Data Protection

Brief overview

DEFINITION

Set of principles and practices to ensure that personal data is collected, used and protected in a way that considers individuals' privacy and any risks that may come to them from not adequately safeguarding their data.

CONCEPTS

Processing: Operation on personal data, including collection, storage, access, analysis, deletion, etc.

Personal Data: Information that relates to an identified or identifiable living, natural person: name, address, gender, age, identification number, photograph, fingerprint, etc. Also more sensitive information: health status, religious or political affiliations or sexual preferences. It is important to know that this list is not definitive, what is personal and even what is sensitive can change depending on the political, social, or economic environment.

Sharing: To provide access to information by sending it by email, providing a link to digital data, making a copy and giving it to someone, providing direct or indirect access to a database.

GENERAL BEST PRACTICES

DO

- Determine which personal data is absolutely necessary to collect before implementing a project.
- Consider local customs and political context when determining what personal data to collect and how to explain the purpose(s) of the collection.
- Consider that location data and demographic data, even though not necessarily personal, can be highly sensitive and put individuals and groups at risk of harm.
- Decide on what information will be provided to affected persons. For instance: the purpose of the project, why data must be collected, how it will be used and who it will be shared with, where to go if he or she has questions about their personal data.
- When providing information or obtaining consent, make a record of the interactions, including: what information was provided, who gave it, the date and place, the audience, whether any objections were raised.
- Determine who will be responsible to answer questions about the use, storage, correction, etc. of personal data.
- Encrypt and/or password protect devices and digital files (word, excel, etc) containing personal (or other sensitive) data.
- Plan for what will happen to the personal data once it is no longer needed. For instance, will it be archived, can it be securely deleted/destroyed?
- Only provide access to digital or paper files containing personal data to those staff (or volunteers, consultants, or other authorized agents) that **need** access in order to do their work.
- Maintain passwords, physical locks, virus protection, firewalls and any other reasonable form of security for computers, mobile phones, filing cabinets, or other places where personal data will be stored.
- Plan to make a written agreement before sharing any personal (or other sensitive) data outside of your organisation.

DO NOT

- Use Dropbox public folders or publicly accessible Google Drive/Docs or other internet-based platforms for sharing or collaborating on documents containing personal (or other sensitive) data, especially where such online document is not password protected.
- Share or provide access to files containing personal data to governments or any other partner without first considering the consequences of providing such and further without formalizing the terms of such sharing.
- Post personal details (including photographs) of affected persons on social media accounts, whether personally or professionally without prior agreement with your organisations communication and legal teams.
- Leave files with personal (or other sensitive) data out in the open. Lock them in cabinets, desks, offices when not in use.
- Use USB storage devices for personal (or other sensitive) data unless the contents are password protected and/or encrypted.
- Assume that simply asking an individual for consent, or whether they agree with something involving the use of his or her personal data, is legally or morally sufficient for you to act. Consent cannot be freely given when the provision of necessary aid is conditioned upon it.

Please note that this information notice is not intended to be comprehensive. There are many areas of data protection that are not covered herein. Always seek advice of counsel when you have questions about the interpretation and/or implementation of data protection practices.

INTERNATIONAL FEDERATION

Contact information
Information Managment, IFRC
im@ifrc.org