The Professional Standards for Protection Work

Carried out by humanitarian and human rights actors in armed conflict and other situations of violence

Chambery, 18.10.2016

Guilhem Ravier
ICRC
Revised edition for 2017

- 59 standards and guidelines
  - Professional standards indispensable
  - Guidelines as useful reference

- Explanatory notes capturing the main challenges and dilemmas
PROFESSIONAL STANDARDS FOR PROTECTION WORK

Overview of the different chapters

- Overarching principles
- Managing protection strategies
- Outlining the protection architecture
- Building on the legal base of protection
- Promoting complementarity
- Managing sensitive protection information
- Ensuring professional capacity
Issues to be revised/redeveloped

- Managing protection strategies (M&E);
  - Strengthen links between assessments, strategies, and outcomes

- Managing sensitive protection information
  - Regulation of collection and use of personal data
  - “sensitive data” > “personal data”
  - Challenges linked to the use of new tech

- Engaging UN peacekeepers and other multinational forces, armed non-state actors,
- CT/CVE/PVE
WHAT IS DATA PROTECTION?
1. What is data protection?

Refers to rights of individuals: Right to data protection

**Scope:** protection of personal data

**What is personal data?**

**Broad definition:** means any information relating to an identified or identifiable natural person.

- Includes data identifying or capable of identifying human remains

**Examples:** Beyond biographical data (name, DoB)
- audio-visual material
- location data / online identifier (IP address)
- factors specific to physical/genetic/mental/eco/cultural/social identity

**Objectives in humanitarian context:**

- To ensure data processing operations **DO NO HARM**
- Strengthen confidentiality as a working method
- Enhance trust from beneficiaries/countries
DATA PROTECTION ON THE RISE

Overview of context
1. What’s happening out there?

Technological Developments

Easier, faster, cheaper to collect massive quantities of data:

- Unmanned Aerial Vehicles
- Smart Phones / Tablets
- Data Analytics / Data Mining
- Cloud
- Geolocation / GIS

➢ Increasing threat to privacy (data breaches, surveillance)
So what?

Regulatory developments to deal with impact on fundamental right to privacy and data protection

**Objective:** strike a balance between

- Protection of individuals rights
- Necessity to process personal data (trade, law enforcement, humanitarian action…)

---

**Image Description:**
The image contains a newspaper clipping titled "Revealed: how UK spied on its G20 allies at London summits." The article includes various bullet points, including privacy-related content. The visual elements include a balancing scale, symbolizing the balance between privacy rights and data processing needs.
2. Regulatory Environment

RIGHT TO PRIVACY

UN Universal Declaration of Human Rights 1948
Article 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

UN General Assembly resolution 45/95 (1990)

The present guidelines should apply to personal data files kept by governmental International organizations […]. Each organization should designate the authority statutorily competent to supervise the observance of these guidelines.

UN General Assembly resolution 68/167: negative impact of surveillance and interception of communications on human rights: Calls on States to review their legislation on communications surveillance/interception/collection of personal data

UN Human Rights Council Resolution (A/HRC/28/L.27) on the right to privacy in the digital age: creation of a Special Rapporteur on the right to privacy
European Convention on Human Rights 1950 (Council of Europe)

Article 8

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
RIGHT TO THE PROTECTION OF PERSONAL DATA

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980

Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 (Convention 108)
Recent Developments

- EU General Data Protection Regulation (more stringent rules)

Context: Migration in Europe

EU countries subject to EU Regulation

If there is no adequate protection of the personal data

No transfer of personal data to countries outside the EU or to international Organisations

Impact on operations ?
COUNCIL OF EUROPE CONVENTION 108 – Modernisation / Open for accession to non European countries (Uruguay, Morocco)

Additional requests for accession: Mauritius, Senegal, Tunisia

NATIONAL LEGISLATIONS: Over 108 countries now have a data protection legislation

Near and Middle East: Egypt, Morocco, ILOT, Saudi Arabia, UAE
Lebanon?

Europe and Central Asia: Bosnia and Herzegovina, Russia, Ukraine

Asia: China, India, Indonesia, Pakistan

Africa: South Africa, Burkina Faso, Senegal

Americas: Mexico, Brazil, Colombia, Argentina, Uruguay, USA

Figure 4. Global percentage of comprehensive, partial/sectoral and draft data protection laws in each region

Source: UNCTAD
Specific privacy and security risks are identified, including the potential for development of monitoring systems, which could be increased by technologies such as management information systems and electronic transfers; digital identity registration and biometrics, mobile phones but also drones. Humanitarian organizations not benefiting from Privileges and Immunities may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism). The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to humanitarian action more generally.
GENERAL DATA PROTECTION PROVISIONS
1. General Principles

- Fair and lawful processing
- **Legitimate Bases** (collection and transfers)
- Purpose Specification
- **Data Minimisation**
- Data Quality
- **Data retention**
2. Data Subject Rights

- Transparency / Information
- Access
- Rectification
- Deletion
- Objection
3. Controller Obligations

- Data Protection by Design / Default
- Attribution of Responsibilities (Processors)
- Record Keeping
- Data Security
- Notification of Data Breaches (to Data Subjects and Authorities)
- Impact Assessments
- Registration / Consultation / Authorisation
- Data Protection Officers
CHALLENGE:
COMPATIBILITY OF GENERAL DATA PROTECTION PROVISIONS WITH HUMANITARIAN / HR ACTIVITIES?
Brussels Privacy Hub/ICRC Project

Launch of the project June 2015 at the University of Brussels (VUB)

**Purpose**: provide guidance to the humanitarian sector in the area of data protection, with particular focus on new technologies

**How**: bring together humanitarian organisations, data protection authorities, academics, corporates to consider topical issues, relevant data protection concerns and guidance. Chatham House Rule.

**Workshops**:  
- Data Analytics/Big Data  
- UAV/Drones  
- Biometrics  
- Mobile Cash Assistance  
- Cloud based data collection  
- Internet of Things

**Other topics**:  
- General Principles  
- Legal Basis for Processing  
- Data Sharing  
- Bulk text messaging  
- Telemedicine  
- Employee Monitoring

**Output**: practical guidance papers, Handbook.
Data Protection Impact Assessment (DPIA)

- Analysis of possible advantages and risks involved in the collection/transfer as well as the data flows and potential mitigating measures:
  - How data will be collected, used, transferred and how the purpose (strictly humanitarian) can be respected?
  - What are the origin, nature, and severity of risks to the rights and freedoms of data subjects arising from a particular processing operation?
  - What are the appropriate measures to be taken to mitigate those risks?

- The first line holder (the Delegate) will carry out the DPIA (except if the processing of personal data involved complex technologies or particularly sensitive data)

- The reviewing and the validation should be done by the Staff in Charge (the staff member handling the files).
## DPIA

### When to carry out a DPIA?
- Using new technologies for data collection & analysis (mobile devices, cloud etc.)
- Processing large amount of personal data
- Transfers outside ICRC (authorities, other IOs)

### Helps ICRC staff to:
- Document processing milestones
- Take measures to ensure data security
- Implement Data Protection By Design