partnership (CaLP) Principles and Operational Standards:

Principle 4: *Organizations 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 it is processed, and by not keeping data for longer than is necessary.*

Principle 7: *Organizations 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.*

WHAT HUMANITARIANS NEED TO KNOW:

Understand what constitutes PII

To minimize the collection of PII, it is important to understand exactly what it is. Simply put, PII is, "Any data that directly or indirectly identifies or can be used to identify a living individual." Names, phone numbers, bank record details, and biometric data (such as fingerprints or iris scanning) are all common examples of PII. However, PII can also be any combination of data sets (sometimes seemingly innocuous ones) that would allow someone to

identify an individual. Since e-transfers are typically distributed to an individual or household, e-transfer programs tend to require PII to be able to target assistance and ensure assistance is received by the correct participant.

Consider the privacy rights of your program participants

Emerging technologies are revolutionizing the way humanitarians can collect, collate and communicate data. While these changes can positively impact planning and program efficiency, it is essential to evaluate whether data is being collected with a view to the privacy rights of program participants. *(See PIA and Registration Tip Sheets for more information).* Possible questions to ask when collecting data are:

- Have you clearly explained how the data will be used and requested program participants' consent?
- If it is not possible to get consent, what have you done to protect participants' data privacy rights?
- Do participants know who will have access to their data?
- Do participants have access to their data, and can they change their minds about giving you access to you later in the program?

Why practice data minimization?

Risk to individuals: The risks of not adequately thinking through data minimization are serious, particularly because of the conditions that individuals and communities face in humanitarian situations. Be realistic. Data breaches happen, and collecting excessive PII increases the chances those breaches will cause harm. Data breaches can have many negative consequences for individuals, such as denial of services or freedoms, fraud and identity theft.

Reputational risk: The use of digital data gathering (DDG) solutions in humanitarian programs is increasing, including biometrics for registration and verification. Much of this technology was not designed for the humanitarian sector. Instead, it was adopted from sectors and not necessarily developed with the communities in which we work in mind. In addition to potential harms to data subjects, privacy breaches and insider leaks can be damaging to the reputation of a humanitarian organization. Practicing data minimization and access minimization (minimizing the number of people with access to sensitive data) mitigates the risk of this happening.

Time and cost-efficiency: Collecting only necessary data minimizes time spent by program participants, collectors, data cleaners, and processors. Conducting a proper assessment of what kind of data you need to collect, who will access it, and how long it should be kept will increase your program's data security. It will also increase your ability to share data later on, if necessary. *(See the PIA and the Data Sharing Tip Sheets for more information.)*

WHAT HUMANITARIANS CAN DO:

While it is tempting to collect as much data as possible in the off-chance that you might need it later, you should resist this temptation. Particularly for humanitarians working with vulnerable groups, there are risks associated with collecting unnecessary data. To meet the principle of data minimization, use the other Tip Sheets in this Starter Kit to help you determine your scope of data collection and retention.

- **Responsible data collection and use:** Think about what data you need for the project (and collect only that information). *(See PIA and Registration Tip Sheets for more information).*
- **Responsible observance of data regulations:** Think about the host country data laws. *(See KYC Tip Sheet for more information.)*
- **Responsible data access and sharing:** Think about who needs to access the data collected and with whom you are required to share it. *(See Data Sharing Tip Sheet for more information.)*
- **Responsible data storage/retention:** Think about how long you'll need to use the data (and keep it only for that length of time). *(See Retention, Archiving and Disposal Tip Sheet for more information.)*

ADDITIONAL RESOURCES:

Anonymisation Decision-Making Framework. UK Anonymisation Network. An interactive guide.

Privacy Principles. Organisation for Economic Co-operation and Development (OECD).

Fair Information Practice Principles. National Strategy for Trusted Identities in Cyberspace, Appendix A. National Institutes of Standards in Technology (NIST).

Professional Standards for Protection Work. ICRC. 2013 Edition.

Anonymisation: managing data protection risk. UK Information Commissioner's Office (ICO). A summary of an anonymisation code of practice.

Hansen, Marit and Andreas Pfitzmann. *A terminology for talking about privacy by data minimization: Anonymity,Unlinkability, Undetectability, Unobservability, Pseudonymity,and Identity Management*. August 2010.

The Electronic Cash Transfer Learning Action Network is convened by Mercy Corps, with support from the MasterCard Center for Inclusive Growth.

MERCY CORPS

MasterCard | MasterCard Center for Inclusive Growth

elan
The Electronic Cash Transfer Learning Action Network