IFRC Data Protection FAQ's 2018

PURPOSE

There are new General Data Protection Regulations (GDPR), sometimes coined the "Eu Data Protection Regulations," came into effect on May 25, 2018. All organizations, companies, and entities operating in the EU will be required to adhere or, at minimum, have preparedness plans. IFRC is an International Organization with some immunities. However, our complex organizational structure, diverse data workflows, digital and data technology needs, and data practices with National Societies and Reference Centers may be affected. The GDPR is considered a "gold standard" which other countries outside the EU may adopt.

IFRC has various stages of data readiness based on department, project, and individuals. A recent Data Protection Impact Assessment (DPIA) made recommendations for changes to be made in lieu of Data Protection gaps in the organization. **The following is a shared "Frequently Asked Questions" to aid IFRC staff plan and prioritize the next steps.**

DATA PROTECTION BASICS

Data Protection laws protect the rights and the privacy of individuals. The application of responsible data use and adhering to the various data protection laws is the practice of "Data Protection".

The following are quick 1-minute videos explaining Data Protection and the risks:
https://www.icrc.org/en/document/watch-videos

ICRC and Brussels Privacy Hub created the Handbook on Data Protection:
https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

BASIC TERMS

Here are some common data protection terms from the Handbook on **Data Protection:**

Anonymization encompasses techniques that can be used to ensure that data sets containing Personal Data are fully and irreversibly anonymized so that they do not relate to an identified or identifiable natural person, or that the Data Subject is not or no longer identifiable.

Data Controller means the person or organization who alone or jointly with others determines the purposes and means of the Processing of Personal Data. A Data Controller is the person who alone or jointly with others determines the purposes and means of the Processing of Personal Data, while a Data Processor is the person who processes Personal Data on behalf of the Data Controller. Finally, a Third Party is any natural or legal person, public authority, agency or any other body other than the Data Subject, the Data Controller, or the Data Processor. (source: ICRC handbook)

Data Processor means the person or organization who processes Personal Data on behalf of the Data Controller.

Data Protection Impact Assessment or DPIA means an assessment that identifies, evaluates and addresses the risks to Personal Data arising from a project, policy, programme or other initiative.

Data Subject means a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Personal Data.

Personal Data means any information relating to an identified or identifiable natural person. (eg. Name, religion, address, bank information, etc.)

Processing means any operation or set of operations which is performedon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination or erasure.

Right to privacy

- Tell people how their data will be used/processed
- Privacy Exception - in humanitarian emergencies there may be a need to balance the rights of all the affected individuals

Types of data - name, surname, mobile phone number, various data collected as part of the 'know your client' processes, geolocation/other phone metadata, and Biometrics. Humanitarian Organisations may also collect data related to socioeconomic factors or vulnerabilities for the purposes of targeting assistance. (ICRC handbook chapter 9)

Sensitive Data means Personal Data which, if disclosed, may result in discrimination against or the repression of the individual concerned. Typically, data relating to health, race or ethnicity, religious/political/armed group affiliation, or genetic and biometric data are considered to be Sensitive Data. All Sensitive Data require augmented protection even though different types of data falling under the scope of Sensitive Data (e.g. different types of biometric data) may present different levels of sensitivity. Given the specific situations in which Humanitarian Organizations work and the possibility that some data elements could give rise to discrimination, setting out a definitive list of Sensitive Data categories in Humanitarian Action is not meaningful. Sensitivity of data as well as appropriate safeguards (e.g. technical and organizational security measures) have to be considered on a case-by-case basis.

Consent

- Explain why collecting the data, what will be done with it. Ask for permission

Right to privacy

- Tell people how their data will be used/processed
- Privacy Exception - in humanitarian emergencies there may be a need to balance the rights of all the affected individuals
- Types of data - name, surname, mobile phone number, various data collected as part of the 'know your client' processes, geolocation/other phone metadata, and Biometrics. Humanitarian Organisations may also collect data related to socioeconomic factors or vulnerabilities for the purposes of targeting assistance (ICRC handbook chapter 9)

Data Lifecycle

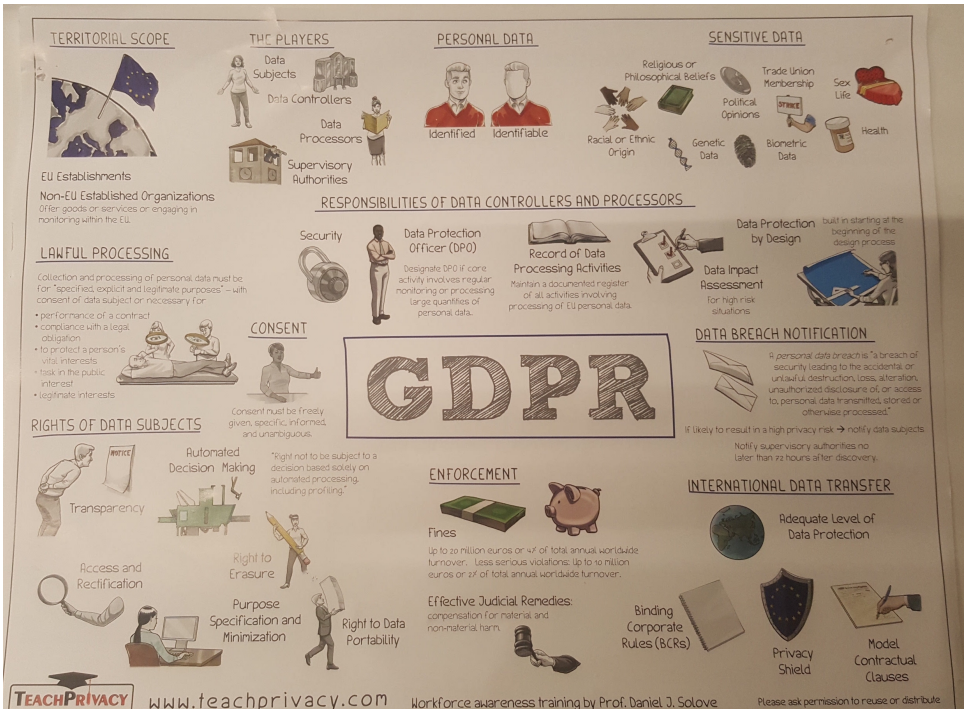
- A data life cycle describes the stages that the data may undergo, from the moment use of data is considered in a project until the data is destroyed. Typically, the following stages can be discerned: 1. Initiation, 2. Collection & Access, 3. Storage and Transport, 4. Processing and Analysis, 5. Dissemination and 6. Closing

- Processing - means collection, storage, use and disclosure of data

Roles and responsibilities

- Every project has various roles and responsibilities. At a minimum a data-driven project would need the following roles: Data curator, Data controller, Data processor, Data analyst, Project lead, IT support, team lead.
- responsibilities should be handled by means of "data governance", i.e. who has ownership of the personal data in your organisation and who is/are allowed to have access to that data?
- A Data Controller is the person who alone or jointly with others determines the purposes and means of the Processing of Personal Data, while a Data Processor is the person who processes Personal Data on behalf of the Data Controller. Finally, a Third Party is any natural or legal person, public authority, agency or any other body other than the Data Subject, the Data Controller, or the Data Processor. (source: ICRC handbook)

WHAT ARE THE BASICS OF A RESPONSIBLE DATA POLICY?



The GDPR required responsible data policies established by companies and organisations operating in the European Union. Source: teachprivacy.com

GENERAL QUESTIONS

How can I prepare a responsible data policy for my department? What is a basic personal data checklist?

The following is a quick Data Hygiene checklist to consider for your various workflows:

- Basic identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data

- Racial or ethnic data
- Political opinions
- Sexual orientation

i. Beneficiary assistance: where sensitive personal data about persons affected and other persons of concern to IFRC is routinely collected, analysed and shared with partners;

ii. Volunteer/relationship management: where personal data, possibly including sensitive data, is collected about volunteers, interlocutors and partners involved in the provision of protection and assistance;

iii. Human resources: where personal data, including sensitive data, is collected about IFRC staff and contractors;

iv. Public internet: where the IFRC's websites collect personal data directly from users and/or utilise cookies, analytics and communications tools that track their activities;

v. Aggregate reporting: in some cases, personal data that is collected about volunteers and persons affected provides the basis for more widely shared reports about IFRC's activities.

The FutureLearn GDPR Online course suggests asking the following questions:

- Try to think about who deals with personal data in your company or organisation.
- Try to identify the nature of the data and the purposes for which they are collected or processed.
- Try to think about which processes are mandatorily followed in your company or organisation when handling the data.
- How are data safeguarded?
- What is the red tape that is likely to arise when changing the ways how people work and how can it be addressed?
- Do you need structural changes? Do you need to appoint a Data Protection Officer? Which competences should he or she have in your organisation and how could he or she best be placed in the organigram?
- Go even further. Identify your weak and strong points. Now, you know the obligations that a responsible data polict introduces for data controllers and processors, step into action ensuring that you, your company or organisation complies with responsible data obligations and avoid potential liabilities or sanctions.

Here are some basic GDPR resources helpful to anyone developing a responsible data policy:

Keep in mind that IFRC, as an International Organization, has some particular immunities. As humanitarians, we will need to prepare. Each National Society in the EU will prepare based on their own programs and guidelines:

- This 2 -page checklist explains some of the considerations.
- Responsible Data Forum Top 5 considerations:
- Responsibility and rights are foundational to the GDPR
- The scope of the GDPR is broad, going beyond Europe
- The GDPR broadens the definition of 'personal data'
- Prepare for data audits now
- The GDPR strengthens the rights of data subjects

- For organisations, this is operational
- https://www.eugdpr.org/
- https://www.teachprivacy.com/gdpr-resources/
- https://www.accessnow.org/data-protection-matters-protect/
- Digital Impact is an initiative of the Digital Civil Society Lab at the Stanford Center on Philanthropy and Civil Society (Stanford PACS). Their summary of key articles: https://digitalimpact.org/gdpr/