2018 ABRIDGED EDITION

PROFESSIONAL STANDARDS FOR PROTECTION WORK

CARRIED OUT BY HUMANITARIAN AND HUMAN RIGHTS ACTORS IN ARMED CONFLICT AND OTHER SITUATIONS OF VIOLENCE

Explanatory note

This document is an abridged version of Professional Standards for Protection Work (3rd edition). Published alongside the full version, it is aimed at humanitarian and human rights actors engaged in protection work and intended to act as an easy reference to the minimum standards to be met and recommended guidelines to be followed in such work. The 45 standards and 15 guidelines are reproduced in full, together with a short explanation in each case of the main challenges they are designed to address. Further information – for example, on the limitations and constraints of the standards and guidelines, and the dilemmas they may pose to protection actors – as well as practical examples of the some of the situations referred to, can be found in the full document. This abridged edition is part of a toolkit accompanying the full document that also includes an e-learning course, mobile application and online micro-site.

PARTNERS:

AMNESTY INTERNATIONAL

DANISH REFUGEE COUNCIL

Global Protection Cluster

handicap international / humanity & inclusion

HPG Humanitarian Policy Group

HUMAN RIGHTS WATCH

ICVA — A GLOBAL NGO NETWORK FOR PRINCIPLED AND EFFECTIVE HUMANITARIAN ACTION

InterAction

JRS accompany · serve · advocate

MEDECINS SANS FRONTIERES

OCHA United Nations Office for the Coordination of Humanitarian Affairs

OXFAM

UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER

UNHCR The UN Refugee Agency

2018 ABRIDGED EDITION

PROFESSIONAL STANDARDS FOR PROTECTION WORK

CARRIED OUT BY HUMANITARIAN AND HUMAN RIGHTS ACTORS IN ARMED CONFLICT AND OTHER SITUATIONS OF VIOLENCE

ACKNOWLEDGEMENTS

TABLE OF CONTENTS

ACRONYMS

ALNAP	Active Learning Network for Accountability and Performance (in humanitarian work)
CHS	Core Humanitarian Standard
CII	Community identifiable information
DDR	Disarmament, demobilization and reintegration
DFID	Department for International Development
DFS	UN Department of Field Support
DPIA	Data protection impact assessment
DPKO	UN Department of Peacekeeping Operations
DRC	Danish Refugee Council
ECOSOC	UN Economic and Social Council
GPC	Global Protection Cluster
HPG	Humanitarian Policy Group
IAP	Integrated Assessment and Planning
IASC	Inter-Agency Standing Committee
ICRC	International Committee of the Red Cross
ICT	Information and communication technology
ICVA	International Council of Voluntary Agencies
IDP/s	Internally displaced person/s
IHL	International humanitarian law
IHRL	International human rights law
IRL	International refugee law
JRS	Jesuit Refugee Service
MARA	Monitoring, Analysis and Reporting Arrangements
MRM	Monitoring and Reporting Mechanism
MSF	Médecins sans Frontières
NGO	Non-governmental organization
OCHA	Office for the Coordination for Humanitarian Affairs
OECD/DAC	Organization for Economic Cooperation and Development/the Development Assistance Committee
OHCHR	Office of the High Commissioner for Human Rights
PHAP	International Association of Professionals in Humanitarian Assistance and Protection
PII	Personally identifiable information
PIM	Protection information management
PoC	Protection of civilians
SMART	Specific, Measurable, Achievable, Relevant, Time-bound
SMS	Short Message Service
UAV	Unmanned aerial vehicles
UN	United Nations
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations Children's Fund
UNPOs	United Nations Peace Operations
UNSG	United Nations Secretary-General

GLOSSARY

Some of the terminology used in this document is generic and may differ from the specific wording used by other organizations.[1]

TERM	DEFINITION
Authority	**Military, police and other State security forces, as well as judicial institutions and ministries with specific responsibilities, such as ensuring access to justice and effective remedies, emergency medical assistance and other services essential to the safety and well-being of the population.** "Authorities" may also refer to all weapon bearers – State entities, armed forces, peacekeepers and other multinational forces, and armed groups and other non-State actors – who are able to launch hostile action against persons or a population, and who are responsible for protecting those who fall under their control.
Causal logic	**A strategic exercise carried out before and during protection activities, to set out the pathways and milestones for the way a particular outcome is expected to be achieved, to identify the sequence of actions to be undertaken (and the assumptions inherent in them), including the various sectors and disciplines that may need to be mobilized to contribute to the desired outcome, and to identify the roles of different actors.** This analysis should underlie all actions taken to achieve the outcome in question. It is sometimes also referred to as the "theory of change'.
Bias	**Any systematic distortion of information, whether intentional or not.**
Community identifiable information (CII)	**Data and information that can be used to identify, classify or track a community or distinct group through demographically defining factors – whether geographic, ethnic, religious, economic, political or military – exposure of which can be life-threatening.** It is sometimes also referred to as "demographically identifiable information" (DII).
Critical services	**Services that address important, fundamental needs of individuals after their life-saving needs (food, water, shelter) have been met.** These services may range from health care to psychosocial services, security measures, tracing services for missing people, documentation services for those lacking essential identity documents, legal services for those in need of legal aid or advice on how to access accountability and redress mechanisms.
Crowdsourcing	**The practice of obtaining information, ideas and services from large (often online) groups of people.** Crowdsourcing has two main dimensions. Digitally connected communities can be used to either generate data – actively or passively – or to analyse them. The process relies on mobile phones, internet-capable devices, online networks, and internet-based applications. Where volunteerism and access to such technologies coexist, skilled internet users, "netizens", become substantial sources of information.
Data	**Facts and information, such as numbers, measurement details and observations.** Data can be qualitative or quantitative, and may include personal data.
Data and information management	**Any operation – by automated or other means – that is performed upon data or sets of data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available, aligning or combining, or erasing.**

---

1 Sources include: Harvard Humanitarian Initiative, *The Signal Code: A Human Rights Approach to Information during Crisis*, January 2017; ICRC, *The ICRC and Data Protection*, August 2017; PIM, *Commonly-used Protection Information Management Technology*, June 2016; *Privacy International website*; UN, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*, UNHCR, May 2015.

TERM	DEFINITION
Data breach	**A breach of security leading to the accidental or unlawful destruction, loss or alteration of – or to the unauthorized disclosure of or access to – personal data or sensitive information transmitted, stored or otherwise processed.**
Data controller	**The natural or legal person or the entity that, alone or jointly with others, determines the purposes and means of processing personal data.**
Data protection	**The process of protecting individuals' personal data that are collected, used, stored and shared, including by humanitarian and human rights organizations.** Protecting the personal data of individuals is an essential part of protecting their lives, physical and mental integrity, and dignity. This is why safeguarding personal data is of fundamental importance for protection organizations.
Data protection impact assessment (DPIA)	**An important tool used prior to carrying out data processing, in order to identify and address all data protection risks, including by implementing risk mitigation measures.** DPIAs are now a requirement in many jurisdictions as well as under the rules of a number of protection actors. They are sometimes referred to as "Privacy Impact Assessments".
Data security	The prevention of unauthorized access to or use of data and information, **and to or of the equipment used for data processing.** This relates in particular to physical security, access rights to databases, computer security or cyber security, the duty of discretion and the conduct of staff. Data security also refers to the preservation of the confidentiality, integrity and availability of information.
Data subjects	**An individual person who can be identified, directly or indirectly, in particular by reference to personal data.**
Evaluation	**The systematic and objective assessment of an ongoing or completed project, programme or policy, and of its design, implementation and results.** Its aim is to determine the relevance and fulfilment of objectives, development efficiency, effectiveness, impact and sustainability.[2]
Information	**Data that have been given some meaning as a result of their being organized and processed, and through relational connection.**
Legitimate basis	Personal data may be processed (collected, used, stored and transferred) only if there is a **legitimate basis** for doing so (including informed consent, vital interest, etc.; see under Standard 6.9.). Legitimate bases may be specified in international, regional or domestic legal frameworks for data protection or in the internal rules or policies of humanitarian organizations.
Metadata	**"Structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is [sic] often called 'data about data' or 'information about information'".**[3] Metadata are used to summarize basic information about data, which can make tracking and working with specific data easier. Some examples include: means of creation of the data; purpose of the data; time and date of creation; creator or author of the data; location on a computer network where the data was created; standards used; and file size.

---

2   Based on the definition contained in OECD, *Glossary of Key Terms in Evaluation and Results Based Management*, Paris, 2002, pp. 21-22.

3   Definition used by the National Information Standards Organization, a non-profit association accredited by the American National Standards Institute (ANSI). Taken from NISO, *Understanding Metadata*, NISO Press, 2004, http://www.niso.org/publications/press.

TERM	DEFINITION
Personal data	Personal data, also known as personally identifiable information (PII), include the following: biographical data, such as name, sex, marital status, date and place of birth, country of origin, country of asylum, individual registration number, occupation, religion, and ethnicity; biometric data, such as a photograph, fingerprint, facial or iris image; and any expression of opinion about an individual, such as an assessment of their legal status and/or specific needs.
Primary duty bearers	**Those who hold the primary obligation and responsibility to respect, protect and fulfil the rights of persons on their territory or under their jurisdiction or control.** Under international law, authorities at all levels of government are primary duty bearers. In addition, all State and non-State parties to conflicts have additional responsibilities under IHL.
Processing data	**Any operation that is performed on personal data, such as collecting, using, sharing, storing, archiving or deleting data.**
Protection actor	**Humanitarian or human rights actors engaging in protection activities or pursuing protection strategies.**
Protection data and information	**Data (and information) collected, used, stored or shared by humanitarian and human rights organizations that pertain to protection risks, rights violations and the situation of specific individuals/groups.** Protection data and information may include personal data, CII or data and information on a specific event, a general situation or a particular context.
Protection outcome	**A reduction of the risk, including through improved fulfilment of rights and restitution, for victims.** It includes reducing the threats people face, reducing people's vulnerabilities to these threats, and enhancing their capacities.
Pseudonymized data/ pseudonymization of data	**The replacement of any identifying characteristics of data with a pseudonym or a value that does not allow the data subject to be directly identified.**
Risk	**The probability of violation or threat, abuse, harm and suffering.**
Sensitive protection data and information	**Protection data or information, unauthorized access to or disclosure of which is likely to cause harm, such as discrimination, to persons such as the source of the information or other identifiable persons or groups, or adversely affect an organization's capacity to carry out its activities or public perceptions of its character or activities.** Certain data and information may be considered sensitive in one context but not in another.

INTRODUCTION

In armed conflict or other situations of violence, the protection of civilians who may be exposed to harm and suffering, including violations of their rights, is critical. However, States and other duty bearers often lack the capacity – or the will – to ensure that protection. In some cases, they may even perpetrate violence or other abuse themselves.

In recent years, the protection response to crises – by governments, international and non-governmental organizations – has increased, as have the number and diversity of humanitarian and human rights actors involved in protection activities. While coherence and coordination among these have improved, there are still wide differences in approaches and aims – and this can cause confusion. In a worst-case scenario, the absence of common professional standards can lead to situations in which protection work could actually harm the people and communities it seeks to protect.

Ensuring uniform quality of the work being carried out requires professional competence and adherence to commonly agreed, overarching professional minimum standards that are applicable to all. Concerted effort to devise such standards began in 1996 with a series of workshops led by the ICRC. These resulted in the formulation of the generally accepted – and still current – definition of protection as encompassing "all activities aimed at ensuring full respect for the rights of the individual in accordance with the letter and the spirit of the relevant bodies of law, i.e. human rights law, international humanitarian law, and refugee law. Human rights and humanitarian organizations must conduct these activities in an impartial manner (not on the basis of race, national or ethnic origin, language or gender)."

Various other initiatives followed, culminating in the publication, in 2009, of the first edition of *Professional Standards*. A second edition was issued in 2013 and work on the third edition began in 2015, the result of which is the full version of this document.

AIMS AND LIMITATIONS OF THE STANDARDS

The objective of *Professional Standards* is to establish a firm, shared basis for protection work in armed conflict and other situations of violence to maximize the effectiveness of that work for its beneficiaries. It consists of a series of ***standards*** – the minimum obligations that all humanitarian and human rights actors engaged in protection work must meet; ***guidelines*** – useful and, in some cases, essential reference criteria for use by actors according to the nature of their work; and ***explanatory notes*** that describe the main challenges that the standards and guidelines are designed to tackle, the limitations and constraints of the standards and guidelines, and the dilemmas they may pose to protection actors.

The standards should be considered umbrella standards and minimum obligations applicable to all those involved in protection work. They are supplementary to and complement other existing standards used by actors (notably, the *Sphere Handbook*).[4] *Professional Standards* should *not* be considered operational guidance. It does not define the extent to which actors should overlap in their work, nor does it advocate uniformity

---

4   http://www.sphereproject.org/handbook/

of approach, nor attempt to regulate or restrict initiatives. Instead, it aims to encourage implementation of a diverse range of approaches and activities according to a baseline, to ensure the safest and most effective response possible.

Professional Standards is aimed mainly at those engaged directly in protection activities but will be useful to all humanitarian actors, insofar as they must all incorporate basic safety and protection considerations in their work and daily activities. It can be used as a reliable reference in developing internal policies, drawing up guidelines and organizing training, and in explaining the principles of protection work to stakeholders. Although drafted with a focus on armed conflict and other situations of violence, the standards can also apply in disaster situations, in which human rights principles must be at the centre of all efforts to help vulnerable people.

WHAT IS NEW IN THIS EDITION?

This third edition involved a considerable rewrite and includes significant new issues and content. It takes into account the changes that have occurred in the environment in which protection actors operate and now reflects the distinctive characteristics of human rights and humanitarian actors engaged in protection work. Given the rapid developments in information communication technology and concurrent growth in data-protection law, comprehensive guidelines on protection information management have also been incorporated. There is now a stronger emphasis on measuring the outcome of protection activities in terms of the extent to which identified risks have been reduced, and on monitoring and evaluation. There are more detailed orientations on the need to uphold a principled approach to protection work when interacting with UN peace operations and other multinational forces. This edition also seeks to clarify how counter-terrorism legislation may affect the activities of protection actors.

The document comprises seven chapters, with the following headings:
- Overarching principles in protection work
- Managing protection strategies
- Outlining the protection architecture
- Building on the legal base of protection
- Promoting complementarity
- Managing data and information for protection outcomes
- Ensuring professional capacities

OVERARCHING PRINCIPLES IN PROTECTION WORK

This chapter describes the central principles of humanity, impartiality and non-discrimination and their interplay; reiterates the fundamental obligation of protection actors to avoid aggravating the situation of those they are seeking to help; and highlights the role of communities and individuals at risk in the protection process.

RESPECTING THE PRINCIPLES OF HUMANITY, IMPARTIALITY AND NON-DISCRIMINATION

The principles of humanity, impartiality and non-discrimination are central to protection work and common to all protection activities and strategies. These three principles underpin international humanitarian law (IHL) and are crucial to establishing and maintaining access to people at risk, and addressing their protection concerns. Neutrality and independence, however, while also important in terms of gaining and maintaining access to victims of armed conflict and other situations of violence, are not given the same weight by all organizations. Nevertheless, protection actors must be both transparent and consistent in their approach to these principles.

Ⓢ

1.1. Protection actors must ensure that the principle of humanity is at the core of their work.

The principle of humanity – that all people must be treated humanely in all circumstances – remains fundamental to effective protection work, placing the individual at risk at the centre of protection efforts. It demands that priority be given to protecting life and health, alleviating suffering and ensuring respect for the rights, dignity and mental and bodily integrity of all individuals in situations of risk.

Ⓢ

1.2. Non-discrimination and impartiality must guide protection work.

The principle of non-discrimination guards against adverse distinction in the treatment of different groups or individuals, on the basis of race, colour, sex, age, language, religion, political or other opinion, national or social origin, property, birth, disability, health, sexual orientation, gender identity or other status.

The principle of impartiality aims to ensure that a protection activity addresses all relevant rights and obligations, as well as the specific and most urgent protection needs of communities and individuals at risk of or subject to violations and abuses. Humanitarian and human rights actors must therefore define the protection activities to be undertaken in their area of responsibility, following an assessment of needs using objective criteria. Such an assessment, which may require consideration of specific vulnerabilities or risk factors, e.g. gender or age, will help protection actors ensure that critical needs are prioritized and addressed, and that their responses do no harm.

Of course, there are challenges inherent in respecting these principles – often generated by lack of access to people affected, insecurity, logistical constraints, as well a perception of bias on the part of protection actors, in terms of who and what they choose to focus on. Consequently, protection actors must take steps at an early stage to mitigate potential discriminatory effects or risks of partiality, and avoid bias in how they collect and/or assess the information on which they base their activities.

S

1.3. Protection actors must ensure that their activities do not have
     a discriminatory effect.

In all their analytical, practical and communication activities protection actors must
take care to ensure that they do not create or reinforce existing discriminatory practices.
It is the collective responsibility of all actors engaging in protection work to ensure that
no high-risk group is overlooked, and to ascertain that the overall response in a given
context is non-discriminatory. In especially challenging situations where 'triage pri-
oritization' is necessary, the criteria guiding such choices must be non-discriminatory
and based on the urgency and severity of carefully assessed needs.

AVOIDING HARMFUL EFFECTS

S

1.4. Protection actors must avoid harmful effects that could arise from
     their work.

In everything they do, protection actors must endeavour, above all, to avoid exacerbat-
ing or even creating additional protection risks for vulnerable people. They are ethically
and legally obliged to take measures to avoid such negative consequences – especially
when planning, analysing, implementing and monitoring their activities.

S

1.5. Protection actors must contribute to the capacity of other actors to
     ensure that no harmful effects derive from their actions.

There is, arguably, a protection dimension to every humanitarian crisis, and it is up to
protection actors to promote a comprehensive approach to it by all those involved. This
means encouraging humanitarian actors to view their response through a 'protection
lens' and take account of protection concerns as part of their fundamental responsi-
bility to do no harm.

PUTTING THE POPULATIONS, COMMUNITIES AND INDIVIDUALS AFFECTED AT THE CENTRE OF PROTECTION ACTIVITIES

S

1.6. Protection work must be carried out with due respect for the dignity of
     individuals.

The principle of humanity underpins all humanitarian and human rights activities.
Respecting the dignity of people in situations of extreme vulnerability by taking the
time to listen to and interact with them, facilitating their access to relevant information
and supporting their capacity to make free and informed choices demonstrates recog-
nition of shared humanity.

S

1.7. Protection actors must seek to engage in dialogue with persons at risk and ensure their participation in activities directly affecting them.

Often, people at risk are well aware of the threats they face and what needs to be done to improve their situation. It is therefore important to engage in dialogue with the individuals and communities affected – via official and informal representatives – to identify needs and any self-developed effective actions. Such information will help in the planning, design and implementation of protection activities.

By actively engaging populations at risk in protection activities, protection actors are also giving people at risk a means to judge them on their performance, which serves to increase the accountability of these actors. The latter should therefore ensure that accessible and easy-to-use mechanisms are available to facilitate the submission of complaints, suggestions, etc. by all members of the communities affected.

G

1.8. Protection actors should consider building on the capacities of individuals and communities to strengthen their resilience.

Given that it is often the people at risk themselves who have the clearest understanding of the threats they face and what is required to mitigate them, protection actors should assess the individual and collective capacities for protection that exist. Where possible – and bearing in mind that it is the responsibility of the authorities to protect individuals and the population as a whole – they should try to reinforce these capacities, while engaging the authorities at all levels and being careful to avoid reinforcing inequitable power relations within a community.

Ideally, community-based protection should originate within and be led by people from the communities affected. Even in circumstances where it is not possible – owing to displacement or the threat level – protection actors should at least attempt to better engage communities in their own protection and seek out the perspective of people affected, with a view to moving towards greater community control of protection strategies over time.

G

1.9. Whenever appropriate and feasible, protection actors should contribute to and strengthen the possibility for populations affected to access information that can help them avoid or mitigate the risks to which they are exposed.

Although the people at risk may have a better understanding of the threats they face than external actors, they will still require information from the latter in order to make informed choices on how best to cope. If it will help them in this regard, protection actors should share with communities their reading of the situation, and other relevant information.

G

1.10. Protection actors working with populations, communities and individuals affected should inform them about their rights and the obligations of duty-bearers to respect them.

Protection actors should inform the people with and for whom they work of their rights and of the obligations of the duty-bearers. This may also imply working with various local actors and may take some time, especially when working with people who may not be well informed of their rights under domestic and international law.

MANAGING PROTECTION STRATEGIES

This chapter emphasizes the importance of detailed, context-specific and continuous analysis and planning by protection actors before they develop or implement a response to protection concerns. It reminds protection actors to focus on their area of competence while seeking complementarity with others, as appropriate and necessary, to achieve protection outcomes. Finally, it highlights continuous evaluation and learning from protection strategy implementation as a basis for ensuring accountability and incorporating lessons into future strategies.

MANAGING PROTECTION STRATEGIES

Monitoring and evaluation are essential for protection actors to be able to identify and make changes and improvements to programmes in real time, and to learn lessons for future application. These revised Standards outline a common basis from which to conduct analysis of risk patterns, create a causal logic describing the pathways and milestones to achieve protection outcomes, monitor programmatic responses and evaluate protection outcomes and impact with a view to improving understanding and accountability.

S

2.1. Protection actors must develop a detailed and context-specific analysis of the risk patterns people are experiencing prior to developing or implementing a response to protection concerns. They should focus on their particular area of competence while soliciting information and sharing findings, as appropriate, with other competent actors. They must use this analysis to determine priorities and establish corresponding strategies to address these risks, which includes mobilizing other key actors of pertinence to the problem being addressed.

Comprehensive and thorough problem analysis is crucial for protection action, which is characterized by nuanced elements in complex and highly dynamic contexts involving myriad actors. Context-specific analysis based on the latest possible data is key in the early stages, while continual analysis is essential to being able to make adjustments over time. The right course of action can only be determined following clear identification of the risks, causes, motivations and circumstances concerned, as well as the primary actors involved. When protection analysis is robust, risks can be better prioritized, desired outcomes more reliably established and a causal logic for a strategy to reduce risk more easily developed.

The four main elements to ensure a robust analysis for protection work are as follows:
• *Analysis of the different ways in which people are at risk.* To identify patterns of violations and abuse, who is vulnerable and why, what capacities people can bring to bear to reduce risk themselves and what actions they think are required to address the identified problems, analysis should start, as far as possible, from the perspective of the people affected. Importantly, there should be a two-way information flow, so that the people affected by crises feel empowered to address the risks they face. Protection actors must be wary of focusing exclusively on pre-defined population groups that are typically assumed to be the most vulnerable and marginalized. They must avoid drawing premature conclusions, endeavouring instead to tailor the response to the specific risk patterns identified.

- *Analysis of the individuals or institutions, including State and non-State actors, and of their roles and responsibilities in relation to the protection concerns being examined*. The behaviour and attitude of these various parties may involve actions of both commission (overt action) and omission (failure to act), so protection actors should take care to analyse how the existing policies and practices – or lack thereof – of the authorities concerned may be driving threats or creating or exacerbating vulnerabilities. The capacity, commitment and willingness of primary duty bearers to address these problems should be included in the analysis, as should consideration of incentives and disincentives to change their behaviour. This analysis should be informed by regular dialogue with the duty bearers, where possible.
- *Identification and analysis of the ability of protection actors and other stakeholders who may exercise influence or be obstructive in, or contribute to, addressing the risk factors identified, including the protection activities they are already undertaking.* This will inform the design of subsequent strategies and efforts to maximize complementarity with other actors.
- *Identification of interrelated problems, including those that do or do not have the same causes and/or arise from the same dynamics, should be taken into account while setting priorities and designing appropriate strategies*. Framing a certain pattern of behaviour in a broader context is critical to understanding how this behaviour should be addressed.

(G)

2.2. **Protection actors should develop the causal logic for the action they are taking to address the protection concerns identified. This causal logic should describe the pathways and milestones to address specific risk factors and achieve the desired outcome of reduced risk. It should serve as the basis for establishing SMART objectives, defining the roles of different sectors or actors contributing to the desired outcome, and identifying assumptions inherent in the strategy.**

Reducing the threats people face, reducing their vulnerability to these threats and enhancing their capacity to address them may require a variety of disciplines working towards a common desired outcome. Developing a context-specific causal logic (or theory of change) can help with the difficult task of pulling all the relevant actions together into a coherent strategy. This causal logic should:

- describe the detailed pathway and milestones between the specific ongoing violations and abuses and the risk factors people are experiencing and the desired outcome of reduced risk;
- describe the sequence of actions, including the multiple sectors and disciplines that may need to be mobilized – at various levels – to contribute to the desired outcomes. The causal logic should identify the spheres of control and influence of the actors contributing to protection outcomes, and issues or actors that are beyond these actors' control and influence. This enables protection actors to situate and understand their role within the broader dynamics of the context, thus creating a sound basis for cultivating complementarity among actors, which will help establish a collective vision, create mutual understanding and, ultimately, reduce risk;
- explicitly articulate the assumptions inherent in the sequence of actions, the roles of the different actors and the results these are expected to yield.

Once the causal logic has been established, the protection strategy can be drawn up. It must include the **desired outcome (or impact)** in terms of reduced risk or violations or abuses; **SMART objectives** that will contribute to the desired outcome; and **specific activities** to be undertaken and the **outputs expected**. Finally, the strategy should be continually adapted and updated as the situation evolves and/or understanding of the situation improves.

MONITORING

Ⓢ

2.3. Protection actors must carry out continuous analysis of changes in risk patterns and undertake continuous programme monitoring in order to adjust strategies and activities as required.

In protection work, establishing measurable results and attributing them to particular actors is undoubtedly challenging but eminently achievable. Having carried out a robust protection analysis (which will allow better definition and description of the risk patterns involved), established the causal logic (which will serve as a basis to monitor critical milestones leading to reduction of risk) and drafted the protection strategy, the next step is to ensure the strategy includes the necessary information management and monitoring systems. These should encompass the choice of indicators, methods and procedures for collecting information, and how the data will be used and by whom.

Monitoring is essential to ensure that programmes are developed and implemented in an iterative way that is responsive to new information and developments in the context. It also allows protection actors to gauge whether their programme is achieving the desired results, whether the causal logic will lead to risk reduction, or whether the assumptions and strategy need to be revised.

Continuous analysis and programme monitoring should also detect any unintended or negative changes in the context.

EVALUATION AND LEARNING

Ⓢ

2.4. Protection actors must seek to learn from their strategies to enhance protection, including by carrying out evaluations of ongoing and completed programmes, with a view to ensuring accountability for the actions taken to address protection concerns and incorporating what they have learnt in the implementation of their strategies.

Taking time out specifically for reflection, together with continuous protection analysis, is essential to ensuring a high degree of adaptability in a dynamic context. A conscious effort to cultivate and encourage adaptability in programming emphasizes evidence-based decision-making and helps ward off demotivation.

Regular investment in learning – involving people affected, staff and other stakeholders – enhances ownership and responsibility for protection strategies and encourages critical discussion. By systematically and objectively evaluating the entire protection action, lessons learnt can be captured and formulated more effectively, and the contributions made by various actions and actors to achieving the desired protection outcome better understood.

Note, however, that evaluating protection strategies is particularly difficult and involves the common (in humanitarian and human rights work) challenge of understanding the relationship between cause and effect, as well as whether and how a result may be attributed to a certain action or actor. It is important, therefore, first to assess whether protection outcomes *can* be evaluated. Having a causal-logic pathway, continual-analysis cycle and clearly articulated desired outcomes and expected results will enhance the evaluability of a programme.

Finally, evaluation should be conducted by trained staff and in accordance with the principles of utility, propriety, feasibility and accuracy.

OUTLINING THE PROTECTION ARCHITECTURE

This chapter outlines the 'global protection architecture' within which all those involved in protection work operate, describing how the various participants relate to that architecture and to each other. The need to understand the role of UN peacekeeping operations and other internationally mandated military and police forces engaged in protection is underlined, and ways to engage with them effectively are explained.

The global protection architecture is based on rights and obligations set out in international humanitarian law (IHL), international human rights law (IHRL) and international refugee law (IRL). It comprises various national and international actors with protection roles and responsibilities: the State (the primary duty bearer), *de facto* authorities, all parties to armed conflicts (including non-State armed groups), UN peacekeeping operations and other internationally mandated forces engaged in protection, and humanitarian and human rights organizations.

RELATING TO THE PRIMARY DUTY BEARERS

Ⓢ

3.1. Protection actors must determine and adjust their approach based on an understanding of the existing protection architecture and the role and responsibilities of primary duty bearers.

Under international law, the State and its authorities, e.g. military, police, other State security services, judicial institutions, hold the primary obligation to respect, protect and fulfil the rights of persons on their territory or under their jurisdiction. Protection actors must understand the role of all of these and seek to establish an interface with them, particularly with a view to reminding these duty bearers of their responsibilities and the need to meet them fully. How protection actors go about this will depend on the issues to be addressed and their own unique capacities and mandate. In any case, they should always strive for complementarity in their collective efforts to improve protection outcomes.

Ⓢ

3.2. Protection actors must at all times avoid action that undermines the capacity and will of primary duty bearers to fulfil their obligations.

In armed conflict and other situations of violence those engaged in protection work should seek to *support* the relevant authorities in terms of fulfilling their obligations rather than *replace* them. Paramount is the avoidance of any action that could undermine or remove responsibility from the primary duty bearer.

Ⓢ

3.3. Protection actors must not substitute for the role of the authorities when the latter have the requisite capacity and will to assume their responsibilities.

Direct substitution for the authorities, i.e. relieving them of their responsibilities rather than helping them to meet them, should only occur in extreme circumstances. Ideally, substitution activities should be accompanied by efforts aimed at building or strengthening the capacities of the authorities and national protection systems to discharge their responsibilities to protect people at risk.

(G)

3.4. Protection actors should include some form of communication with the relevant authorities in their overall approach.

Communication with the authorities, whether formal or informal, direct or indirect, should be a key part of the work of protection actors, especially when they are working in substitution for the formal authorities. When establishing such communication, it is vital that protection actors are transparent about their activities, mandate and/or mission statement.

(G)

3.5. Protection actors should ensure that, whenever feasible, they establish a protection dialogue with armed non-State actors.

To secure access to all areas, improve the security of operations and achieve protection outcomes for the population, it is often essential for protection actors to establish a dialogue with all those who have actual or potential responsibilities under IHL. This includes non-State armed groups. Engaging with them to remind them of their obligations should be based on a detailed examination of the impact of these groups on people's lives, their motivations and their strategies, as well as a good understanding of the context in which they are operating.

It is important to ensure in any interaction with armed non-State actors that messages are coherent and that the staff involved are competent for and fully supported in this challenging task.

(S)

3.6. All protection actors must specify their roles, protection objectives, institutional priorities and means of action.

To facilitate interaction and complementarity, all protection actors should clearly specify their operational intent, priorities and objectives, sharing them as appropriate with other protection actors, relevant authorities, communities affected, and individuals and other stakeholders concerned.

INTERFACE WITH UN PEACE OPERATIONS AND INTERNATIONALLY MANDATED MILITARY FORCES AND POLICE SERVICES

UN Peace Operations

UN peace operations (UNPOs) are required to respect and protect civilians while conducting their operations, in accordance with IHRL and, where applicable, IHL. In addition, the Security Council has explicitly mandated most UN missions to protect civilians under threat of physical violence, from both State and non-State actors, and to promote and protect human rights. This 'protection of civilians' (PoC) mandate may also include a specific focus on particular themes or vulnerable categories of people. Most UNPOs have mandates and tools that are relevant to protection, and they often undertake complementary protection activities.

In UNPOs, implementing a PoC mandate can involve, for example, the show or use of force to protect civilians under threat of physical violence, advocacy by civilian and uniformed actors to deter such violence or, longer-term, more structural efforts such as training, mentoring or supporting national military and security staff.

OTHER INTERNATIONALLY MANDATED MILITARY FORCES AND POLICE DEPLOYMENTS

UN Security Council mandates provided to international forces operating outside the UN system have, in the past, included language encouraging the protection of civilians through adherence to IHL and other legal obligations, and sometimes even an explicit mandate to protect against physical threats posed by other parties.

S

3.7. Protection actors must understand the role and responsibilities of UN peace operations and internationally mandated military forces and police services in ensuring the protection of civilians where they are deployed.

Protection actors must familiarize themselves with the structure, components and coordination mechanisms, and with the relevant documents and policies, of UNPOs and internationally mandated military forces and police services with regard to the protection of civilians – both at the general/policy level and in-country.

Humanitarian action alone cannot protect civilians from the effects of armed conflict, so engaging with UNPOs and other internationally mandated military forces and police services is a necessity. However, there has long been concern among humanitarian and human rights actors that such engagement can affect their independence and impartiality, and how these are perceived. This is particularly worrying for those humanitarian organizations that rely on their neutrality to gain access to the population and to all armed actors.

To prevent any blurring of roles and responsibilities, and with a view to improving and supporting everyone's capacities and activities, humanitarian organizations must seek to engage in dialogue with UNPOs and other internationally mandated military and police forces. Whatever the context, any dialogue and interaction must not undermine adherence to the humanitarian principles of independence and impartiality nor expose populations affected or humanitarian workers to greater risks.

G

3.8. Protection actors should proactively engage UN peace operations with a view to promoting positive protection outcomes for populations at risk.

Open communication channels and established protocols between protection actors and UNPOs will help the latter analyse the PoC element of their mission and thus prioritize the response. Areas of complementarity will also be more easily identified.

S

3.9. Protection actors should ensure some level of interaction with internationally mandated military forces and police services in order to facilitate a protection dialogue aimed at securing respect for IHL, IRL (where applicable) and IHRL, as well as at ensuring more informed protection efforts.

A consistent and constructive dialogue with internationally mandated military forces and police services should involve promotion and respect for IHRL and, where applic-able, IHL and IRL by such actors.

S

3.10. When engaging with UN peace operations and internationally mandated military forces and police services, protection actors must do so in a manner that does not pose further risks to civilians or undermine the ability of protection actors to operate.

Given that UNPOs and internationally mandated military and police services may not be perceived as neutral and impartial by all sectors of the population and parties to the fighting, protection actors will need to determine – and regularly assess – whether their engagement with such operations and services conveys an image of partiality and thus adversely affects those actors' acceptance and the security of the humanitarian community.

OTHER ACTORS

S

3.11. Protection actors must take into account the various protection roles of political, judicial and economic actors.

Domestic and international actors in political, judicial and economic realms can, among other important roles, help create an environment conducive to protection and compli-ance with international law. These roles must be taken into account by protection actors when planning and implementing activities, to maximize complementarity while also respecting the principles of humanitarian action.

BUILDING ON THE LEGAL BASE OF PROTECTION

This chapter emphasizes the importance of understanding the applicable laws and standards in a given context, as well as the policies for implementing them, so that protection actors are in the best possible position to remind the authorities, and others, of their obligations.

KNOWING THE LEGAL FRAMEWORK

Ⓢ

4.1. Protection actors must be familiar with the various legal frameworks that are applicable.

There are many international standards that require States and other actors to protect individuals or communities in armed conflict or other situations of violence. Some are specific to certain categories of person, situations, violations and weapons. While a detailed knowledge of the applicable laws is generally not necessary, all protection staff must understand the basic principles and standards of the universal protection norms that create binding international obligations:

- International humanitarian law (IHL) is a body of law designed specifically for situations of armed conflict. It aims to ensure respect and protection for persons who are not, or are no longer, taking direct part in hostilities, and to regulate the means and methods of warfare during international and non-international armed conflict.
- International human rights law (IHRL) lays down obligations, primarily for States, to respect, protect and fulfil the human rights and fundamental freedoms of individuals in their territory or within their jurisdiction.
- International refugee law (IRL) regulates protection due to persons who, owing to a well-founded fear of persecution, find themselves outside the territory of their country of nationality.

REFERRING TO THE LAW WITH CONSISTENCY AND IMPARTIALITY

Ⓢ

4.2. A protection actor must be consistent and impartial when making reference to, reporting on or urging respect for the letter or spirit of relevant law, as applied to various parties to an armed conflict or other situation of violence.

Protection actors must not accept, even tacitly, one party breaching the law while reporting or condemning another for the same acts. This standard implies that a protection actor should analyse the effects on the population of the actions, or the lack of action, of the various perpetrators or parties to the conflict, in light of their obligations. If, as a result of this analysis, the protection actor decides to concentrate efforts on a particular risk group, type or gravity of violation or specific region in the larger conflict area, they must ensure that it is not implicitly weakening the protection available to others.

MAINTAINING COHERENCE AND ACCURACY

S

4.3. When protection actors take action to ensure that the authorities (including armed non-State actors) respect their obligations towards the population, their references to the law must be accurate. Messages and actions must be in accordance with the letter and spirit of the existing and applicable legal frameworks.

If a protection actor chooses to refer to the law and the obligations of the authorities, it must ensure that its references are correct and invoke the most relevant applicable legal framework. By being both coherent and accurate when addressing the authorities, the protection actor enhances its credibility and avoids confusion. To that end also, a degree of consultation is recommended among protection actors that are addressing the authorities on similar patterns of violations or abuse.

REFERRING TO RELEVANT REGIONAL AND DOMESTIC LAWS AND OTHER RELEVANT STANDARDS

G

4.4. When relevant regional and domestic law, or other relevant standards, reinforce overall protection, and are in conformity with international law, protection actors should include them in their work.

It is worth investing effort in assessing the relevance of regional and domestic law, standards and traditions (including social, religious and cultural norms) to the work of protection actors, in order to draw parallels between them and IHL and IHRL and thus emphasize the universal relevance of these international legal frameworks. Another good reason to take domestic laws into account when dealing with the authorities is that they – and the general population – are usually more familiar with their own legal standards and provisions.

Before invoking local standards, however, protection actors must first thoroughly assess their compatibility with different bodies of international law. They should identify those domestic normative frameworks that can serve to support their arguments, while advocating changes to those that fall short of international law and standards.

UPHOLDING EXISTING LEGAL STANDARDS

S

4.5. Protection actors must be aware that international law and standards cannot be lowered and must be respected and upheld. In certain cases, a series of progressive steps may be required in order to attain compliance with these norms over time.

Protection actors must make it clear in their dealings with the authorities, parties to a conflict and groups involved in other situations of violence that the norms embodied in international law and standards cannot be adapted or adjusted according to the domestic context. Protection actors may still, however, suggest realistic changes in law and policy that could ease compliance with relevant international law and standards while improving respect for the population affected.

PROMOTING COMPLEMENTARITY

This chapter explains why protection strategies should incorporate the contributions of various actors in order to reduce risk, and aims to establish some minimum standards for complementarity, built around managing interaction among humanitarian and human rights actors to facilitate the achievement of protection outcomes.

The multi-faceted nature of crises typically demands a variety of solutions. In terms of protection risks, a growing and diverse range of actors is now involved in providing these solutions. While those actors may all share similar objectives, they also have different identities, mandates, priorities, approaches and activities. This is often the reason why complementarity is required in protection work.

Seeking and enhancing synergies among protection actors can lead to greater benefits for the populations at risk. Gaps, potential overlaps, duplication and the danger of one actor's efforts disrupting or undermining another's can be identified and dealt with through any of the four Cs: coexistence, coordination, cooperation/collaboration or contractual partnership.

But there is no uniform approach to protection work, and care must be taken to respect and maintain the actors' various identities and principles, and to avoid blurring their individual responsibilities for the safety of the populations at risk.

COMPLEMENTARITY OF ACTION AMONG PROTECTION ACTORS

Ⓢ

5.1. Protection actors must take account of the roles, activities and capacities of others, avoiding unnecessary duplication and other potentially negative consequences, while endeavouring to build synergies.

Protection actors should share information at the operational level regarding their general protection strategy and their target areas and populations, so that other actors can incorporate it into their analyses and planning. This will also help ensure the actors' intentions and work are understood and that unnecessary overlaps do not occur. When planning or undertaking activities in a new context or with a new population, it is helpful to consult those already there, to identify potential gaps in the response.

COMPLEMENTARITY OF PRINCIPLES AMONG PROTECTION ACTORS

Ⓢ

5.2. Protection actors must acknowledge and respect the efforts of those among them who choose to subscribe to the principles of independence and neutrality.

While humanity, impartiality and non-discrimination are central to all protection work, some actors also maintain the principles of neutrality and/or independence as core values. Their commitment to doing so should be acknowledged and respected. In particular, actors that are not neutral in a crisis – or not perceived to be so – should be careful not to publicly implicate others in their actions.

COMPLEMENTARITY OF ANALYSES

(G)

5.3. Protection actors should seek to share their analyses in order to contribute to a better understanding of protection issues and their impact on various populations at risk.

The range of perspectives and approaches delivered by the various humanitarian and human rights actors doing protection work helps increase understanding and contributes to a more comprehensive response. Contextual analysis is critical for the effectiveness of that response. It should examine, primarily, the environment, pattern of violations and abuses, perpetrators, duty bearers and their capacity and willingness to protect, as well as the impact on the populations affected. The information gathered should be shared as appropriate, with due respect for confidentiality requirements.

MOBILIZING OTHER PROTECTION ACTORS

(S)

5.4. Other protection actors with the requisite competencies and capacities must be encouraged to get involved when important, unaddressed protection issues are suspected to exist.

Encouraging others to respond will help promote a more comprehensive response for those at risk. If significant gaps exist, actors with the requisite expertise and capacities to fill them may need to be mobilized. The overall aim is to share information and analysis of unaddressed protection concerns, not to direct the response of those encouraged to get involved.

PROVIDING INFORMATION ON PROTECTION SERVICES AND FACILITATING REFERRAL TO RELEVANT SERVICES

(G)

5.5. Protection actors should map critical services that exist in their area of operations, make this information available whenever appropriate and feasible, and proactively facilitate access to such services.

In all situations, protection staff should be able to provide information to those in need on the services available – both State-run and those offered by civil-society organizations. Ideally, referral information should be given after due assessment of the quality of these services and their conformity with professional standards. In some circumstances, protection actors should, whenever possible, also consider facilitating access to such services.

RESPONDING TO HARM AND VIOLATIONS

G

5.6. When a protection actor learns of allegations of abuse or of violations of IHL or IHRL, and it lacks the capacity or the requisite mandate to take action, it should alert other organizations that have this capacity or mandate.

Protection actors should take appropriate action when they learn of possible abuses or violations of IHL or IHRL. They may directly witness the violations or abuses, or observe the consequences suffered by the populations affected, or they may receive information from a third party. The type of action they subsequently take will depend on the circumstances and the mandate, role and capacity of the actor. It will also depend on the nature of the violation, and on the particular needs and capacities of the victim(s). It is important to recall that taking such action does not relieve primary duty bearers of their responsibilities.

Any reporting or referral should be done with these considerations in mind: preventing harm to populations affected; respecting the informed consent provided by sources of information; and protecting the security of staff.

MANAGING DATA AND INFORMATION FOR PROTECTION OUTCOMES

The overall objective of this chapter is to facilitate the principled, responsible and collaborative management of protection data and information. The chapter is divided into three parts: the general standards applicable to the management of all data and information used in protection work; the standards applicable specifically to the management of personal data and sensitive protection data and information; and guidance on assessing the risks associated with the management of protection data and information on risk-mitigation measures.

INTRODUCTION

What is protection and data information management and why is it important?

Collection and analysis of protection data and information is essential for evidence-informed protection work. Given the potential sensitivity of that data and information, it is imperative to ensure that it is handled appropriately at each step of the information management process. The exceptional circumstances in which protection actors operate create special challenges regarding that process. Overall and most importantly, the risks relating to requests for and the provision of information must be mitigated to ensure that the 'do no harm' principle is respected throughout.

Protection data and information – types of data, sensitivity and legal requirements

Before collecting data or designing a protection information management system, protection actors must determine what data will be required for a specific and defined purpose and what their level of sensitivity is. Protection actors must also identify the risks and establish proper safeguards to mitigate them. The more sensitive the data and information, the stricter the data protection rules and standards that will have to be applied.

Protection data and information comprises certain kinds of data and information collected, used, stored or shared by humanitarian and human rights organizations. It pertains to protection risks, rights violations and abuses, and the situation of specific individuals/groups. It may include personal data and/or 'community identifiable information'.

Personal data, or personally identifiable information (PII), are data relating to a person that can be identified from that data, from other information, or by means reasonably likely to be used related to that data, e.g. a name, ID number or location data. 'Data subjects', i.e. those whose personal data are processed, have rights with respect to the way their data are handled. Although not absolute, these rights should be considered and balanced with other human rights and fundamental freedoms, in accordance with the principle of proportionality. The professional standards set out in this document require the principles of data protection to be applied to all personal data, in line with international best practices and recent legal and regulatory developments.

Sensitive protection data and information are those that, if disclosed or accessed without proper authorization, are likely to cause harm to a person or a negative impact on an organization's capacity to carry out its activities. Note that the same types of data may have different levels of sensitivity in different contexts, and that sensitivity may change over time.

Sensitive personal data are those that, if disclosed, are likely to result in harm for the individual concerned. Consequently, many international instruments on data protection include stricter rules for the processing of such data. Note that sensitivity of data and appropriate safeguards will be context-dependent and may change over time, so they need to be considered on a case-by-case basis.

The use of ICT and other technologies

Information communication technologies undoubtedly offer enormous benefits to protection actors, improving efficiency, effectiveness and accountability, especially in areas where access for humanitarian actors and opportunities to freely engage with people affected are limited. Combining information gained through various digital tools with information collected directly from communities and individuals affected, and with other sources of information, is becoming standard good practice. However, these technological developments have also increased the risk to individuals' privacy and safety, resulting in legal and regulatory responses throughout the world. Protection actors must therefore have a good understanding of the risks that can result from the use of any tool or technology, old or new, before using it.

Who should apply these standards

The professional standards set out in this chapter are addressed to **all protection actors involved in handling protection data and information**, including personal data. They should also be applied, when appropriate, by **professionals working in humanitarian or human rights responses but not in traditional 'protection' work** and who process information collected from affected persons, witnesses or other sources. The principles and safeguards set out in this chapter should also be upheld by **service providers partnering protection actors in collecting or handling data and information** relating to specific threats and vulnerabilities giving rise to protection risks. They may also be relevant to **a range of other actors handling personal data or sensitive information**, such as other sectoral colleagues, donors, development actors, peacekeepers, and civil-society groups in various contexts. Likewise, **actors dealing with aggregated information for the purpose of trend analysis** should also be aware of possible risks and sensitivities associated with the information they handle and how to safeguard it.

🔒

Note: Professional standards that are derived from internationally accepted data protection standards and which therefore must be applied when dealing with personal data are identified below by a padlock icon.

SECTION 1 – GENERAL STANDARDS FOR THE MANAGEMENT OF DATA AND INFORMATION

This section presents the general standards that apply to the management of protection data and information, including the collection, use, sharing, storage, archiving and deletion (processing) of such information and data.

Competencies and capacities

(S)

6.1. Protection data and information management must be carried out only by skilled and trained staff, using appropriate information management systems and protocols.

In armed conflicts and other situations of violence, information is often sensitive and there may be a very high risk of causing harm if it is mismanaged. Data literacy and risk awareness are particularly important, therefore. Protection data and information, including personal data, should be collected only by trained staff with the requisite skills and experience. Interviews with victims and their relatives, witnesses or other sources should also be conducted only by such trained staff.

Inclusive people-centred approach

(S)

6.2. Protection data and information management must be guided by the interests and well-being of the population affected and other persons providing information, who should be given an opportunity to influence the design and approach of all stages of the data and information management process that affect them.

People affected by armed conflict and other situations of violence should be able to influence protection actors' approaches and decision-making through feedback mechanisms, whenever possible.

Clearly defined, specific purpose

(🔒)(S)

6.3. Protection data and information management must serve clearly defined, specific purposes and aim at achieving protection outcomes.

Protection data and information management must serve a specific purpose that has been clearly defined in advance, and protection actors must collect and process information only when necessary for the design and implementation of protection activities. Protection data and information and personal data can be used for purposes other than those specified at the time of collection *only if* such further processing is compatible with the original purpose and *certainly not if* foreseeable risks to the individual concerned outweigh the benefits. Information that is not necessary for the identified purpose should simply not be collected. In the interests of transparency, protection actors should, at the outset of data collection, consider and identify all possible future purposes and ensure that the consent obtained covers possible relevant future purposes.

Cooperation and exchange

(S)

6.4. Protection actors must avoid, to the extent possible, duplication of information collection efforts, in order to avoid unnecessary burdens and risks for victims, witnesses and communities.

Protection actors should avoid repeatedly asking sources of information the same questions and should seek to ensure that the information source does not need to provide the same information to multiple actors. To this end, protection actors should consult each other to determine who is to collect what type of information and for what pur-

pose. They should also determine how much information is already available, as well as if and how it can be shared.

Avoiding bias and discrimination

S

6.5. Protection actors must gather and subsequently process protection data and information in an objective, impartial and transparent manner, to avoid or minimize the risk of bias and discrimination. Management of protection data and information must be sensitive to age, gender and other factors of diversity.

In collecting and processing data and information protection actors must remain aware of the possible under- or over-representation of some categories of the population, and of the possibility of bias. This can stem from respondents, intermediaries or the protection actors themselves, or be due to discriminatory practices and power dynamics, as well as the methods used for data collection. Bias should be minimized by designing information collection procedures that ensure representative sampling, training and coaching staff appropriately and using a combination of methodologies and sources.

Protection actors must endeavour to identify instances of discrimination by ensuring the information they collect can be disaggregated on several bases: age, gender, sexual orientation, rural/urban, ethnicity, nationality, affiliations, etc.

G

6.6. Protection actors should, to the degree possible, keep the persons who provided information informed of the action that has been taken on their behalf – and of the ensuing results.

Follow-up action in the form of return visits, public communication or information campaigns allow the protection actor to keep those who have provided information up to date on what has been done and achieved. It also demonstrates respect for those who took part in the information collection process.

G

6.7. Protection actors should be explicit about the level of reliability and precision of the data and information they collect, use or share.

Protection actors should take measures, to the extent possible, to minimize the risk of presenting an incorrect or incomplete picture of the issues they intend to address. Any internal or external report should mention the reliability and precision of its contents in general terms. Tags may be used to identify the different levels of reliability. Every protection actor needs to balance this transparency requirement with the need to respect confidentiality and guarantee the safety and privacy of persons providing potentially sensitive information.

When the reliability, precision or currency of the information collected are limited, protection actors should take the necessary action to address any resulting gaps in the quality of the information that may affect the protection response.

SECTION 2 – SPECIFIC STANDARDS FOR THE MANAGEMENT OF PERSONAL DATA AND SENSITIVE PROTECTION DATA AND INFORMATION

🔒

The standards in this section are derived mainly from the principles of data protection, so protection actors *must* follow them when processing personal data and, when processing protection data and information that do not include personal data, apply them as a matter of best practice, to the extent required.

The internationally accepted basic principles of data protection when processing personal data may be summarized as follows:
• Lawful and fair processing
• Purpose specification
• General principle of legitimacy
• Data minimization and proportionality
• Data quality
• Transparency and information
• Data security
• Duty of confidentiality
• International transfers and sharing of data
• Accountability
• Rights of data subjects

Compliance with relevant legal frameworks

🔒Ⓢ

6.8. Protection actors must collect and handle information containing personal data in accordance with the rules and principles of international law and relevant regional and national laws on data protection.

Prior to collecting or processing personal data, protection actors must assess the international, regional and national legal frameworks for data protection for their applicability, and ascertain whether there are any specific contextual factors that might, at any stage, affect the safekeeping of the information collected.

Legal requirements may differ, depending on the protection actor concerned. International organizations usually enjoy diplomatic privileges and functional immunities under international law, but NGOs and private companies they contract, as well as private individuals, typically do not. This should be taken into account when assessing the risks associated with sharing or transferring data.

Legitimate and fair processing

Legitimate basis

🔒ⓢ

6.9. Personal data and sensitive information must be processed only if
there is a legitimate basis for doing so. If there is no legitimate basis
for doing so, they must not be processed.

Processing means any operation that is performed on personal data: collecting, using,
correcting, sharing, retaining, deleting, archiving, etc. Protection actors may rely on
the following legitimate bases to process personal data:
• Consent
• Vital interest of the person providing the data or of another person
• Public interest
• Legitimate interest
• Performance of a contract
• Compliance with a legal obligation

Consent of the person concerned – or, if they are unable to provide it, that of their legal
guardian – is the preferred legitimate basis for processing personal data. For consent
to be valid, it must be *informed* and *freely given*, based on a clear appreciation and
understanding of the facts, risks, implications and future consequences of an action.
For consent to be regarded as informed, the data subject must be told the identity of the
entity collecting the information, the purpose of the information collection exercise,
details of the potential risks and benefits of participating in it, the duration for which
the information will be used or stored, how and where it will be stored, and with whom
the data will or may be shared. Data subjects must also be reminded of their rights with
regard to the use, processing and storage of the data they provide.

Informed consent should always be obtained by suitably trained staff in ways that are
culturally appropriate and relevant, and using language and communication means
that are easy to understand. Details of the consent given and the level of confidentiality
required should be documented or recorded and accompany the information through-
out the process.

Above all, obtaining the necessary consent does not absolve protection actors from
their responsibility to assess and mitigate the risks for data subjects. If the risks of
collecting and processing personal data or protection information are determined to
outweigh the benefits, the information should not be processed, even if informed con-
sent has been obtained.

Alternative legitimate bases

In some situations, consent may not be meaningful or sufficient, or may not be obtain-
able. Complex data flows, involvement of multiple stakeholders and the susceptibility
of data or information to interception and misuse can also mean consent is not mean-
ingful. In such cases, the protection actor will require another legitimate basis to pro-
cess personal data, such as the vital interest of the source of information or of another
person; or pursuant to the public interest.

Transparent processing

🔒 Ⓢ

6.10. Data processing must be transparent to the persons concerned, who must be given a certain minimum amount of information about the processing.

Fair processing is based on the principle of transparency, which requires that a minimum amount of information concerning the processing be provided to the person concerned at the time of the collection, using easy-to-understand language and methods.

Data minimization

🔒 Ⓢ

6.11. Protection data and information must be adequate and relevant to the clearly defined, specific purposes for which they are collected and processed. This means that the data processed must not exceed the purposes for which it was collected.

Protection actors must determine the scope, level of precision and depth of detail of the information collection process, in relation to the intended use of the information collected. They must be able to distinguish what *might be interesting* and what is *necessary to know* – and only collect the latter – in order to achieve the defined outcome.

Data quality

🔒 Ⓢ

6.12 Personal data must be as accurate and up to date as possible. Inaccurate personal data must be corrected or deleted without undue delay.

Every reasonable precaution must be taken to ensure that inaccurate personal data are corrected or deleted without undue delay, taking into account the specific purpose for which they are being processed. To this end, protection actors should periodically review the information collected in order to assess if and to what extent it is reliable, accurate and up to date.

Data retention

🔒 Ⓢ

6.13. In order to ensure that personal data and sensitive data are not kept longer than necessary, a minimum retention period must be set, at the end of which a review must be carried out to determine whether the retention period should be extended or the data erased or archived.

Personal data should be deleted when: they are no longer necessary for the purpose for which they were collected; that purpose can no longer be achieved; subjects withdraw their consent or object to further use of their data; applicable data protection legislation or the regulations of the organization concerned provide for deletion. However, personal data may not be deleted when there is a legitimate reason for archiving them.

Data security

🔒Ⓢ

6.14. Personal data and sensitive information must be processed in a manner that ensures an appropriate degree of security for as long as data are retained.

Data security is a crucial component of an effective data protection system. Security safeguards, appropriate to the sensitivity of the information and the format in which they are kept, must be in place prior to any collection of information to ensure protection from loss or theft, unauthorized access, disclosure, copying, use or modification. It is the responsibility of the protection actor to ensure that data is processed with the legal, technical and organizational measures that are appropriate in terms of the existing risk, possible consequences to the persons concerned, sensitivity of the data, context in which it is being processed and obligations under applicable national legislation. If an appropriate level of confidentiality and security for personal data or sensitive protection information cannot be guaranteed, the protection actor should refrain from collecting the data, or from transferring them. If security challenges develop, owing to a change in the environment since the data collection, the protection actor should destroy the data if the data-security risks cannot be mitigated.

Data security measures should be routinely reviewed and upgraded to ensure a level of data protection that is appropriate to the sensitivity of the personal data. Monitoring mechanisms and corrective measures should be put in place to deal with and mitigate the impact of any data security breaches. Such breaches should also be reported, particularly if they put the persons concerned at risk.

🔒Ⓢ

6.15 The confidentiality of personal data and sensitive information must be maintained at all times.

The confidentiality of personal data and sensitive information must be respected for as long as data are retained or as long as the disclosure of the data may place the person or another individual or a community at risk.

Sharing, transferring and publishing

In protection activities, the sharing and transfer of personal data and sensitive information among protection actors and with third parties is a routine operational requirement. Nevertheless, it should only occur if it serves a protection purpose and there is a legitimate basis for it. Protection actors must also be aware of and comply with national data protection laws in this regard.

🔒Ⓢ

6.16. Data must be transferred to or shared with only those recipients who offer the required level of data security and protection.

This is because of the very high risk of causing harm if personal data or sensitive protection data and information are mismanaged. Protection actors must also take measures to ensure that the sharing of such data and information does not compromise the identity or character – humanitarian or human rights, non-political – of these actors, jeopardize human rights, or undermine the climate of trust and confidence that has to exist between humanitarian and human rights actors and the persons approaching them for protection and/or assistance.

Accountability

🔒Ⓢ

6.17. Protection actors must ensure accountability for the processing of personal data and sensitive information. They must establish formal procedures for the data and information management process, from collection to exchange and archiving or destruction, including coaching of staff and volunteers and monitoring of quality and supervisory mechanisms.

Protection actors must be in a position to demonstrate that adequate and proportionate measures have been undertaken within their respective organizations to ensure compliance with the standards set out here, and to prevent the harm that may result from unauthorized access. Moreover, they are responsible for ensuring that any parties to whom they may subcontract information collection or processing also apply the required standards at every stage.

SECTION 3 – ASSESSING THE RISKS

At every stage of data processing – from collection to use, sharing and archiving or destruction – risks must be identified and mitigated to the extent possible. In addition, preserving the safety and dignity of the persons and the population involved (witnesses, families, communities, etc.) must be a priority, in line with the principle of 'do no harm'.

🔒Ⓢ

6.18. Protection actors must assess the risks at each step of collecting and processing data and information, and must mitigate any potential adverse consequences for those providing it, and for their families and communities.

Protection actors who collect personal data or sensitive protection data and information are responsible for assessing and mitigating, to the extent possible, all of the associated risks, and regularly reviewing them. This also applies in the case of using or replicating data or information that has been made public by other entities or individuals, including online.

Assessing the risks should involve a preliminary analysis, followed by a data protection impact assessment (DPIA), which is particularly useful if collecting information from the internet. It also requires dialogue with the persons concerned, and raising awareness among them, about perceptions of risk. Measures to mitigate risks may include technical solutions, operational and/or organizational controls, and/or communication strategies.

If it is assessed that the processing of the information will jeopardize the safety of the persons concerned, and if the protection actor is unable to mitigate the risks to an acceptable level, they must refrain from directly collecting information and should direct victims and witnesses to other protection actors that are better equipped to handle the information.

ENSURING PROFESSIONAL CAPACITIES

This chapter deals with the internal processes, competencies and capacities necessary for humanitarian and human rights actors engaged in protection work in armed conflict and other situations of violence. It underscores the importance of ensuring congruence between the stated intentions of a protection actor and its capacity to deliver, and looks at the possible implications for staff management when engaging in protection work.

ENSURING RELEVANT CAPACITIES AND COMPETENCIES

Ⓢ

7.1. Protection actors must identify and address gaps in their professional capacity to carry out protection activities.

Protection work is staff-intensive and demands a range of technical competencies, including persuasion and negotiation skills, ability to analyse contexts and problems, knowledge of applicable legal frameworks and capacity to work under various operational and security constraints. To be able to identify and fill gaps and skills in knowledge as required, protection actors must undertake regular and systematic assessments of their professional competencies and those of their teams.

Ⓖ

7.2. Protection actors should make every effort to secure sufficient resources to support their protection activities at the level and for the duration of their commitment.

Before undertaking a response, protection actors should endeavour to secure the resources they require for an adequate period of time. In addition, they should work with donors to ensure their funding is flexible enough to avoid having to curtail programmes or projects while there are ongoing protection needs. The possibility of this happening should be planned for and the likely impact on the population in question analysed.

STAFF TRAINING

Ⓢ

7.3. Protection actors must ensure that their staff are adequately trained and have the requisite expertise and capacities.

Protection work can be sensitive and often takes place in complex and dynamic circumstances. Protection actors have a duty to ensure that their staff have the knowledge, skills and attitudes required to perform satisfactorily in such environments. Those actors who do not have the means or desire to develop their own comprehensive training programmes should facilitate access for their staff to other available opportunities.

(S)

7.4. Protection actors must keep themselves informed of and adopt, as appropriate, current practices and guidelines of relevance to their protection activities.

A wide range of standards and guidelines are now available on specific protection issues, and their number is expected to grow. Protection actors must seek to draw from collective experience and keep up to date on the evolution of protection work. By documenting their own activities, lessons learnt and good practices, they can also actively contribute to that evolution and thus to the development of their sector.

MANAGING STAFF SAFETY

(S)

7.5. Protection actors must take measures to minimize the risks to which their staff (including volunteers) are exposed.

Protection work is inherently dangerous and stressful. Within the framework of their duty of care, protection actors must put adequate measures in place to help minimize the risk to staff members' health and mitigate the physical and mental consequences of their work. Such measures can be established based on an analysis of the threats their activities might generate and the subsequent risks they may face. It is important to bear in mind that national staff can face different – and often greater – risks.

In all circumstances, staff must be informed of the risks they may face and their options in that regard. It is essential that the organizational culture encourages staff to report any distress and seek assistance, when necessary. All protection actors should develop clear policies and guidelines to help management/senior staff mitigate and respond to risks – including consequences of accumulated stress and vicarious trauma – faced by protection staff. Adequate training in security management should also be provided.

ENSURING PROFESSIONAL AND ETHICAL CONDUCT BY STAFF

(S)

7.6. Protection actors must adopt an institutional code of conduct and ensure compliance.

Protection actors must ensure that all their staff conduct themselves according to established professional and ethical standards, respect applicable legal frameworks, including those that pertain to human rights, and demonstrate the highest standards of integrity. Protection actors must have in place a code of personal conduct, as well as concrete measures to ensure it is complied with. Such a code should also feature in the terms of reference of positions, unit/work plans and in performance appraisals.

ANNEXES

REFERENCE MATERIAL FOR CHAPTER 1

Charter on Inclusion of Persons with Disabilities in Humanitarian Action.

Core Humanitarian Standard.

DFID, *Guide to Disaggregating Programme Data by Disability*, DFID, 2015.

ICRC, *Enhancing Protection for Civilians in Armed Conflict and Other Situations of Violence*, ICRC, Geneva, 2013.

The Sphere Project, *Humanitarian Charter and Minimum Standards in Disaster Response*, The Sphere Project, Geneva, 2011.

Washington Group on Disability Statistics.

World Vision UK, *Minimum Standards for Protection Mainstreaming*, World Vision UK, 2012.

Anderson, Mary B., *Do No Harm: How Aid Can Support Peace or War*, Lynne Rienner, Boulder, 1999.

Giossi Caverzasio, Silvie (ed.), *Strengthening Protection in War: A Search for Professional Standards: Summary of discussions among human rights and humanitarian organizations*, Workshops at the ICRC, 1996–2000, ICRC, Geneva, 2001.

Mahony, Liam, *Proactive Presence: Field Strategies for Civilian Protection*, Centre for Humanitarian Dialogue, Geneva, 2006.

Slim, Hugo, "Why Protect Civilians? Innocence, Immunity and Enmity in War", *International Affairs*, Vol. 79, No. 3, May 2003, pp. 481–501.

REFERENCE MATERIAL FOR CHAPTER 2

ALNAP, *Evaluating Humanitarian Action using the OECD–DAC criteria*: *An ALNAP guide for humanitarian agencies*, Annex 1 Joint Committee on Standards for Educational Evaluation, London, 2006, pp. 71–76.

ALNAP, *Evaluating Protection in Humanitarian Action*, 2014.

Results-Based Protection (InterAction): A problem-solving approach to enhance protection and reduce the risk people experience in complex humanitarian crises.

IASC, *Policy on Protection in Humanitarian Action*, IASC, 14 October 2016.

IASC, *Provisional guidance on the development of Humanitarian Country Team Protection Strategy – Provisional Guidance Note*, September 2016.

OECD, *Glossary of Key Terms in Evaluation and Results Based Management*, Paris, 2002, pp. 21–22.

United Nations Secretary-General's *Human Rights Up Front Initiative*.

REFERENCE MATERIAL FOR CHAPTER 3

GPC, *Diagnostic Tool and Guidance on the Interaction between Field Protection Clusters and UN Missions,* GPC, 2013.

InterAction Protection Working Group, *Protection in Practice: A Guidebook for Incorporating Protection into Humanitarian Operations,* InterAction, Washington, 2005.

IASC, *Growing the Sheltering Tree: Protecting Rights through Humanitarian Action – Programmes and Practices Gathered from the Field,* IASC, Geneva, 2002.

IASC, *Civil-Military Guidelines and Reference for Complex Emergencies,* IASC, Geneva, March 2008.

IASC, *Policy on Protection in Humanitarian Action*, IASC, 14 October 2016.

Overseas Development Institute, *Humanitarian Response,* HPG Policy Brief 29, ODI, London, 2007.

UN, *Report of the Panel on United Nations Peace Operations* (the Brahimi Report), [A/55/305], 21 August 2000.

UN, *Special Measures for Protection from Sexual Exploitation and Sexual Abuse*, Secretary-General's Bulletin, [ST/SGB/2003/13], UNSG, 9 October 2003.

UN, *United Nations Peacekeeping Operations, Principles and Guidelines*, UNDPKO/DFS, New York, 2008.

UN, *Operational Concept on the Protection of Civilians in United Nations Peacekeeping Operations,* UN DPKO/DFS, New York, 2010.

UN, *Human Rights Due Diligence Policy on UN Support to non-UN Security Forces*, [A/67/775], 5 March 2013.

UN, *United Nations Policy on Integrated Assessment and Planning*, United Nations Development Group, 2013.

UN, *Aide-Memoire for the Consideration of Issues Pertaining to the Protection of Civilians in Armed Conflict*, OCHA, 2014.

UN, *Security Council Norms and Practice on the Protection of Civilians in Armed Conflict*, OCHA, 2014.

UN Security Council Resolution 2210, 16 March 2015.

UN, *Uniting our Strengths for Peace – Politics, Partnership and People*, Report of the High-Level Independent Panel on Peace Operations, June 2015.

UN, *The Future of United Nations Peace Operations: Implementation of the Recommendations of the High-level Independent Panel on Peace Operations*, [A/70/357-S/2015/682], UNSG, 2 September 2015.

REFERENCE MATERIAL FOR CHAPTER 4

Geneva Call, online *Directory of Armed Non-State Actor Humanitarian Commitments*.

GPC, *Minimum Standards for Child Protection in Humanitarian Action*, GPC, Geneva, 2012.

IASC, *Policy on Protection in Humanitarian Action*, IASC, 14 October 2016.

ICRC, International Rescue Committee, Save the Children, UNICEF, UNHCR and World Vision, *Interagency Guiding Principles on Unaccompanied and Separated Children*, ICRC, Geneva, 2004.

ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, Geneva, October 2015.

Norwegian Refugee Council, *Risk management toolkit in relation to counterterrorism measures*, Geneva, 2015.

UN, *Standard Minimum Rules for the Treatment of Prisoners*, UN ECOSOC, Resolution 663 C (XXIV) of 31 July 1957 and 2076 (LXII) of 13 May 1977.

UN, *Madrid International Plan of Action on Ageing*, Report of the Second World Assembly on Ageing, New York, 8–12 April 2002.

UN, *Guiding Principles on Internal Displacement*, OCHA, New York, 2004.

UNICEF, *The Paris Principles and Guidelines on Children Associated with Armed Forces or Armed Groups*, Paris, 2007.

De Schutter, Olivier, *International Human Rights Law: Cases, Materials, Commentary*, Cambridge University Press, 2010, p. 5.

REFERENCE MATERIAL FOR CHAPTER 5

IASC, *Civil-Military Relationship in Complex Emergencies*, IASC, Geneva, 2004.

IASC, *Civil-Military Guidelines and Reference for Complex Emergencies*, IASC, New York, 2008.

IASC, *Terms of Reference for the Humanitarian Coordinator*, IASC, 2009.

Overseas Development Institute, *Leadership Reform in the Humanitarian System*, HPG Policy Brief 27, ODI, London, 2007.

de Maio, Jacques (ed.), *The Challenges of Complementarity: Report on the Fourth Workshop on Protection for Human Rights and Humanitarian Organizations*, ICRC, Geneva, 2000.

Giossi Caverzasio, Silvie (ed.), *Strengthening Protection in War: A Search for Professional Standards: Summary of discussions among human rights and humanitarian organizations,* Workshops at the ICRC, 1996–2000, ICRC, Geneva, 2001.

Graves, Sue, Wheeler, Victoria and Martin, Ellen, *Lost in Translation: Managing Coordination and Leadership Reform in the Humanitarian System,* HPG Policy Brief 27, ODI, London, 2007.

REFERENCE MATERIAL FOR CHAPTER 6

Brussels Privacy Hub/ICRC, *Handbook on Data Protection in Humanitarian Action*, BPH/ICRC, 2017.

Harvard Humanitarian Initiative, *The Signal Code: A Human Rights Approach to Information during Crisis*, January 2017.

ICRC/Engine Room/Block Party, *Humanitarian Futures for Messaging Apps: Understanding the Opportunities and Risks for Humanitarian Action*, ICRC, March 2017.

ICRC, *The ICRC and Data Protection*, August 2017.

International Organization for Migration, *Data Protection Manual*, IOM, 2010.

National Information Standards Organization, *Understanding Metadata*, NISO Press, 2004.

OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2013.

Oxfam, *Responsible Program Data Policy*, Oxfam International, August 2015.

Oxfam, *Responsible Data Management Training Pack*, March 2017.

PIM, *Second Protection Information Management Working Meeting Outcome Document*, Geneva, December 2015.

PIM, *Protection Information Management Common Terminology*, June 2016.

PIM, *Principles, Matrix and Process – Quick Reference Flyer*, March 2017.

UN, *Guidelines for the Regulation of Computerized Personal Data Files* [A/RES/45/95], 14 December 1990

UN, *The right to privacy in the digital age* [A/HRC/27/37], Report of the UN High Commissioner for Human Rights, OHCHR, June 2014.

UN, *Summary of the Human Rights Council panel discussion on the right to privacy in the digital age* [A/HRC/28/39], Human Rights Council, December 2014.

UN, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*, UNHCR, May 2015.

World Food Programme, *WFP Guide to Personal Data Protection and Privacy*, 2016.

Silverman, Craig (ed.), The Verification Handbook, European Journalism Centre, 2014.

Dette, Rahel, *Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts*, Global Public Policy Institute, Berlin.

African Union Convention on Cyber Security and Personal Data Protection (2014).

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

European Union General Data Protection Regulation (GDPR, 2016).

International Covenant on Civil and Political Rights.

International Standards on the Protection of Data and Privacy (the "Madrid Resolution"), 2009.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (EU General Data Protection Regulation), [2016] OJ L119/1.

UN Universal Declaration of Human Rights (1948).

REFERENCE MATERIAL FOR CHAPTER 7

Global Cluster Coordinator Group, *Cluster Coordination Performance Monitoring – Guidance Note*, January 2014.

Human Rights Law Centre, *Guiding Principles for Human Rights Field Officers*, University of Nottingham, 2008.

Human Rights Law Centre, *Working in Conflict and Post-Conflict Environments – Consolidating the Profession: The Human Rights Field Officer* (project), School of Law, University of Nottingham, 2008.

IASC, *Plan of Action and Core Principles of Codes of Conduct on Protection from Sexual Abuse and Exploitation in Humanitarian Crisis*, IASC, Geneva, 2002.

ICRC/International Federation of Red Cross and Red Crescent Societies, *Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief*, ICRC, Geneva, 1994.

Oxfam, *Improving the Safety of Civilians: A Humanitarian Protection Training Pack*, Oxfam GB, Oxford, 2009.

The Keeping Children Safe Coalition, *Keeping Children Safe: A Toolkit for Child Protection*, The Keeping Children Safe Coalition, London, 2011.

UN, *Protecting Refugees: A Field Guide for NGOs*, UNHCR, Geneva, 1999.

Bugnion, Christian, *Analysis of the "Quality Management" Tools in the Humanitarian Sector and Their Application by the NGOs*, ECHO, Brussels, 2002.

The ICRC helps people around the world affected by armed conflict and other violence, doing everything it can to protect their dignity and relieve their suffering, often with its Red Cross and Red Crescent partners. The organization also seeks to prevent hardship by promoting and strengthening humanitarian law and championing universal humanitarian principles. As the authority on international humanitarian law, it helps develop this body of law and works for its implementation.

People know they can rely on the ICRC to carry out a range of life-saving activities in conflict zones, including: supplying food, safe drinking water, sanitation and shelter; providing health care; and helping to reduce the danger of landmines and unexploded ordnance. It also reunites family members separated by conflict, and visits people who are detained to ensure they are treated properly. The organization works closely with communities to understand and meet their needs, using its experience and expertise to respond quickly, effectively and without taking sides.