Myanmar National Protection Sector

DATA PROTECTION TIPSHEET FOR HUMANITARIAN ACTORS

Data protection is defined as "the systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the processing of personal data."[1] The personal data means "any information relating to an identified or identifiable natural person".

This Tip Sheet is intended as a list of suggestions to ensure "do no harm" for protection (or other sectors/clusters) partners on data related to our population of concern. It is not meant as an exhaustive list, but guidance for humanitarian workers and actors on how they can strengthen and support data protection in humanitarian actions.

Consent and assent	Prior to personal data collection, always explain the purpose of data collection in a language that he/she understands properly and receive his/her consent. In the case of minor or others who are not able to provide his/her legal consent, seek assent which is the expressed willingness to participate in data collection.
Confidentiality	Be aware of the risks specific to their context and to explicitly think through the possible implications to individual, their family, communities, and for the organization, if data reaches into the wrong hands. All staff in contact with the data must have a strong understanding of the sensitive nature of the data, value of data confidentiality and security.
	Always keep the personal data of population of concern confidential, including even after the specific individual or affected person is no longer in need of humanitarian support.
	Personal data 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 communication.
Data security	To protect against external breaches as well as unauthorized/inappropriate access to data, ensure having necessary safeguards, procedures and systems to prevent, mitigate, report and respond to security breaches.
	Password protect digital documents that contain information on population of concern.
	All paper-based forms and information related to population of concern must be stored safely in a locked cabinet.
	Computers, USB, tablets, and mobile phones etc. should be password protected. Two-steps authentication is recommended (for example a login password plus receiving a code through the authenticator app on your phone).
	Notify the data focal point or manager immediately upon a breach of sensitive data breach. Assess the nature of the breach and its impact, take remedial action, and respond to any protection concerns for population of concern.
Managing and sharing data	Humanitarian organizations have an obligation to account for and take responsibility for their data management.
	Data collection should be limited to the information that is relevant and necessary only.
	Organizations should develop and implement Standard Operating Procedures (SOPs) to manage data including handling of the data within the organization, identify focal point and assigning manager for internal oversight.
	Any personal data or sensitive non-personal data to other organizations should be managed through data sharing agreements and/or protocols. If personal level data is not required by the requested organization, anonymizing or aggregating data to make a data subject unidentifiable directly or indirectly can be done prior to sharing.
Reach out and key resource	For clarifications on data protection, contact your manager or data protection focal point within your Organization. You may wish to contact to Protection Working Group Coordinator in your area or National Protection Sector Coordinator if needed.
	Familiarize yourself with the Inter-Agency Standing Committee's Operational Guidance on Data Responsibility in Humanitarian Action for more information.

March 2021

[1] *Definition developed by the UN Privacy Policy Group in 2017*