PSEA Network Myanmar

Sample Data Protection Policy

This policy has been drafted by the PSEA Network Myanmar as a sample that can be downloaded and adapted by any organization seeking to improve data protection within their organization. It is intended to cover all forms of data that may be collected by an organization, including data on sexual exploitation and abuse (SEA).

Introduction

There is a recognised right to privacy for individuals over their personal information and communications. While Myanmar has no specific data privacy law, the Law Protecting the Privacy and Security of Citizens[1] provides some protections on individual privacy and communications, including electronic communications.[2]

In serving affected people in Myanmar, [Organization Name] needs to handle information about people in need. This includes personal data (data that can identify an individual, such as their name, date of birth, address, phone number, ID number, thumbprint, photo, health status etc).

This data protection policy describes how [Organization Name] collects, handles, stores and disposes of personal data, in a manner that protects the rights of people in need and complies with legal and ethical obligations. This policy includes information that may be collected by [Organization Name] regarding allegations of sexual exploitation and abuse. The policy consists of 10 key data protection principles.

Data protection principles

1. **Legitimate purpose:** [Organization Name] will only collect data for a specific, legitimate, lawful purpose (such as to register people for assistance) and use it in a manner that is consistent with that purpose. Personal data may be used for secondary purposes provided these have a reasonable and direct connection to the original specified purpose (such as monitoring).

2. **Risk-informed:** [Organization Name] will assess risks relating to privacy and personal data protection for each specific context, including risks relating to choice (if individuals can freely choose to give their data), confidentiality (risk of it being given out inappropriately or being hacked), and protection risks (risk that giving personal data, or the way it is used, does harm to a person's rights including safety and dignity). [Organization Name] will adjust how it collects and carries personal data according to the risks, will implement a range of mitigating measures and will monitor their effectiveness during implementation.

3. **Data minimisation:** [Organization Name] will collect only what personal data is needed to achieve the lawful purposes. It will not collect unnecessary information about people such as their race, ethnicity or religion, and for other information such as education level, disability, health and IDP/refugee status will depend upon the programmatic context. [Organization Name] will endeavour to use any data collected to actively improve and develop programming and implementation of policies, particularly in terms of access and targeting.

4. **Data adequacy:** [Organization Name] will ensure personal data being collected is relevant and adequate, and will take reasonable steps to ensure it is accurate and kept up to date. Accuracy should be strived for through corroboration (such as documentary ID). To minimise the creation of multiple additional data sets, personal data will be maintained in a central database.

5. **Minimum access:** [Organization Name] will minimise the number of people who have access to personal data, and the amount of personal data staff have access to, based upon their role within

[1] Union Parliament Law 5/2017, 8 March 2017.
[2] Section 8.

the Organization. The Organization will put in place tiered access, rather than having all fields visible to all staff accessing a database containing personal data. The Organization will identify personal data which is sensitive (such as information about sexual exploitation and abuse) and ensure it is kept confidential and reported strictly in accordance with organizational protocols. For personal data related to sexual exploitation and abuse, this should be kept in a separate database.

6. **Informed consent:** [Organization Name] obtains personal data only with the freely given and informed permission of the person whose data is being collected (or their legal guardian). This includes ensuring the person understands what is being collected, who will be collecting it, when and how, for what purpose, how it will be used, stored, shared and disposed of, and any risks to their privacy that may result from them giving their personal data to the Organization. Consent may be explicit (given verbally or documented by signature or thumbprint) or implicit (the person has been given the information, has no obstacle to exercising and expressing their free will, and has not objected when given the opportunity to do so. In some cases proxy consent will be sufficient, such as a parent or guardian consenting in the best interests of a child or a person without mental or intellectual capacity to give informed consent directly.

7. **Data security:** [Organization Name] has systems in place to ensure personal data is safely stored and protected from loss or unauthorised access. For paper copies this includes storing them safely in a locked drawer or cabinet, and disposing of them in a secure manner such as through shredding. For electronically stored personal data, this includes having IT systems in place including use of strong passwords, file encryption, anti-virus programmes, firewalls, use of approved servers and cloud storage and regular back-ups. Removable media such as USB drives or CDs are to be safely locked away when not in use. The Organization will take immediate action in the event of a data breach.

   Random password generator can be accessed here

   Instructions on how to wipe/remove data from a Windows 10 laptop can be accessed here

8. **Timebound:** [Organization Name] will not hold onto personal data for longer than is necessary to achieve the lawful purposes of having it. People who have given permission for the Organization to have their personal data retain the right to access it, request for it to be updated or deleted, they have a "right to be forgotten". Personal data relating to finished projects will be stored for the minimum period required or audit purposes and then disposed of. It may however be legitimate to retain personal data if, for example, it may be needed for the purposes of emergency assistance such as following a disaster.

9. **Data sharing:** Data should be anonymised before sharing with third parties, so that it cannot identify the people to whom the data relates. If personal data is requested or compelled by state, military or other actors, or if it is confiscated by a power holder despite objection, the staff will refer this to the data protection focal point. If there is legitimate need to share personal data there must be a data sharing agreement entered which sets out what data will be shared and how it will be used and protected. Where the Organization shares personal data with a third party, it will do so with consent of the people whose data is to be shared. Where the Organization receives personal data from a third party, reasonable enquiries will be made to ensure the people know and consent to this.

10. **Accountability:** The Organization is accountable to affected people regarding their personal data. The Organization will consult affected people about the processing of their personal data, will ensure information provided to them about data protection is accessible taking into account differences in age, gender, language, literacy, disability and other diversity. The Organization will use its complaints and feedback mechanism (CFM) as a means for people to request changes and to make complaints regarding how their data is being used. Personal data of CFM Users will

strictly be handled in accordance with this policy and with the policy on Protection from Sexual Exploitation and Abuse/Safeguarding policy.

Responsibilities

- Everyone who works for or with the Organization is responsible for data protection and must ensure any data they handle is processed in accordance with this policy.
- The Organization has appointed a data protection focal point who is to be consulted whenever personal data is to be collected, received or shared. The data protection focal point is responsible for ensuring new staff are informed about data protection, including the application of this policy, and trained in how to apply it in their work.
- The IT focal point is responsible for ensuring all systems, services and equipment used for storing data meet acceptable security standards and is regularly checked and scanned.
- Any staff who leave the Organization are responsible for ensuring they do not have any beneficiary personal data in their possession, including in emails, on laptops, smart phones, USB sticks, or paper copies.