INTERSOS

Data Protection & IT Asset Management Policy

SUMMARY

1. IT Data Protection Policy

The Data Protection Policy is one of the policies that address the beneficiaries' data. This policy must be considered together with the following other policies, already in place within INTERSOS:

- Global Child Protection policy (GCP)
- Protection from Sexual Exploitation and Abuse policy (PSEA)
- Data Protection Protocol
- Other Data Protection policies adopted both at HQ and field level

The same policies are to be applied in case the data is on hard support (paper documents).

1.1 Purpose of data protection

Given the sensitive nature of the information collected from beneficiaries, INTERSOS has developed this policy with the following objectives:

- To ensure the same management, integrity and protection of beneficiaries' sensitive data;
- To respect the privacy and confidentiality of beneficiaries;
- To develop and implement a security protocol and mitigation measures for privacy-related risks associated with the collection and handling of beneficiaries' personal data;
- To provide practical guidance for treatment, safekeeping and transfer of personal data, including data sharing.

When collecting and processing data from vulnerable families and individuals, risks such as loss, interception, theft, accidental or malicious dissemination or unauthorized disclosure might happen, causing critical risk and harm to the persons concerned, as well as to INTERSOS and its staff. Therefore, this policy is of particular importance for INTERSOS as it has the responsibility to foster the respect of data protection principles, in line with global standards and guidelines. **This Policy applies to all personal data held by INTERSOS in relation to any project being implemented. Compliance with this policy is mandatory for all INTERSOS staff.**

1.2 Definition of Personal Data

Any personal information obtained during outreach assessments or house-to-house visits, from external and/or internal referrals or by any other means, is by definition classified as confidential and sensitive. Personal data include:

- biographical data, such as date of birth, marital status, address, racial or ethnic origin, etc.;
- biometric data, such as iris scan, fingerprints etc.;
- material circumstances, such as political opinions, religious or other beliefs, sexuality of human rights violations, employment history, etc.;

- images of recordings;
- external reports, such as medical certificates, police statements, criminal proceedings or convictions, etc.;
- personal documents, such as health records, bank details etc.;
- verification documents, such as copies of passports, UNHCR certificates etc.;
- any other personal detail of whatsoever nature.

All this information can only be processed under strict conditions, as specified in the following paragraphs.

1.3 Guidelines for managing Personal Data

All INTERSOS personnel must respect the confidentiality of personal data. Only people who are authorized to process data can access it. Personal data must always be handled and processed appropriately, no matter how this information is encountered, which includes recording or holding such data or carrying out any operation or set of operations on the data, including organization, adaptation or alteration; disclosure by transmission, dissemination and alignment, combination, blocking, erasure, or destruction.

In order to ensure and respect the confidentiality of beneficiaries' data, any collected information – assessment forms, referral forms, individual case files, external certificates etc. - must be filed and stored in a way that it is accessible only to authorized personnel and transferred only through the use of protected means of communications as defined in this policy.

All individual case files, whether followed up or not, are considered permanent records and are the responsibility of INTERSOS and its missions, for a period defined by the mission according to INTERSOS' regulations, and to Donors' requirements on Record Keeping of Official Project Documentation (usually at least five (5) years from the completion of a specific action). This follows also the principle of GDPR (retaining personal data), in which it is specified that "sensitive and confidential data processed for any purpose shall not be kept for longer than is necessary for that purpose".

Finally, all Donors' provisions, if they are stricter than INTERSOS' ones, must be respected.

1.4 Protection Information Management (PIM)

PIM is the principled, systematised, and collaborative process to collect, process, analyse, store, share, and use data and information to enable evidence-informed action for quality protection outcomes.

The objective of PIM is to provide quality data and information on people in displacement situations in a safe, reliable, and meaningful way. PIM is helpful in ensuring the efficient and targeted use of resources and in enabling the coordination, design, and delivery of protection responses.

The PIM principles underlie and characterize all PIM systems, regardless of their purposes, methods, or products. Here the full information about PIM (see also http://pim.guide/):

- People-centred and inclusive. Data and information activities must be guided by the interest, well-being, and rights of the affected population and their hosts, which must participate and be included in all relevant phases.
- Do no harm. Data and information activities must include a risk assessment and take steps, if necessary, to mitigate identified risks. The risk assessment must look at negative consequences that may result from

data collection and subsequent actions or service delivery for as long as the data and information activity is carried out.

- Defined purpose. Given the sensitive and often personal nature of protection information, data and information activities must serve specific information needs and purposes. The purpose must: be clearly defined and communicated; be proportional to both the identified risks and costs vis-à-vis the expected response; aim at action for protection outcomes, including the sharing and coordination of protection data and information.
- Informed consent and confidentiality. Personal information are to be collected only after informed consent has been provided by the individual(s) in question, and that individual must be aware of the purpose of the collection. Furthermore, confidentiality must be clearly explained to the individual before the information is collected.
- Data responsibility, protection, and security, Data responsibility goes beyond data privacy and data protection. It entails a set of principles, purposes, and processes that seek to guide humanitarian work and leverage data to improve affected populations’ and their hosts’ lives in a responsible manner while adhering to international standards of data protection and data security. Data and information activities must adhere to international laws and standards of data protection and data security. Persons of concern have a right to have their data protected according to international data protection standards.
- Competencies and capacities. Actors engaging in data and information activities are accountable for ensuring that data and information activities are carried out by information management and protection staff who have been equipped with data and information core competencies and have been trained appropriately.
- Impartiality. All steps of the data and information cycle must be undertaken in an objective, impartial, and transparent manner while identifying and minimizing bias.
- Coordination and collaboration. All actors implementing data and information activities must adhere to the principles noted above and promote the broadest collaboration and coordination of data and information internally, among humanitarian actors, and externally, with and among other stakeholders. To the extent possible, data and information activities must avoid the duplication of other data and information activities and instead should build upon existing efforts and mechanisms.

1.5 General purpose of IT Tools for managing Personal Data

1.5.1 Data collection

There are mainly 3 types of data collection tools:

- Web forms (online)
- Mobile Apps (offline)
- Spreadsheet/Word processor templates (offline)

Online web forms such as Google Form are used for collecting information both with laptops and mobile devices. Since data is automatically stored into a database after the submission, there are no data protection violation risks (no data is stored inside the device).

On the other hand, mobile Apps such as Kobotoolbox, ODK-based app, Fulcrum store data inside the device itself, because they need to work offline. In this case, the following rules must be followed:

- HQ must be informed of each device used in data collection in order to enforce security policy (PIN/password) by connecting the device to the INTERSOS MDM system;
- Each device (Tablet or smartphone) used in data collection must be protected by a PIN or any kind of password;
- Each installed data collection APP should be set in order to delete automatically the data collected after the synchronization with the main database. If this is not possible (for example Fulcrum does not allow this setting) the data collected must be deleted manually;
- Each device must be kept updated to the latest APP version available.

In case the data collection is carried out by using classic office tools such as Spreadsheet (e.g. MS Excel), word processor (e.g. MS Word), local databases (e.g. MS Access), the files must be protected by password. If the file is transferred by email, the password must be sent in a separate email or via another means (e.g. Skype).

1.5.2 Data access and archive

The main principle to apply for accessing archived data is the “need-to-know”. According to this principle, the data must not be accessible to those who do not need the data itself. If the data is collected via paper document, such document must be stored in a safe box/cupboard and it must be accessible only to those who need-to-know.

There are mainly 3 methods for storing and accessing the data:

- Cloud databases directly connected to either the Web forms (online) or the Mobile Apps
- Cloud documents repository
- Personal laptop or Network Area Storage (NAS)

The **cloud databases** (such as Kobotoolbox, Fulcrum) are websites where the data collected using mobile apps is recorded. They usually have only one level of access, which is the Administrator one. The administrator account must be held by the M&E person (or equivalent position) and must not be shared among the operative staff.
Note: Google form records the data in Google Drive (see next paragraph).

Cloud documents repository (e.g. Google Drive, Dropbox) are websites where the data is stored with Folder/Files logic (e.g. MS Excel, Word, pdf files, etc). One of the main features is the possibility to share the data with other users. For this reason, the data must not be shared with those who are not entitled to access it. The M&E person should periodically check the sharing status. Finally, the M&E person should set the sharing permission in order to avoid (better, prevent) that the operative staff is able to share the data further with someone else.

It could be that the data is kept within the **laptop or NAS**: if possible, this method should be avoided. In fact, there are two main risks: loss of data (for example, when the laptop is formatted because a new person is using it), and an unpermitted access (usually NAS are not protected by password). If the data is stored in personal laptop or NAS, that device must be protected by password.

1.5.3 Data reporting and sharing

Reports should be aggregated. All reports must not contain any direct reference to the person of concern such as name, phone number or ID. If there is a need to report for specific persons (as in the case of referrals), the Case Code must be used (e.g. CMAM1), which is an internal reference number with no direct connection to the person itself.

Sometimes, donors request the full information for the managed cases. In this scenario, the data must be sent trying to limit as much as possible the Cc addresses, and of course protecting the content by password.

1.5.4 Specific purpose of IT Tools for managing Personal Data

Since 2017, INTERSOS has developed a dedicated web platform for case management (used for now in Lebanon and Iraq), for needs assessments (Jordan, Cameroun, Nigeria and RCA) and for complaints.
All platforms are developed with the cloud platform Knack, which grants high availability and security. The log-on access is managed with single sign-on and users are profiled according to the need-to-know principle. These platforms grant the highest level of confidentiality compared with the other, general, apps.

1.5.6 Restrictions

Based on consultations with the Data Protection Officer, and other relevant counterparts at HQ level, INTERSOS may refuse to provide a response, or may limit or restrict its response to a request or objection under which:

- It would constitute a necessary and proportionate measure to safeguard or ensure one or more of the following:
  - The safety and security of INTERSOS, its personnel or the personnel of Implementing Partners; or
  - The overriding operational needs and priorities of INTERSOS in pursuing its mandate.
- There are grounds for believing that the request is manifestly abusive, fraudulent or obstructive to the purpose of processing.

2. IT Asset Management policy

2.1 Purpose of IT asset management

The policy outlined below relates to the responsible use of computers and information systems. This policy addresses the use of internet, email and all INTERSOS offices' equipment including, but not limited to, computers, laptops, tablets, smartphones, scanners, printers, storage devices & projectors.
The policy and guidelines outlined here aim at preventing unnecessary expenses, repairs, systems failures to INTERSOS equipment and Data Protection violations (see chapter 1 of this document). Additionally, the measures outlined below are to prevent misuse of equipment that may result in a slower internet and networking system, virus attacks to INTERSOS network and exposure to websites, photos and other material not deemed appropriate for a workplace. Failure to comply with this policy may result in disciplinary action (verbal and written warnings), loss of privileges, denial of access to these resources and, in extreme circumstances, immediate dismissal.

- The purpose of Information & Communication Technology systems is to conduct INTERSOS business. Personal use is to be kept to a minimum.
- The Organisation's access to the Internet (World Wide Web) is to be used primarily for work purposes. INTERSOS reserves the right to access and review records of employees' use of the World Wide Web.
- Employees are required to contact the IT Department in Rome HQ in order to obtain its authorization before attempting to download or install any software from the Internet/CD/DVD, with the exception of updates and software patches to standard INTERSOS software (including anti-virus software).

For information on security and network maintenance purposes, the IT Officer, with authorization from the Secretary General, may monitor equipment, systems and network traffic at any time.

2.2 IT asset management principles

2.2.1 Emails and communications activities

- The purpose of Email communication system is to conduct INTERSOS business. Access to personal emails should be reasonably limited.
- All INTERSOS work-related email correspondence is to be conducted through the dedicated email addresses.
- There are risks inherent to sending and storing messages on the Internet, and the IT Department cannot control Internet attacks or breaches of security to Internet emails.

- Emails should be used in a respectful and appropriate way. Any form of harassment via email, whether through language, frequency, or size of messages is prohibited. The Organisation's policies prohibiting discrimination and harassment apply equally to the email system.
- Employees are not permitted to read, intercept, copy, use, or disclose email communications directed to others without express authorization. Accessing another employee's electronic mailbox without the latter's express permission is prohibited.
- Sending credit card numbers or similar confidential donors' information, through unencrypted end-user technologies, such as emails and instant messaging (chat), is prohibited.
- Sending messages for any commercial purpose other than INTERSOS business is prohibited.

2.2.2 Internet

The following admonitions and prohibitions must be adhered to with no exceptions.

It is prohibited to:

- Access websites and media deemed inappropriate or offensive;
- Download, broadcast, transmit, distribute or store obscene or pornographic materials on INTERSOS equipment or systems. This also includes material that is obscene, defamatory, malicious, threatening (or that in any other way causes grievance), has a racist theme, violates export control laws, contains sexual implications or threats, racial slurs, or any other comment that offensively addresses someone's age, gender, sexual orientation, marital status, religious or political beliefs, nationality, or disability;
- Use Internet for online, peer to peer software, torrents, Internet Download Manager etc., which monopolizes internet bandwidth;
- Purposeful introduce malicious programmes into the network or server (e.g., virus worms, Trojan horses, email bombs, etc.)

2.2.3 ICT Equipment and Systems

The following admonitions and prohibitions must be adhered to with no exceptions.

It is prohibited to:

- Attempt repairs at INTERSOS equipment personally or through an unapproved vendor. All repairs and maintenance are to be conducted through the IT Department or by the IT Focal Person;
- Violate any software license or copyright, including redistributing software;
- Install pirated software or any software without informing the IT Department;
- Use INTERSOS information systems for any illegal or unauthorized purpose, or to access obscene materials;
- Make personal use of information systems or electronic communication for non-INTERSOS consulting, business or employment, without the written approval of the Headquarters.

2.2.4 Data Access

All products of work during INTERSOS time is considered the possession of INTERSOS and must be available for access by supervisors and management at any moment. This includes, but is not limited to, correspondence, researches, reports, data and translations. Should the employee become unavailable due to illness or other reasons or should he/she refuse to provide the information requested, the IT Department or its designee may be required to access information with the approval of HQ.