



PROFESSIONAL STANDARDS FOR PROTECTION WORK

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

THIRD EDITION, 2018



A GLOBAL NGO NETWORK FOR PRINCIPLED AND EFFECTIVE HUMANITARIAN ACTION



PARTNERS:



PROFESSIONAL STANDARDS FOR PROTECTION WORK

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

THIRD EDITION, 2018

ACKNOWLEDGEMENTS

The advisory group extends its appreciation to all those who took part in this revision. A product of an interactive process, the revision faithfully reflects contemporary concerns and is of direct relevance to most actors involved in protection work.

The ICRC would like to sincerely thank all the members of the advisory group. They were requested to serve in a personal capacity, based on the depth and diversity of their protection experience and expertise within their agencies and organizations. The advisory group consisted of the following:

Amnesty International: Caroline Ford (2008–2009), Michael Bochenek (2011–2013), Anne Fitzgerald, Joanne Mariner, Tirana Hassan (2015–2017)

Danish Refugee Council (DRC): Kathrine Starup (2011–2017)

Department for International Development (DFID): Patrick Saez (2008–2009)

Global Protection Cluster (GPC): Simon Russell, Eva Garcia Bouzas (2015–2017)

Handicap International: Sarah Rizk (2011–2012), Nathalie Herlemont Zoritchak (2011–2017)

Humanitarian Policy Group (HPG): Sorcha O’Callaghan (2008–2009), Victoria Metcalfe (2011–2012), Eva Svoboda (2012–2017)

Human Rights Watch: Michael Bochenek (2015–2017)

International Committee of the Red Cross (ICRC): Alain Aeschlimann (2008), Cathy Huser (2008–2009), Pierre Gentile (Project Manager, 2008–2012), Andreas Wigger (2008–2013), Nicolas Farcy (2011–2012), Guilhem Ravier (Project Manager, 2012–2017), Romain Bircher (2011–2013), Pilar Gimeno Sarciada (Project Manager, 2018 onwards)

International Council of Voluntary Agencies (ICVA): Ed Schenkenberg van Mierop (2008–2012), Nan Buzard (2012–2017)

InterAction: Ray Lynch (2008–2009), Jenny McAvoy (2011–2017)

Jesuit Refugee Service (JRS): Michael Gallagher (2008–2017)

Médecins sans Frontières (MSF) – Operational Centre Amsterdam: Kate Mackintosh (2008–2009), Sean Healy (2011–2013), Judith Fisher (2011–2012)

Office for the Coordination of Humanitarian Affairs (OCHA): Simon Bagshaw (2011–2013), Dina Abou Samra (2014–2017)

Oxfam: Rachel Hastie (2011–2017)

Office of the United Nations High Commissioner for Human Rights (OHCHR): Matthias Behnke (2007–2009), Francesca Marotta, Mara Steccazzini (2015–2017)

Office of the United Nations High Commissioner for Refugees (UNHCR):

Atle Solberg (2008–2009), Josep Zapater and Leonard Zulu (2008–2013), Allehone Abebe, Louise Aubin, Elizabeth Eyster, Gregor Schotten (2015–2017)

Thanks are due also to:

- Shantha Rau Barriga and Lea Labaki (Human Rights Watch) for their contribution to Chapter 1
- Jessica Lenz (InterAction) for her contributions to Chapter 2
- Marlies Bull (OCHA) and Ernesto Granillo (ICRC) for their contributions to Chapter 3
- Sophie Clavet, Monique Crettol, Julia Joerin, Massimo Marelli and Yanya Viskovich (ICRC) and Caroline Dulin Brass (UNHCR) for their contributions to Chapter 6.

The ICRC would also like to thank all those others who participated at different stages in the preparation of this 3rd edition (2015 – 2018), including:

- Angharad Laing and Markus Forsberg, International Association of Professionals in Humanitarian Assistance and Protection (PHAP), for organizing a survey and a webinar on the draft revision
- Trevor Keck and Sara Owens (ICRC) for organizing a consultative workshop in Washington DC on Chapter 6
- Neil Dillon and John Mitchel (ALNAP), who organized, jointly with InterAction, a consultation with experts and practitioners, titled “Managing Protection Strategies: Measurability, Adaptability, and Evaluability of Protection”, in London in December 2016
- Margot Champeix, Chiara Capobianco, Marta Ghittoni, Ciara Laverty, Johanna Bohl, Isabell Meenen and Pamela Jiménez Cárdenas (ICRC), who contributed to the revision and supported the work of the advisory group at different stages of the revision
- Emily Richard (ICRC), for her thorough revision of the legal aspects of the text
- Ameline Peterschmitt Nussbaumer and Maryline Signoret (ICRC) for their support in the development of the app and the eLearning tool that accompany this document
- Aninia Nadig and Christine Knudsen (Sphere), for their help in ensuring consistency and cross-referencing between Sphere and the professional standards.

The ICRC would also like to thank the Swiss Federal Department of Foreign Affairs (Human Security Division) for providing financial support for the revision, dissemination and promotion of *Professional Standards*.

TABLE OF CONTENTS

Acknowledgements	2
Acronyms	6
Glossary	7
Introduction	10
Why protection standards are needed and still relevant	10
Background	11
Scope and limitations of the document	12
Using the standards	13
For whom the standards are intended	14
The standards' applicability during disasters	14
Structure of the document	15
What has been updated?	16
Issues covered by the standards	17
Chapter 1: Overarching principles in protection work	21
Respecting the principles of humanity, impartiality and non-discrimination	24
Avoiding harmful effects	27
Putting the populations, communities and individuals affected at the centre of protection activities	28
Annexes to Chapter 1	33
Chapter 2: Managing protection strategies	37
Monitoring	45
Evaluation and learning	48
Annexes to Chapter 2	51
Chapter 3: Outlining the protection architecture	57
Relating to the primary duty bearers	60
Interface with UN peace operations and internationally mandated military forces and police services	65
Engaging UN peace operations and internationally mandated military forces and police services	69
Other actors	72
Annex to Chapter 3	74
Chapter 4: Building on the legal base of protection	77
Knowing the legal framework	79
Referring to the law with consistency and impartiality	82
Maintaining coherence and accuracy	83
Referring to relevant regional and domestic laws and other relevant standards	84
Upholding existing legal standards	86
Annex to Chapter 4	89

Chapter 5: Promoting complementarity.....	91
Complementarity of action among protection actors.....	95
Complementarity of principles among protection actors	96
Complementarity of analyses.....	97
Mobilizing other protection actors	98
Providing information on protection services and facilitating referral to relevant services	98
Responding to harm and violations.....	100
Annex to Chapter 5	101
Chapter 6: Managing data and information for protection outcomes	103
Introduction.....	106
<i>What is protection data and information management and why is it important?</i>	<i>106</i>
<i>Structure of the chapter</i>	<i>110</i>
<i>Protection data and information – types of data, sensitivity and legal requirements</i>	<i>111</i>
<i>The use of ICT and other technologies.....</i>	<i>115</i>
Section 1 – General standards for the management of data and information	117
<i>Competencies and capacities</i>	<i>117</i>
<i>Inclusive people-centred approach.....</i>	<i>117</i>
<i>Clearly defined, specific purpose</i>	<i>118</i>
<i>Cooperation and exchange.....</i>	<i>119</i>
<i>Avoiding bias and discrimination</i>	<i>120</i>
Section 2 – Specific standards for the management of personal data and sensitive protection data and information	123
<i>Compliance with relevant legal frameworks</i>	<i>124</i>
<i>Legitimate and fair processing</i>	<i>125</i>
<i>Data minimization</i>	<i>129</i>
<i>Data quality</i>	<i>129</i>
<i>Data retention</i>	<i>129</i>
<i>Data security</i>	<i>130</i>
<i>Confidentiality</i>	<i>132</i>
<i>Sharing, transferring and publishing</i>	<i>133</i>
<i>Accountability.....</i>	<i>135</i>
Section 3 – Assessing the risks	136
Annexes to Chapter 6	140
Chapter 7: Ensuring professional capacities	151
Ensuring relevant capacities and competencies	153
Staff training	154
Managing staff safety	155
Ensuring professional and ethical conduct by staff	156
Annex to Chapter 7.....	158

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 of 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

The protection of people caught up in armed conflict and other situations of violence is a critical challenge. In many armed conflicts, the distinction between civilians and combatants is deliberately blurred. All too often, civilians are exposed to reckless conduct by parties to conflict; they are subjected to attacks, to systematic violations of their rights and to other abuses as well. States and other relevant duty bearers frequently lack the capacity – or the will – to ensure effective protection for people at risk. Worse still, they may themselves perpetrate violence or other abuse against certain segments of the population.

Governments, international organizations and non-governmental organizations (NGOs) have not been indifferent to this challenge. The protection response to crises has improved significantly in recent years. A key factor has been the marked increase in the number and diversity of humanitarian and human rights actors involved in promoting the protection of those at risk of violations or other abuses in armed conflict and other situations of violence. Today, a broad range of humanitarian and human rights actors can be found at work in virtually every hot spot in the world, as well as in other critical situations not covered by the global media.

As a result, protection work has become more diversified and sophisticated, a positive and welcome development. However, the increased numbers and diversity of actors have also complicated matters. A strengthened operational presence has meant greater proximity between humanitarian and human rights actors engaged in protection work, who have now developed complementarities in extremely complex operating environments. The broad gap that previously separated humanitarian and human rights workers has narrowed, and greater coherence has been established. But differences in approaches and aspirations still exist. While the presence in one place of many different actors can produce positive synergies, it can also cause confusion occasionally. This document recognizes distinctions between the two sets of actors, but is founded on the conviction that there is enough common ground between them for establishing a firm, shared basis for their protection work in armed conflict and other situations of violence, as well as possibilities for maximizing complementarity to provide more effective protection for those who need it.

WHY PROTECTION STANDARDS ARE NEEDED AND STILL RELEVANT

These new possibilities for a stronger or expanded response offer greater breadth and depth of specificity and increased complementarity, but they also inevitably cause unevenness in the quality of the protection work being done. The absence of common professional standards can, in fact, lead to situations in which protection work could actually harm the very people and communities it seeks to protect.

It is now agreed that a protection response cannot be effective without the necessary professional competence. A concerted effort is therefore required to ensure that protection work by humanitarian and human rights actors meets commonly agreed minimum professional standards. These establish a baseline to be respected by all, while respecting the diversity of actors and approaches involved. However, defining what that means, to the satisfaction of everyone concerned, has been a major challenge.

Workshops led by the International Committee of the Red Cross (ICRC), between 1996 and 2000, initiated a collaborative project to determine professional standards for strengthening protection in armed conflict and other situations of violence. Besides agreement on a common understanding from which to create shared minimum standards, the project also resulted in the formulation of a generally accepted definition of protection – quoted below – that remains in effect.

DEFINITION OF PROTECTION

“The concept of protection encompasses:

‘... 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)’.”⁴

This definition has helped establish greater understanding between humanitarian and human rights actors, and has led the former increasingly to adopt a rights-based approach.

Several initiatives have contributed, since then, to the quest to define professional standards in protection work, including the Sphere Project,⁵ and various United Nations (UN) and NGO initiatives.⁶ However, all these efforts tended to be based on a specific approach to protection or a given operational context. Overarching principles and fundamental elements, on which a foundation for safe and effective protection work could be based, were yet to be articulated. The focus of this project has therefore been to develop such a set of commonly agreed standards applicable to all humanitarian and human rights actors doing protection work in conflict and other situations of violence.

BACKGROUND

The first edition of *Professional Standards for Protection Work*, published in 2009, reflected the broad consensus that emerged from a two-year consultative process involving numerous humanitarian and human rights organizations.

From the outset, publication of *Professional Standards* was thought to be an evolutionary process. It was therefore foreseen that revisions would take place regularly. A second edition was published in 2013. In October 2015, the ICRC, together with an advisory group composed of experienced practitioners and researchers, agreed to undertake a second revision of *Professional Standards*. This enabled us to take stock of some important developments in the area of protection, and of our views and evolving practice with regard to major issues and challenges.

⁴ S. Giossi Caverzasio (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.

⁵ See: The Sphere Project, *Humanitarian Charter and Minimum Standards in Disaster Response*, 2011.

⁶ See, for example: World Vision UK, *Minimum Inter-Agency Standards for Protection Mainstreaming*, 2012.

On the basis of these discussions members of the advisory group began to work on draft proposals. These were discussed throughout 2016, and then shared with the wider community of practitioners.

The broader consultative process, which began in the autumn of 2016, sought to ensure that the standards took into account the challenges faced by various actors in the field, and that they reflected the consensus of the protection community as a whole. This process entailed a series of face-to-face meetings, specific events and thematic workshops, mobilization of various networks of organizations, and a webinar with accompanying online survey that canvassed opinion on the proposed changes. All this resulted in considerable rewriting of parts of the initial standards and the inclusion of significant new issues and content. On the whole, the consultations confirmed the value and relevance of the standards. They also drew attention to the need to improve the dissemination of the standards and to ensure more effective capacity-building measures or activities for staff. For instance, the standards are widely known, and used to update and develop guidelines and training modules, but spreading knowledge of them, and promoting their use in the drafting of context-specific strategies, remain challenging.

This document takes into account the changes that have occurred in the environment that protection actors work in, and proposes standards and guidelines for addressing the challenges that have arisen. It could not have been prepared without the advisory group's remarks and suggestions or the findings and conclusions drawn from comprehensive consultations with relevant partners and the broader humanitarian and human rights community.

SCOPE AND LIMITATIONS OF THE DOCUMENT

The standards constitute the minimum obligations applicable to any humanitarian or human rights organization engaged in protection work in armed conflict and other situations of violence; organizations that cannot meet them are advised not to implement protection activities. In armed conflict and other situations of violence these standards may be regarded as an umbrella over other existing sets of standards developed by humanitarian and human rights organizations.

They are not intended for use as operational guidance; instead, they offer a broader perspective, expressed as principles and good practices for ensuring that protection work is as safe and effective as possible. They also seek to orient protection actors within the formal global protection architecture, and with regard to one another. Within this broader perspective, a "protection actor" is a humanitarian or human rights organization, as opposed to an individual or some other duty bearer with protection responsibilities (States and non-State actors, peace operations, etc.). A "protection worker" is an individual engaged in protection work.

The scope of this project is fairly broad but it makes no claim to be exhaustive. Moreover, there is nothing in the standards to suggest any attempt at further refining the definition of "protection" (as presented in the box above). In fact, they reflect the view that people at risk must themselves be at the centre of any action taken in their behalf.

The contents of this document are equally applicable to humanitarian and human rights actors. And differences in approach are pointed out. However, no attempt is made to define the extent to which humanitarian and human rights actors should seek overlap, distinction, commonality or complementarity in their protection work.

At the same time, there is no intention to set limits on who can do what in protection. There is also no intention to standardize protection work by encouraging uniformity of approach or to regulate and thus restrict the rich and evolving diversity that is a strength of the sector. Instead, the aim is to encourage diversity of approach and activity at both organizational and collective levels, while providing a baseline to ensure the safest and most effective response to the critical needs of people at risk.

The standards outlined in this document supplement, and are in no way an attempt to replace, other standards used by protection actors: for instance, the *Inter-agency Guiding Principles on Unaccompanied and Separated Children* (2004), the *Field Handbook on Unaccompanied and Separated Children* and the *Toolkit on Unaccompanied and Separated Children* (2017) prepared by the Inter-agency Working Group on Unaccompanied and Separated Children, the *Minimum Standards for Child Protection in Humanitarian Action* (2012), the Inter-Agency Standing Committee's *Policy on Protection in Humanitarian Action* (2016), the ICRC/Brussels Privacy Hub's *Handbook on Data Protection in Humanitarian Action* (2017) and the standards for monitoring, advocacy and protection – in relation to human rights – developed by the Office of the UN High Commissioner for Human Rights (OHCHR).

Finally, the *Sphere Handbook* has a chapter on “protection principles”; the principles it sets out in the 2018 edition are of fundamental importance for everyone involved in humanitarian response, even those who don't regard themselves as protection actors. It is worth noting that these efforts in standard-setting in the field of protection are complementary, rather than duplicative or contradictory.

USING THE STANDARDS

The professional standards presented in this document provide a reliable source of reference for reviewing or developing internal policies, guidelines and training materials. That applies to organizations engaged in protection work, but the standards can also help practitioners in the field design and implement protection strategies.

The standards can also serve as a useful point of reference for other actors with an interest in protection, including those who do not regard themselves as protection actors. In addition, protection actors can use them to explain to various stakeholders, including authorities, the principles on which their work is based.

All protection actors are urged to use this document to devise and implement more effective protection-related activities. They are also encouraged to use the tools that accompany this third edition – the e-learning course, mobile application, online micro-site and summary version – to disseminate the standards and guidelines to their colleagues and partners. Some of these tools – the micro-site, for example – are designed to make the standards more accessible and user-friendly, as well as more flexible, in terms of incorporating reactions from protection workers and updating the document.

FOR WHOM THE STANDARDS ARE INTENDED

These standards are addressed to all humanitarian and human rights actors engaged in protection work to benefit communities and individuals who are at risk of violations and other abuse, or who are subjected to such misconduct, during armed conflict and other situations of violence. Such work can include efforts to persuade duty bearers to assume their obligations more fully; or to strengthen the capacity of those at risk to avoid or reduce their exposure to threats, and to overcome or cope more effectively with the consequences of protection failures that affect them. However, others – such as development or peace-building actors, and those who interact with humanitarian and human rights organizations in these situations – may also find the standards useful.

Not all humanitarian actors carry out protection activities *per se*, but all of them have to incorporate basic safety considerations and concerns in their practice. Such concerns are already present in concepts such as “doing no harm”, “mainstreaming protection”, and “good-quality programming”. Clearly, every humanitarian actor must ensure that its activities (whether for relief or development, or for other goals) do not contribute to creating risks for the communities and individuals for whose benefit they work, or to exacerbating the risks they are already facing. In fact, ensuring their safety must be regarded as a basic element of any effort to help them. For instance, water and sanitation programmes must ensure that latrines or other facilities are as safely situated as possible. Actors occupied mainly with incorporating protection concerns in their daily activities can certainly gain inspiration from these standards but are likely to find more practical guidance in the latest version of the Sphere standards and in *Minimum Standards for Protection Mainstreaming*.

The protection actors specifically targeted by this document are those humanitarian and human rights actors that engage directly in protection work during armed conflict and other situations of violence, i.e. those for whom the issue of protection is at the centre of their efforts. In the example above, of the safe location of facilities, the actor concerned might also decide to take direct action to persuade the authorities to make the area safer. It might document incidents, and later make use of them to urge the police or military to act immediately to improve security in the area of concern.

THE STANDARDS' APPLICABILITY DURING DISASTERS

These standards have been drafted with a focus on armed conflict and other situations of violence, but many of them are equally applicable in human rights and humanitarian work undertaken during disasters. Certain standards or guidelines may not apply, or might do so only in a less stringent way, during disasters, as their pertinence is limited to situations where the conduct of armed actors is the main threat.

Natural phenomena – earthquakes, typhoons and other meteorological or geological events – do not inevitably result in “natural disasters”. That requires a human presence;

and even then, the determining factor will be the degree to which the people in question are exposed and vulnerable to the threat of natural disasters, and their resilience. All this can be addressed by human (including State) action. When governments and others fail to reduce people's exposure and vulnerability, or strengthen their resilience, or take effective mitigatory measures, their failure is a human rights issue.⁷

Human rights principles must be at the centre of all pertinent efforts – risk reduction, prevention, preparedness, response, recovery and reconstruction – undertaken during disaster response; this must be the case in every phase of a response. International human rights norms should inform all activities – carried out immediately after a disaster – to ensure that survivors are safe and treated for their injuries, and that they are clothed, fed and sheltered. Full respect for human rights is essential at all stages of the crisis; it should not be regarded as an indulgence that can wait until order has been restored. The Sphere standards provide invaluable guidance for disaster preparedness and response. Their approach, based on the rights and the dignity of the people affected, is wholly compatible with that of the professional standards for protection work.

People affected by disasters – including those who have been displaced – remain entitled to the protection of human rights law. Displacement or any other consequence of the disaster does not deprive them of any of the rights granted to the population in general. At the same time, people who are at risk and those who have been affected by a disaster have particular needs and vulnerabilities that demand specific protection and assistance measures in addition to and taking precedence over those required for the general population. Human rights concerns become more urgent, and violations often increase, during and immediately after a disaster. These concerns include such matters as discrimination in aid distribution, exploitation, physical and other forms of violence (including gender-based violence), issues related to land, housing and property rights and loss of official documents.

In all responses to natural disasters, humanitarian or human rights actors engaged in protection work must pay close attention to the following: the principles of humanity (Standard 1.1), non-discrimination and impartiality (Standards 1.2, 1.3), human dignity (Standard 1.6), the duty to do no harm (Standards 1.4, 1.5), and the need to ensure the active participation of people at risk (Standard 1.7). As they should do during armed conflict and other situations of violence, protection actors responding to disasters must analyse protection needs in their area of competence (Standard 2.1) and must monitor and evaluate protection outcomes and impact (Standards 2.3, 2.4).

STRUCTURE OF THE DOCUMENT

Standards, guidelines and explanatory notes

The document presents a series of standards and guidelines, each accompanied by explanatory notes.

The standards constitute the minimum obligations that all humanitarian and human rights actors doing protection work must fulfil. It is likely that, in specific areas, some actors will be able to establish internal standards that are more demanding than those to be found here, owing to the expertise and capacities they possess and their approach to protection work. Clearly, the higher standard (as set by a given organization) should take precedence.

⁷ United Nations Human Rights Council, *Promotion and protection of the rights of indigenous peoples in disaster risk reduction, prevention and preparedness initiatives – Study by the Expert Mechanism on the Rights of Indigenous Peoples [A/HRC/27/66]*, United Nations, 2014.

The guidelines, on the other hand, are intended as useful and, in some cases, essential reference criteria. However, their application is likely to require more flexibility than that of standards, as they cannot be applied at all times by all actors. Certain guidelines could even be adopted as standards by some organizations; but other organizations – depending on the nature of their work, the approaches they adopt and the activities they undertake – might find the same guidelines to be unrealistic, impracticable or irrelevant.

The explanatory notes aim to delineate the main elements that sustain and justify each standard or guideline. They describe the main challenges the standards and guidelines are designed to tackle, the limitations and constraints of the standards and guidelines, as well as the dilemmas they might pose to protection actors. They also cover certain practical considerations in connection with their application. The explanatory notes are the result of an extensive consultative process. Even so, they are not exhaustive; their aim is illustrative. The notes must not be treated as an operational manual on the application of the standards and guidelines, or on conducting protection activities. It is the responsibility of each protection actor to determine how to incorporate these standards and guidelines in its own practices.

Throughout the text, the standards are flagged by the symbol **S** and the guidelines by the symbol **G**.

WHAT HAS BEEN UPDATED?

The following are the main areas that have been developed and updated for the current edition. However, what follows is not an exhaustive list, as many other, smaller updates have been made in all chapters.

1. Applicability for humanitarian and human rights actors (throughout)

Special attention was given to ensuring that the standards and guidelines are equally relevant to human rights and humanitarian actors. Whenever pertinent, the document now reflects the distinctive characteristics of human rights and humanitarian actors engaged in protection work.

2. Managing data and information for protection outcomes (Chapter 6)

Given the rapid proliferation of initiatives to use information and communication technology in new ways for protection purposes, and the growing body of law on data protection, the advisory group agreed to review the scope and language of the standards on managing data and information. Comprehensive guidelines for protection information management (PIM) have been incorporated in Chapter 6, which has been significantly updated and now also describes the full cycle of information management as it relates to protection. The revised standards reflect the experiences and good practices of humanitarian and human rights organizations, as well as those of actors in the area of information and communication technology; they also reflect data protection law more clearly.

3. Managing protection strategies (Chapter 2)

The need to adopt a strategy based on sound analysis of the situation, and for regular monitoring and evaluation of its implementation, had already been recognized in the 2009 and 2013 editions. Drawing on the discussions still in progress among protection practitioners about the challenges of measuring protection outcomes, the revised

version places a stronger emphasis on protection as an outcome (success being measured by the extent to which pertinent risks have been reduced). The revised standards also include an elaboration on the importance of establishing the causal logic of action to achieve a protection outcome, and underline the importance of monitoring and evaluation.

4. Interaction and dialogue between protection actors and UN peacekeeping missions and other internationally mandated military and police forces (Chapter 3)

The UN Security Council has expressly mandated a number of UN peace operations to “protect civilians”. Implementing such mandates can entail the use of force to protect civilians and a range of other activities that are complementary to those carried out by humanitarian and human rights actors. The advisory group recognized that dialogue and interaction between humanitarian and human rights actors and UN peacekeeping operations and other internationally-mandated military and police forces are necessary, in order to secure positive protection outcomes while upholding a principled approach to protection work. This edition of *Professional Standards* provides more detailed guidelines for interacting with UN peace operations and other multinational forces.

5. The impact of counter-terrorism legislation on principled protection work

Recent national, regional and international efforts to tackle “violent extremism” may raise protection concerns, as they are often followed by new legislation and action plans related to counter-terrorism. These new laws and plans of action might threaten the fundamental rights and freedoms of those affected by them, both in detention facilities and in the communities concerned. This edition of *Professional Standards* seeks to clarify how counter-terrorism legislation may affect the activities of protection actors.

ISSUES COVERED BY THE STANDARDS

The standards and guidelines are numbered sequentially, and the order is followed from one chapter to the next. They are organized into seven chapters, divided into two categories, as shown below:

Overarching principles and operational framework

1. Overarching principles in protection work

This first chapter describes the main principles that are central to protection work undertaken by humanitarian and human rights actors, and that are common to all protection activities and strategies.

2. Managing protection strategies

This chapter defines the main stages of the project management cycle. Attention is drawn to certain elements, particular to protection work, that should be taken into account while analysing protection needs, setting out priorities and monitoring and evaluating the results of protection work.

3. Outlining the protection architecture

This chapter describes the components of the existing formal/legal protection architecture, and how humanitarian and human rights actors doing protection work should relate to this architecture as well as to each other.

Technical issues**4. Building on the legal base of protection**

This chapter emphasizes the necessity for humanitarian and human rights actors involved in the field of protection of understanding and referring to applicable law.

5. Promoting complementarity

This chapter is concerned with managing the interaction between the wide range of humanitarian and human rights actors doing protection work. It recognizes that their approaches may differ, and defines the minimum measures required to ensure that their activities complement those of others.

6. Managing data and information for protection outcomes

This chapter deals with the management of data and information (personal data, information on specific instances of violation and abuse, and so on). While not, *per se*, a protection activity, data management is an integral aspect of all protection activities. The necessity of having sound PIM processes that comply with international data-protection laws has become more important, owing to the growing number of initiatives to create a strong evidence base for protection. This chapter therefore goes into considerable detail, describing the PIM process and emphasizing the need for due care throughout.

7. Ensuring professional capacities

This chapter is concerned with the attention that all protection actors must give, internally, to ensuring that their stated intentions correspond to their ability to deliver. It emphasizes that a protection actor must be able to define its objectives, specify how it plans to achieve them, ensure that it has the necessary capacities and realize its stated intentions in a reliable and predictable manner.



CHAPTER 1

OVERARCHING PRINCIPLES IN PROTECTION WORK

Respecting the principles of humanity, impartiality and non-discrimination

- S** 1.1. Protection actors must ensure that the principle of humanity is at the core of their work.
- S** 1.2. Non-discrimination and impartiality must guide protection work.
- S** 1.3. Protection actors must ensure that their activities do not have a discriminatory effect.

Avoiding harmful effects

- S** 1.4. Protection actors must avoid harmful effects that could arise from their work.
- S** 1.5. Protection actors must contribute to the capacity of other actors to ensure that no harmful effects derive from their actions.

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.
- S** 1.7. Protection actors must seek to engage in dialogue with persons at risk and ensure their participation in activities directly affecting them.
- G** 1.8. Protection actors should consider building on the capacities of individuals and communities to strengthen their resilience.
- 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.
- 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.

This chapter describes the main principles that are central to protection work undertaken by humanitarian⁸ and human rights actors, and that are common to all protection activities and strategies.

The first section emphasizes the importance of the principles of humanity, impartiality and non-discrimination; it also emphasizes that it is concern for individuals at risk that drives protection work. Broadly speaking, these are the principles that underlie international humanitarian law and form an indispensable part of efforts to establish and maintain humanitarian access and address the protection concerns of people at risk.

The principles of neutrality and independence are often crucial for gaining access to and maintaining proximity with all victims in armed conflict and other situations of violence, and for securing credibility and acceptance for organizations and their protection work. However, while these principles are central to some organizations' identities and operational approach (for philosophical as well as practical reasons), they may not be so for all organizations; and the weight an organization places on these principles may vary according to its identity, mandate and operational realities. For this reason, while the principles of humanity, impartiality and non-discrimination are fundamental to the protection work of all humanitarian and human rights actors, and are therefore given particular importance in this document, the principles of neutrality and independence are not. Protection actors should nevertheless aim for transparency and consistency in their approach to these principles, carefully weighing alternative approaches and their implications.

The second section reiterates the fundamental obligation for all actors doing protection work to avoid activities that could aggravate the situation of those they seek to help support. It explains that protection work can be extremely sensitive and can have potentially severe consequences for the population. Responsibility for managing and mitigating these risks lies with those actors doing the work.

The last section underlines that communities and individuals at risk – to whom protection workers should be answerable – are themselves critical actors in the protection process. Protecting and promoting their rights, dignity and bodily integrity is essential for the effectiveness of this work. It entails ensuring that they play a key role, influencing decisions and making practical recommendations based on their intimate understanding of the nature of the threats, violations and abuses to which they are exposed. It is also important to strengthen any effective capacities and coping mechanisms established among communities or individuals affected.

⁸ Both the professional standards and the Sphere Protection Principles build on the principles applicable to all humanitarian actors. These principles are specified in *The Sphere Handbook* and include respect for human dignity, the right to protection, accountability and a people-centred approach.

A PRINCIPLED APPROACH TO PROTECTION WORK

Practitioners will often be confronted with a range of challenges that require taking tough decisions guided by the principles mentioned above and finding and maintaining the necessary balance between them. Problems such as lack of access to people affected, insecurity or logistical constraints often limit protection actors' ability to deliver an impartial and non-discriminatory response. Prioritizing one principle over another may sometimes be necessary, provided this is based on a serious analysis of the challenges, and aimed at achieving effective protection outcomes. The principle of "do no harm" should, however, remain central and must not be compromised.

In addition, these constraints and choices need to be identified, explained and discussed with other relevant actors (other humanitarian and human rights actors, donors, etc.) and the population concerned; this must be done with transparency.

The consequences of the decisions taken should be regularly monitored, with a view to adapting or adjusting the choices made as the situation evolves. For instance, ongoing armed conflict and insecurity may prevent access to certain areas, and make it impossible to establish direct contact with the population and gather information for the purpose of reporting publicly on human rights and humanitarian law violations and abuses. While measures can be taken to compensate for the inaccessibility of some territories – for instance, by gathering information through remote monitoring – such lack of access might make it difficult to report on the conflict as comprehensively as the principle of impartiality requires. Reporting may need to be done in stages, covering more ground as information becomes available. Protection actors must explain these constraints and persevere in their efforts to overcome them.

RESPECTING THE PRINCIPLES OF HUMANITY, IMPARTIALITY AND NON-DISCRIMINATION

S

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.

S

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 affected that are at risk of or subject to violations and abuses. The principle of impartiality also requires holding all duty bearers to similar standards with regard to their obligations and responsibilities, and possible breaches thereof (see Standard 4.2). It thus requires that humanitarian and human rights actors define the protection activities to be undertaken in their area of responsibility, following an assessment of needs using objective criteria.

The application of these principles does not preclude taking account of particular elements (such as gender or age) as factors that may require a targeted response. On the contrary, as indicated in Standard 1.3 below, such factors must be duly considered when assessing needs. Children, for example, tend to be disproportionately affected by conflicts and other situations of violence, and are usually at greater risk owing to their stage of development and dependence on adults, especially when separated from their families or habitual caregivers. Taking such specific vulnerabilities or risk factors into account is essential in order to analyse needs, consult and plan, and to ensure that critical protection needs are prioritized and addressed and that protection responses do not result in or reinforce patterns of marginalization or discrimination.

The challenge of respecting the principles of non-discrimination and impartiality is often compounded by the complex operating environment in which protection work occurs. Protection actors have to make difficult choices when they are unable to address all the urgent needs they confront. The people affected may not understand or may disagree with certain protection-related activities that focus on specific segments of the population, like children associated with armed forces or armed groups or people in detention. Their efforts to reach those people within a given community who are most vulnerable or most exposed to risks of violations and abuses, or those who face the most imminent or direct threats, may lead to protection actors being perceived as biased and unresponsive to the difficulties facing the community as a whole. In devising their activities, protection actors need to take into account and mitigate possible tensions within or between communities that their activities may generate or exacerbate.

Bias in assessing and/or collecting the information on which humanitarian and human rights actors rely can also distort analysis, advocacy and subsequent programming in ways that may be perceived as discriminatory.

For example, when relying on information sent by individuals affected, via SMS or the internet, unequal access to technologies in different regions, or across generations, may create such bias. So would a data-collection effort using a format inaccessible to persons with visual, hearing or cognitive impairments. This being said, non-representative data can still be extremely useful and save lives, particularly at the onset of an emergency. As specified in Chapter 6, it is then up to every protection actor to be aware of these biases and to try to minimize them.

Finally, problems such as inaccessibility due to denial of access, insecurity or infrastructural constraints often limit protection actors' ability to deliver an impartial and non-discriminatory response. These constraints need to be identified, and explained to and discussed with the population concerned. Early action should be taken to overcome them in order to mitigate potential discriminatory effects or risks of partiality.



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

In their work, protection actors must ensure that their analyses, activities or communications do not convey a distorted view of the situation or cause others to misunderstand its true nature. Disproportionate representation or, worse still, the misrepresentation of protection issues either in bilateral communications with duty bearers, or more publicly, can severely distort understanding of a situation and misinform the response of others.

It is common practice when defining operational objectives for protection actors to establish priorities according to themes, population groups, etc. While these priorities are not discriminatory as such, measures should be taken to prevent them from leading to unintentionally discriminatory practices. For instance, while certain categories of population enjoy a particular status or protection under international law, it is essential to ensure that a needs analysis doesn't discriminate between persons with similar needs or vulnerabilities, based solely on their specific status. The response undertaken may take into account a particular status, but must also ensure that needs are addressed in a non-discriminatory way and that protection activities do not reinforce existing discriminatory practices.

It is important to adjust responses to meet the specific needs of particular groups within any population at risk, in order to ensure that all have the possibility to assert their rights. For example, specific population groups with recognized vulnerabilities, such as children (or multiple vulnerabilities, such as children with disabilities), may need targeted protection activities by protection actors with the skills necessary to provide them. However, protection activities should not be focused solely on a given group with particular needs, if this is to the detriment of another portion of the population affected that is suffering particular abuse or violations. This could, for example, be the case when abuses causing displacement of a certain population focus attention on internally displaced persons (IDPs) to the exclusion of those left behind – such as the elderly, persons with disabilities, the sick or wounded – who might be physically unable to leave.

In the broader perspective, 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 of the many protection actors involved in a given context is non-discriminatory. Questions relating to effective complementarity among different actors responding to the needs of diverse segments of the population affected are the subject of Chapter 5.

Finally, in cases where urgent needs exceed the capacity of a given protection actor and “triage prioritization” is necessary, the criteria guiding such choices must be non-discriminatory and based on the urgency and severity of carefully assessed needs.

NON-DISCRIMINATION, IMPARTIALITY AND PERSONS WITH DISABILITIES

In armed conflict and other situations of violence, persons with disabilities may be extremely vulnerable and have specific protection concerns. The principles of non-discrimination and impartiality require that protection actors, while carrying out a humanitarian response, address the rights and needs of persons with disabilities, take into account the specific risks that they face and treat their needs as a matter of priority.

As persons with disabilities are often among the least visible members of communities affected, protection assessments are likely to overlook them. Thus, protection workers should proactively seek to identify individuals with disabilities to analyse and address their needs.

Recognizing persons with disabilities' capacities and promoting their participation is of paramount importance in upholding their rights and dignity. The failure to include persons with disabilities in protection activities and in the humanitarian response as a whole may lead to significant harmful effects, exacerbating their marginalization in the community and exposing them to further abuse.

AVOIDING HARMFUL EFFECTS

S

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

Poorly conceived or carelessly implemented protection activities can aggravate or even generate additional protection risks for populations at risk or subject to violations and abuse (see Chapter 2). Although it is often extremely difficult to foresee the consequences of certain activities, or to determine when an action could result in harmful effects, it is nonetheless the ethical and legal obligation of protection actors to take measures to avoid such negative consequences. Such measures are essential when protection activities – including all processes of information gathering and use of such information – are being designed, analysed, implemented or monitored.

Protection actors must keep in mind that protection activities can inadvertently stigmatize individuals or communities who may be seen as providing sensitive information (see Chapter 6). Such perceptions must be kept in mind by protection actors, who bear the responsibility of preventing or mitigating such negative consequences of 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.

Those involved in protection activities tend to have a comparative advantage when it comes to analysing potential protection risks. They thus have a special role to play in raising awareness of the protection implications and potential risks of various actions. Examples include providing relief to IDP camps in a country at war, when armed groups are present among the displaced population, or re-establishing water pumps in villages regularly raided by neighbouring communities.

Arguably, every humanitarian crisis has a protection dimension, which requires all humanitarian actors to consider protection concerns as part of their humanitarian activities. They must all use a “protection lens” in their analysis and incorporate protection concerns in their response, for example, in the context of “protection mainstreaming” or “good quality programming” or in the application of the principle of “do no harm”. Protection actors must encourage and contribute to the discussion of these concerns among non-protection experts, and suggest measures they could take to reduce such protection risks.

In some extreme cases, the mere presence of humanitarian actors can be manipulated by an authority⁹ as part of its strategy to continue violating fundamental rights. A typical example is when national authorities plan to forcibly relocate a segment of the population, and call for the involvement of humanitarian actors at the relocation sites, in the hope that this engagement will diminish controversy and reduce international outcry over the process, possibly even legitimize it. Such cases raise serious ethical issues, such as having to choose between the urgent need to alleviate the situation of those affected (in terms of food, shelter, sanitation, etc.) and the consequences of being manipulated while abuses are committed. These critical protection dilemmas can even prompt humanitarian actors to contemplate withdrawal.

Protection actors must therefore promote a more comprehensive approach to the protection dimensions of humanitarian crises, as part of their fundamental responsibility 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.

Respect for the dignity of persons affected, encompassed in the principle of humanity, must underpin all protection activities. While this is an important principle for all humanitarian and human rights work, it is essential in protection. Showing respect to individuals in situations of extreme vulnerability, such as detention, signifies recognition of shared humanity. It implies, *inter alia*, taking the time and having the empathy to listen to, and interact with individuals and communities.

Measures to respect, safeguard and promote the dignity of persons at risk are not limited to engaging with them in a respectful manner. These measures also include facilitating their access to accurate and reliable information, ensuring their inclusion and meaningful participation in decision-making processes that affect them, and supporting their independent capacities, notably those of making free and informed choices, and of asserting their rights.

⁹ In this document, the expression “authority” covers all primary duty bearers as defined in Chapter 3, in particular 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.

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

The involvement of populations at risk helps ensure that protection activities respond to their needs and protect their rights. A dialogue with those at risk should contribute to the identification of these rights and needs, the planning, design and implementation of protection activities, as well as their monitoring, evaluation and adjustment. In addition to formal representatives, it is useful to identify existing forums and associations, such as women's groups, farmers' associations, disabled people's organizations and cultural associations where members of minority groups meet.

It is common for people at risk to have a detailed and intimate knowledge of the threats they face, and of the action that can be taken to improve their situation. Individuals and communities also devise independent strategies to cope better with their environment. It is thus important that a dialogue with individuals and communities affected should help identify self-protective actions that have proved to be effective, and could be reinforced.

In other cases, individuals affected or their families, groups and communities might be able to document violations and abuses that they themselves suffered or witnessed. Communities can, for example, establish lists of missing persons, inventories of belongings, map possible mass graves, etc. Protection actors who wish to recommend or support such efforts should, if not themselves competent to do so, seek the help of organizations with the appropriate expertise and responsibility to document or investigate. Any actor involved in such efforts must refer to applicable standards regarding evidence and other aspects of good practice for documenting violations and abuses, as well as how to do this without placing individuals at risk. This is particularly important if there is a possibility that the information gathered will be referred to later during a formal inquiry.

Confidence needs to be built to ensure an open and constructive dialogue with the population affected. The level of this involvement will nevertheless depend on the population concerned, and the intended action. Special sensitivity and training are needed to engage in a meaningful dialogue with individuals or communities affected, notably in the case of interviews with children, families of missing people, and victims of sexual abuse and their families.

In some instances, unhindered access to the population most affected may not be possible. Access to some places of detention or to particular communities or geographic areas may, for instance, be denied. Here, the correct course of action should be chosen on the basis of the best interest of the population affected.

Other barriers may also exist. In certain instances, some individuals and groups may be ostracized from the community in which they live. The community might even be the source of discrimination and intimidation against these groups and individuals, who may be the beneficiaries of a protection action (families of known political opponents, HIV-positive detainees, etc.). In other instances, an intended protection action may rely on maintaining a confidential dialogue with the authorities, and the involvement of the community might jeopardize the action. In such cases, it should nevertheless be possible to explain to the community the purpose and potential risks and benefits of protection action, without entering into confidential details.

Once implementation of the protection activity has begun, protection actors should, where possible, re-visit the population affected to inform them of progress made or

problems encountered. They should take this opportunity to monitor any positive or negative consequences for the population. In situations where the protection response is of a long duration, such as tracing of missing persons, the protection actor should consult periodically with the community, in order to gather any new, relevant information and report on progress.

Actively engaging populations at risk in protection activities provides a means for them to judge the performance of protection actors – which serves to increase the accountability of these actors. In reality, however, this accountability can be elusive. The relationship between communities and individuals at risk and protection actors is characterized by a marked imbalance of power. The rapid spread of communication technologies has enabled many individuals and communities to mobilize public opinion and, directly or indirectly, humanitarian and human rights organizations, when abuses and violations are being committed, including during armed conflict and other situations of violence. In this way, individuals may collectively be able to influence the agenda of these organizations.

Although some might use social media to publicize their dissatisfaction, communities still have relatively little recourse when the measures taken by protection actors are inadequate, inappropriate or ineffective. Humanitarian and human rights organizations may react differently to social-media criticism but should seek to address the underlying issues raised.

Protection actors are often formally accountable to some form of overseeing body, such as member States, boards of directors, or donors. Nevertheless, these bodies may, at best, have only a limited relationship with the population affected. This type of accountability, however important, therefore cannot be a substitute for direct engagement with populations affected. Proactive measures are required to help overcome this structural deficiency, and to establish a reasonable level of accountability to communities and individuals targeted by protection activities. These might, for example, take the form of complaints procedures established by protection actors to allow them to receive and treat complaints from populations and individuals: formal complaint mechanisms, hotlines or suggestion boxes.

Protection actors need to ensure that such mechanisms are as accessible as possible and do not exclude certain segments of communities affected (the elderly, the illiterate, persons with visual or hearing impairments, etc.).

ACCOUNTABILITY OF HUMANITARIAN ACTORS

The Core Humanitarian Standard glossary defines “accountability” as follows: “The process of using power responsibly, taking account of, and being held accountable by, different stakeholders, and primarily those who are affected by the exercise of such power.”

G

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

Those at risk usually have the clearest understanding of the nature of the risks they face (type of threats, potential perpetrators, time when the risks are higher). They often know

what some of the most effective means of mitigating these risks are. Protection actors should assess the individual and collective capacities for protection that exist within the community affected. At a minimum, they must ensure that their own actions do not diminish these capacities. More ambitiously, they should try, to the extent feasible, to reinforce these capacities and to strengthen the resilience of communities over time.

When supporting community-based protection mechanisms, protection actors must nevertheless be aware of the limits to this strategy, for it is the responsibility of the authorities to protect individuals and the population as a whole. Furthermore, they must be careful to avoid reinforcing inequitable power relations by, for example, excluding segments of the population, or other practices that might be harmful to particular groups within a community.

Whenever feasible, protection actors should thus favour a longer-term strategy that builds on the capacity of populations affected to organize themselves, and that engages the authorities at all levels (see Chapter 3) to safeguard their rights.

COMMUNITY-BASED PROTECTION

Methods and approaches to community-based protection have been developed by protection actors who have a significant presence among communities affected and support those communities in the measures they take to protect themselves.

Community-based protection uses a community-based approach to address the protection issues that a community faces. Depending on the severity and prevalence of the risk being addressed, these community-based efforts should form part of a larger strategy carried out by other actors that support the community-based approach.

Ideally, community-based protection will *originate within and be led by people from the communities affected*. This means that community actors control resources and decision-making and that this is supported by external actors.

This is not always possible, however, given that communities may be dispersed as a result of displacement or fragmented owing to the political dynamics of the conflict, or because continual threats inhibit community-level organizing. In these circumstances, opportunities for community-based protection strategies can still be pursued: protection actors may seek to *better engage* communities in their own protection – for example, by facilitating the mapping of threats, undertaking safety audits, creating a “problem tree”, or creating an action plan and supporting its implementation.

Even under the most difficult circumstances, protection actors carrying out analyses and protection activities should, at the very least, begin by seeking out the perspective of people affected – for example, by hiring full-time community outreach staff, undertaking focus group discussions and conducting participatory assessments. Over time, as the situation evolves and these methods of engaging communities take effect, it may be possible to move towards greater community initiative and control over protection strategies.

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.

To make informed choices and develop resilience, and self-protection and coping mechanisms, communities and individuals at risk need a good understanding of the threats to which they might be exposed. While they normally have a better understanding of these threats than external actors, there may be cases where protection actors possess essential pieces of information that could influence how communities apprehend the risks they are facing. Withholding such information may in some cases have negative consequences for individuals and communities.

Without disclosing any confidential information, protection actors should share with communities and individuals their reading of existing abuses and violations and related trends, if doing so will help those communities better define their own protection strategies. One area where this is typically done in a coordinated manner is related to the risks posed by mines and explosive remnants of war.

Nevertheless, given common fears of providing information of military nature to one party, or of being perceived to be doing so, protection actors should be extremely careful not to disclose information they have acquired through their field presence that could be regarded as “military intelligence”, such as the location of mobile checkpoints along roads they have just travelled, movement of troops they have witnessed, or the presence of a local commander from a rebel group in a village they have recently visited. The nature of what can be perceived, by local authorities and armed actors, as military intelligence might vary from one context to another. Protection actors should be attentive to the way armed actors perceive them.

Furthermore, protection actors must develop an adequate understanding of the culture, and the organizational and leadership structures of populations affected, before engaging in information sharing, to ensure that information reaches all members of the community and that authoritarian or abusive power relations within the community are not unintentionally reinforced.

Individuals and communities that have already been affected by abuses and violations also need to receive adequate and timely information on existing services and support they can obtain (see Guideline 5.5).

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 associations – such as those of families of missing persons – women’s groups, representatives of indigenous peoples and minority groups, disabled people’s organizations or LGBTI organizations. This may take time, especially when working with people who may not be well informed of their rights under domestic and international law.

ANNEXES TO CHAPTER 1

ANNEX 1: PROTECTION WORK FOR PERSONS WITH DISABILITIES

According to the Convention on the Rights of Persons with Disabilities, “disability results from the interaction between persons with impairments [physical, mental, intellectual or sensory] and attitudinal or environmental barriers that hinders their full and effective participation in society on an equal basis with others”. According to the World Health Organization, about 15% of the global population lives with some form of disability – a proportion likely to be higher in countries affected by armed conflict, owing to violence-induced injuries and mental-health trauma. In spite of these significant numbers, persons with disabilities are often overlooked in humanitarian emergencies and lack access to adequate protection and support.

Yet, the overarching principles of humanity, non-discrimination and impartiality require that protection actors respond to the needs and rights of persons with disabilities. Individuals with disabilities are among the most at-risk groups in armed conflict and other situations of violence, and experience specific threats and challenges.

When populations affected by conflict flee to safety, persons with disabilities are likely to be left behind and to fall victims to violence because they are not able to move as fast as others or may require additional support. They risk being separated from their caregivers and may lose assistive devices such as wheelchairs and hearing aids, thus making them even more susceptible to a range of threats. Persons with disabilities are also often excluded from social networks, which provide much-needed support in situations of armed conflict or displacement. As a result of this isolation, they often experience abuse in the community, ranging from discrimination and neglect to physical and sexual violence. In addition, children and women with disabilities experience multiple layers of risk owing to their age or gender coupled with their disability.

In order to ensure that the protection concerns of persons with disabilities, and the specific barriers and threats they face, are adequately reflected and addressed, it is essential that protection actors collect data and disaggregate this information not only by gender and age but also by disability.¹⁰

However, biases in the assessment and/or the collection of information often prevent protection actors from addressing the risks faced by persons with disabilities. For example, protection workers conducting an assessment may not immediately notice large numbers of individuals with disabilities (because these people may be confined to their homes); this may cause them to wrongly infer that there are no persons with disabilities among the population affected. Protection workers should thus proactively seek to identify persons with disabilities.

Protection actors may also simply not be aware of how to detect a disability. Too often, humanitarian workers may associate disability with the use of a wheelchair and may not recognize the broader spectrum of disabilities, including invisible ones, such as intellectual and psychosocial disabilities (mental-health conditions). Building knowledge and understanding among protection actors of the rights and needs of persons with disabilities is key to ensuring that protection work is inclusive.

The failure to include persons with disabilities in protection activities and in other sectors of the humanitarian response may have harmful consequences for persons with

¹⁰ Disability data should be collected based on the [guidelines set out by the Washington Group on Disability Statistics](#). See also [DFID's guide to disaggregating programme data by disability](#).

disabilities and their families and may exacerbate their marginalization in the community. For example, if food distributions or sanitation and hygiene facilities are inaccessible to persons with disabilities, they must depend on other people to fulfil their most basic needs, which makes them particularly susceptible to exploitation and abuse. It is important that protection actors sensitize non-protection experts on protection concerns affecting persons with disabilities, and on how to mitigate them through their activities.

Upholding the rights and dignity of persons with disabilities must guide all protection activities. To this end, protection workers should always consult with persons with disabilities and their representative organizations and involve them in the planning, implementation, monitoring and evaluation of all activities affecting them. Persons with disabilities know better than anyone else the threats they face and the protective actions that should be taken, and their capacities and resources should be acknowledged and used. When interviewing persons with disabilities, protection actors should pay specific attention to confidentiality and privacy, in some cases also privacy from their families or caregivers, and support the right of persons with disabilities to make their own informed choices. Such support may include the use of alternative means of communication, such as sign language.

Protection workers should also partner with local organizations of persons with disabilities, which can assist them in identifying persons with disabilities and facilitate referral to local support services.

Humanitarian organizations increasingly acknowledge the challenges faced by persons with disabilities in emergencies and the need to better include them in the humanitarian response. In May 2016, the [Charter on Inclusion of Persons with Disabilities in Humanitarian Action](#) was launched at the World Humanitarian Summit in Istanbul. In the Charter, States, humanitarian NGOs, UN agencies and disabled persons' organizations committed to removing barriers to relief, protection and recovery support for persons with disabilities and ensuring their participation in humanitarian programming.

ANNEX 2: 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.

Gioffi 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.



CHAPTER 2

MANAGING PROTECTION STRATEGIES

- 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.
- 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.

Monitoring

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

Evaluation and learning

- S** 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.

In recent years, many protection actors have sought to enhance their capacity to monitor and evaluate the efficiency and effectiveness of their protection strategies. Yet, when compared to most assistance and relief programmes, it appears that results related to protection work remain more difficult to plan for and measure.

The following standards and guideline refer to the main stages of the project management cycle already recognized and used by most organizations. They highlight certain elements particular to protection work that should be taken into account, from context-specific analysis and development of strategies to monitoring and evaluation of protection work.

It is commonly agreed that monitoring and evaluation are essential for making improvements and changes to programmes in real time, as they enhance accountability and make it possible to learn from past experiences and then to use the lessons learnt in future programmes.

Revision of these standards was driven by the growing understanding that “protection” needs to be approached in a manner geared towards achieving measurable protection outcomes. These are manifested in the form of reduced risk, including through improved fulfilment of rights and restitution for victims. “Risk” refers to the probability of violation, abuse, harm and suffering. Analysing risk requires assessing both the source of the threat and the vulnerability and capacity of those exposed to it.

This chapter uses generic terminology that may differ from the specific wording used by various organizations with regard to analysis, strategy, objectives, impact, etc.

Standard 2.1 underscores the importance of protection analysis, conducted on a continual basis, and presents some of the key elements of an analysis of the protection situation and environment, in order to establish priorities and subsequently draft strategies.

Guideline 2.2 presents the utility of establishing a causal logic for the actions to be taken to achieve the desired outcome of reduced risk and how to relate these to protection strategies and programme objectives.

Standard 2.3 underlines the importance of ongoing analysis of risk patterns and monitoring of programme implementation, and describes the challenges involved and the possible approaches.

Finally, Standard 2.4 addresses the need for evaluations of protection action to be carried out and for protection actors to seek actively to learn from their efforts to reduce risk.

Continual analysis of risk patterns (including existing or potential violations and abuses) in combination with monitoring of the programmatic response enables the periodic capture and possible measurement of the intended – and unintended – results achieved. It supports the proper implementation of the strategy chosen, allowing for sound decision-making processes that enable the chosen strategies to be adapted to the fast-changing environment in which protection work often takes place. These Standards outline a common basis from which to conduct this analysis and monitoring.¹¹

11 The [IASC Policy on Protection in Humanitarian Action](#) and the [IASC provisional guidance on the development of Humanitarian Country Team Protection Strategies](#) are also references for formulating protection strategies. For the United Nations system, the [UN Secretary-General’s Human Rights Up Front initiative](#) tasks Resident Coordinators or Humanitarian Coordinators to lead and coordinate the Country Team in developing and implementing a country-level strategy to address potential or actual violations. Other strategies should aim to complement and mutually reinforce these.

Evaluation allows additional and better understanding of the accountability of the various stakeholders involved and enhances the ability to draw lessons from the action conducted. Whereas continual analysis and programme monitoring are ongoing activities that should already be incorporated in the initial design of protection strategies, formal evaluations tend to take place on a case-by-case basis once a protection strategy has been completed, or when it is well under way. A variety of techniques can be used for evaluating protection outcomes and impact, including learning reviews, participatory evaluations with target groups, and both internal and formal external evaluations.



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.

To respond to protection concerns in a manner that is relevant to people's needs, the underlying factors driving the risks people are experiencing must be clearly identified and analysed in their constitutive elements and in the specific context where they are occurring. While comprehensive and thorough problem analysis is an important prerequisite for all programming, it is absolutely crucial for protection action. The content of protection action depends on nuanced elements in highly complex contexts involving numerous actors and characterized by ongoing changes in dynamics. Context-specific analysis, using up-to-date data as far as possible, is key to determining an initial course of action, while continual analysis is essential to informing its adjustment over time.

Detailed identification of the risks and the primary actors concerned, and of causes, motivations and circumstances, is essential for determining the right course of action. Addressing only the symptoms can sometimes do more harm than good.

The following box outlines the information that needs to be collected and the analysis that needs to be undertaken as the basis for identifying effective action. It can be adapted to specific contexts, to the risk patterns being examined, and to the needs of each organization.

ELEMENTS OF A SOUND ANALYSIS FOR PROTECTION WORK

- **Analysis of the different ways in which people are at risk.** Analysis should start, as far as possible, from the perspective of the people affected, in order to identify ongoing patterns of violations and abuse, specific threats, who is vulnerable to these threats and why, what are the sources of the threats, and what capacities people can bring to bear to reduce risk themselves. Capacities may be manifested in individual or community-based initiatives to address the threats that individuals and communities experience and in mechanisms for coping with ongoing threats. Protection actors should ideally seek to strengthen relevant and positive capacities and coping mechanisms as the starting point for their protection strategies. However, some harmful coping mechanisms – such as trading sex for food, or child labour – may themselves constitute protection problems.

Analysis should not be focused exclusively on pre-defined population groups that are typically assumed to be most vulnerable and marginalized, and should always avoid drawing premature conclusions. Protection actors should also avoid pre-determining what the response will be and instead ensure that they tailor the response to the specific risk patterns identified. This will be greatly aided by detailed disaggregation of risk factors. In addition to sex and age, exposure to certain threats may arise from the location of populations at risk or subject to violations or abuses, the activities that different populations carry out, the time and place in which they are undertaken, as well as from people's access to services or resources. How people are affected by specific types of threats is also often a function of gender, disability, sexual orientation or social, ethnic, religious or political affiliation (see Chapter 1).

- **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.** They may be positively embracing their obligations and contributing to an environment conducive to respect for populations at risk or subject to violations or abuses, while also inadvertently harming people and damaging property and infrastructure, or overtly committing violations or abuses. Their behaviour and attitude may involve actions of both commission (overt action) and omission (failure to act). These may or may not constitute outright or deliberate violations or abuses but they nevertheless affect people's vulnerability. This analysis should therefore take into account the gaps and the existing policies and practices of the authorities concerned that drive threats and create or exacerbate vulnerabilities in relation to the specific risk being analysed. Analysis should also include the capacity, commitment and willingness of the primary duty bearers to fulfil their obligations and address these problems.

This analysis should also consider incentives and disincentives to change the behaviour of those responsible for the threats. This should include understanding their interpretation of social, religious, moral or legal norms in relation to the specific risk being analysed. To the extent possible and for a better understanding of the circumstances, an analysis of structures, chains of command, motivations, objectives and diverse driving interests – be they political, economic, criminal, personal, familial, ethnic, etc. – should be included. An analysis of the applicable legal frameworks is also important. How far a protection actor should take this part of the analysis will depend on its specific mandate, relevant expertise and the activities it carries out, as well as the specific risk being addressed.

- **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 (see Chapter 5).
- 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. For example, the behaviour of security forces may not be limited to mistreatment of IDPs in camps, but may be mirrored in soliciting bribes at checkpoints or other misconduct, which, taken together, may indicate an absence of discipline within the chain of command. Framing a certain pattern of behaviour in a broader context is critical to understanding how this behaviour should be addressed.

Analysis should include information gathered from the population at risk or subject to violations or abuses with regard to the actions they think are required to address the identified problems. For example, they may want a particular checkpoint to be moved further away from inhabited areas or female police to patrol areas near women's latrines and bathing facilities in IDP camps. People in insecure areas often have very clear ideas about what will improve their situation. Protection actors should establish appropriate methods of facilitating two-way information flow with people affected. In part, this is to enable their ongoing engagement in decisions about action taken on their behalf. In addition, being uninformed is disempowering for people affected by crises, and access to information may be a critical means of enabling people to address the risks they face. Protection actors should be mindful of gatekeepers of information, as they are capable of both supporting and acting as barriers in the flow of information to and from people affected.

Even during emergencies, protection analysis should, wherever practicable and safe, be conducted as far as possible in a participatory way and include a broad cross-section of the population at risk or subject to violations or abuses. Care should be taken to include potentially marginalized and discriminated-against persons and groups, as they may otherwise be prevented from voicing their concerns.

Where dialogue with duty bearers can be established, it should continually inform protection analysis as well as the identification of options to address the problems faced; both processes should incorporate the perspectives, challenges and capacities of the relevant authorities.

In addition, protection analysis may require the involvement of various disciplines, sectors and actors in order to make it possible to fully understand the factors driving certain risk patterns and to enable the identification of all possible means of reducing the risk factors. For example, to understand traditional norms and societal attitudes regarding the treatment of children during armed conflict, it may be necessary to consult with traditional leaders or sociologists at a local university. Understanding the consequences of the presence of unexploded ordnance may require contextual knowledge and expertise with national or traditional laws and practices regarding land tenure.

Accordingly, a combination of diverse methods, and a mix of quantitative and qualitative data, should be used to understand the context and the protection implications of the dynamics present – ethnographic mapping, stakeholder mapping, conflict analysis, perception data, surveillance data, etc. Instead of duplicating existing analyses, every effort should be made to draw on existing information available from other actors. Care should be taken, however, to ensure that existing data are used appropriately, especially where they include personal data or sensitive protection data and information, and are not used to make excessively broad generalizations – for example, interpreting findings from one community as being applicable across a broader context. In this regard, protection actors should ensure that they are confident in the sources and methods of information collection that inform the analysis on which they are basing their decisions (see Chapter 6).

Protection analysis should not be treated as a one-off exercise; instead, it should be carried out continually throughout the response. An initial protection analysis can serve as the basis for an initial and interim response. Interim or initial response activities can then provide a basis for further dialogue and deeper analysis with the relevant stakeholders, in order to clarify assumptions, develop partnerships and develop strategies to more comprehensively address the risk patterns.

A strong protection analysis lends itself to prioritization of the risks to be addressed, establishing desired outcomes in terms of reduced risk, and to development of a causal logic for a strategy to reduce risk, as well as to identification of key indicators of risks to be continually analysed in order to know whether the strategy is yielding the desired results.

6

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.

Achieving a protection outcome, or ultimate impact, of reduced risk means that the component parts contributing to risk must be addressed. In other words, efforts should be oriented towards reducing the threats that people face, reducing people's vulnerabilities to these threats, and enhancing the relevant capacities in relation to these threats.

It is unlikely that a single type of activity can achieve comprehensively reduced risk. Even within one organization, achieving reduced risk may require a variety of disciplines working towards a common desired outcome.

For example, depending on the risk pattern being addressed, this may entail simultaneous delivery of material and medical assistance, dialogue with authorities and support for community-based protection strategies. Protection actors should aim to maximize complementarity with other actors, as well as between different activities and programmes within the same organization, in order to address the various risk factors.

Pulling all relevant actions together into a strategy can be a complex exercise. It will be greatly aided by the development of a context-specific causal logic (or theory of change), designed to address a specific risk pattern and achieve a reduction in the threats and vulnerabilities, and also to enhance the capacities of the population affected. 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. These milestones may include certain changes in behaviour, attitude, policy or practice on the part of certain duty bearers or other stakeholders necessary to reduce the risk factors.
- describe the sequence of actions, including the multiple sectors and disciplines that may need to be mobilized to contribute to the desired outcomes. Action may be needed at a variety of levels, ranging from the individual or community level to sub-national, national or international levels. 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 then allows for the identification of proactive means of expanding spheres of influence and of the various roles of a range of actors in achieving an outcome. This is the basis for cultivating complementarity among actors for the purpose of comprehensive risk reduction.
- explicitly articulate the assumptions inherent in the sequence of actions, the roles of the different actors, and the results these are expected to yield with respect to changing the risk factors to bring about overall reduced risk. The rationale behind the assumptions – based on past patterns of behaviour, new policies or agreements that have emerged, etc. – should be made clear.

Establishing the causal logic for an activity or response enables protection actors – individually and collectively – to situate their role within the broader dynamics of the context, including in relation to opportunities to influence key duty bearers to meet their obligations under international law, and in relation to other actors who have a decisive influence on events and on the policies and practices of duty bearers. The process of developing a causal logic can thus help protection actors better understand their own spheres of control and influence in relation to their larger sphere of concern.

These steps can also be helpful in carefully weighing the implications of broader contextual challenges, such as humanitarian access and factors constraining access. As such, the task of cultivating the conditions necessary to reach people affected and carry out the necessary work should become part of the strategy rather than be treated as constraining factors separate from the risk factors being addressed.

When multiple actors need to work together to achieve the desired outcome, the process of developing this causal logic can serve as the basis for establishing a collective vision and mutual understanding of each other's unique roles. This causal pathway can then be combined with SMART objectives and specific activities to form a comprehensive strategy.

Different protection actors may use the terms “outcome” and “impact” in different ways. Regardless of preferences in terminology, managing protection strategies requires an orientation towards the reduction of risk, supported by an analysis, an articulated causal logic and SMART objectives.

Protection strategies should include:

The Desired Outcome (or Impact) in terms of reduced risk of violations or abuses. These may include outcomes achieved in the short, medium and long term, as well as impact that is sustained beyond the implementation period.

SMART Objectives: These are specific, measurable, achievable, relevant and time-bound changes – underpinned by a causal logic – that will contribute to the desired outcome. They may be:

- changes in specific risk factors, i.e. the threat, the vulnerability vis-à-vis the threat, capacities vis-à-vis the threat; and/or
- milestones to be achieved in order to change these risk factors – for example, in the form of the expected changes in the behaviour, attitude, policy, practices or decisions of the duty bearers or other relevant stakeholders.

Activities and Outputs: The specific activities to be carried out and the outputs expected – who will carry out the activities, the time frame within which they are to be carried out, and how they are linked to one another – in order to meet the identified objectives.

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 continual analysis of changes in risk patterns and undertake continual programme monitoring in order to adjust strategies and activities as required.

In recent years, different kinds of monitoring activities have been undertaken more frequently and systematically. However, it remains a challenge to ensure that ongoing analysis and monitoring are designed in a purposeful manner, relevant to the desired outcome or impact.

Using protection analysis and the causal logic for a response or an activity as starting points, a protection strategy should include the necessary information management and monitoring systems, in order to:

- continually develop and deepen the protection analysis
- monitor programme implementation, including critical milestones
- adjust and change operational plans during the programme cycle
- learn from the present experience to inform future strategies and programmes and
- be accountable to key stakeholders, including the local population.

The information management and monitoring systems should include the choice of indicators, methods and procedures for collecting information, and how the data will be used and by whom. Every effort should be made to draw on the information available to other actors in order to avoid duplication and to triangulate information (see Chapter 6).

Measuring the actual outcomes (or impact) and results of protection strategies presents considerable challenges. The better the protection analysis, the more feasible it is to define and describe precisely the risk patterns faced by a population and to establish a baseline of risk factors that a protection strategy seeks to address, and ultimately reduce, to achieve a protective outcome or impact. In addition, the causal logic that underpins the strategy serves as a basis to monitor critical milestones leading to reduction of risk.

Establishing a quantitative baseline against which to measure outcomes and impact is often very difficult. For example, owing to practical and/or ethical considerations, it may not be possible to collect information on the frequency of incidents of sexual violence against women. In fact, in most cases, it is not possible to consistently undertake incident-based monitoring or assess direct impact by comparing the number of incidents that took place before and after the programme got underway.

However, when a protection analysis is carried out to tease apart the various factors contributing to ongoing violations, abuses and risk patterns, these factors can then be used to define key indicators to monitor the underlying specific threats, vulnerabilities and capacities. Tracking whether these variables are going up or down should enable the protection analysis to be deepened and refined, and serve as a basis for continually assessing whether the strategy is achieving the desired results and, if it isn't, to undertake course adjustments to achieve the desired results. This should also enable the detection of new risk factors and any negative consequences that may arise from the implementation of the strategy. In this regard, monitoring is an essential activity to ensure that programmes are developed and implemented in an iterative way that is responsive to new information and developments in the context.

This means that tracking risk patterns will often entail assessing less direct indicators (also known as proxy indicators), such as people's perceptions (those of entire communities or of sub-categories, such as men and women, boys and girls, traders) of their safety or the degree to which they increase or reduce their movements in a given area. Such proxy indicators can reveal shifting trends affecting a specific protection problem.

Different actors will approach this continual protection analysis in different ways, depending on their unique mandates and expertise, and on how the continual analysis influences the ultimate outcome they seek to achieve. For example, human rights monitoring is in itself central to the work of human rights organizations, providing the basis for their analyses and activities and ultimately, for improved and strengthened protection outcomes.

In addition, once the causal logic underpinning the response strategy has been established, the milestones leading towards the reduction of risk, and which underpin the programme design, serve as the basis for programme monitoring. Monitoring programme implementation, including key activities and progress, against these milestones allows protection actors to gauge whether their programme is achieving the desired results, whether the causal logic underpinning the response is a viable pathway to achieve the reduction of risk, or whether the assumptions and the strategy need to be revised.

Protection information management systems should be designed to meet these ongoing protection analysis and monitoring needs. This is essential for ensuring that strategies to achieve protection outcomes are not treated as linear processes but as iterative and adaptable processes that are sensitive and responsive to complex and dynamic realities (see also Chapter 6).

One way to overcome the difficulty of measuring protective impact is to use "result monitoring" to track changes in the behaviour of perpetrators, the actions of the authorities responsible, the behaviour of other relevant actors (e.g. regional/international actors who have an influence on the situation) and the actions of the people affected themselves. These results represent changes in risk factors and intermediary steps or milestones towards the desired outcome of overall risk reduction. Various kinds of qualitative and quantitative indicators can be defined according to the expected results defined in the SMART objectives.

As mentioned above, in many contexts, it may not be possible or ethically appropriate to collect detailed information on the occurrence of sexual violence. In such cases, monitoring will often depend on **proxy indicators** derived from the protection analysis and the assumptions present in the causal logic, which can reveal whether there are changes in the risk patterns and whether the desired outcome or impact is being achieved.

The choice of indicators and the way in which related data are collected should, to the extent possible, be based on consultations with the people at risk. When deciding on sources of information, protection actors should avoid duplicative information collection as far as possible and seek to draw on existing relevant monitoring mechanisms (see Chapter 6). Inter-agency or peer reviews in particular may help assess the validity of the causal logic underpinning the strategy, as they enable protection concerns to be considered within the context of the broader humanitarian situation and response.

Isolating the effects of the efforts of any one protection actor from the diversity of factors influencing a given situation can be challenging. Qualitative indicators should be triangulated with other indicators and sources in order to be interpreted correctly and, whenever possible, to assess to what degree a change in the risk factors can be attributed to the action of specific actors. While every effort should be made to systematically track the results achieved by protection activities, over-emphasis on measurable indicators should not distract attention from capturing and understanding meaningful results that cannot be measured.

Continual analysis and programme monitoring should also detect the unintended or negative changes in the context. Protection actors sometimes face dilemmas when engaging in an action that, although expected to improve the situation for the people they want to serve, might have some negative consequences in the short or long term. They may nevertheless engage because they foresee that the positive outcome will largely outweigh the potential negative consequences (see Chapter 1, on the principle of “do no harm”, and Chapter 6, on managing risks). While carrying out monitoring activities, they ought to make sure that they assess all results and thereby identify both the positive and the potentially negative changes.

When deciding on the most relevant indicators, organizations should be realistic regarding the resources they will need to establish a baseline, to report against these indicators and to use the information provided. In any purposeful and proportionate approach to information management, a careful balance has to be struck between the expected benefit of the information provided by the indicator and the resources needed to collect and analyse it. At the same time, protection actors must avoid harmful effects when conducting monitoring activities (see Standards 1.4 and 1.5, and Chapter 6).

In addition to using indicators, assessing the effects of a protection action should also involve a more qualitative and general analysis of changes in the political, social or economic contexts. As is the case when analysing needs and problems, protection actors must make all possible efforts to involve – in analysing the effects of protection action – the population at risk or subject to violations or abuses. Changes in the lives of the population affected can be captured through participatory monitoring and by collecting stories giving evidence of these changes.

The challenges in establishing measurable results and in attributing these results to particular actors should not deter protection actors from endeavouring to innovate in this challenging area, and/or to tackle complex protection issues.

EVALUATION AND LEARNING

S

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.

Enhancing protection during crises involves working within the interplay of numerous complex and continually changing dynamics. As noted above, this necessitates continual protection analysis, including ongoing monitoring of the risk factors protection actors seek to address. This is essential in order to enable a high degree of adaptability throughout the course of strategy implementation. A conscious effort to cultivate and encourage adaptability in programming de-emphasizes overly simplistic success/failure judgments of programmes (which can translate into risk aversion and paralysis in the face of complex challenges); instead, it emphasizes evidence-based decision-making and risk-taking.

Protection strategies thus benefit from allowing space and time specifically for protection actors to regularly reflect on the actions taken to reduce risk, and to review and adapt their objectives and activities as they relate to achieving the desired outcome. While informed risk-taking should be encouraged, every effort should be made to ensure that the entire burden is borne by the implementing organization, not the population at risk or subject to violations or abuses.

Regular investment in learning – involving people affected, staff and other stakeholders – enhances ownership and responsibility for the methods, processes and results of protection strategies. Organizations engaged in protection should also seek to encourage adaptability and systematically internalize lessons arising from programme implementation – for example, by disseminating programme documents internally, incorporating new methods in organizational policy and guidance, and encouraging critical discussion among staff.

Finally, evaluations of the entire protection action may be conducted whenever necessary in order to better capture and formulate lessons learnt. By evaluation, we mean: “The systematic and objective assessment of an ongoing or completed project, programme or policy, its design, implementation and results. The aim is to determine the relevance and fulfilment of objectives, development efficiency, effectiveness, impact and sustainability.”¹²

Care should be taken to avoid definitively attributing results or outcomes to solely one actor or action. The presence of numerous dynamic variables in crises makes it practically impossible to confidently establish causation between actions taken and specific outcomes. Rather, we should seek to understand the relationships between changes in risk patterns and the actions of various actors in terms of partial attribution or contribution to outcomes.

Evaluations are especially important to better understand the contributions that various actions and actors make to achieve a protection outcome. Having established the causal logic for the activity or response, evaluations can seek evidence for the contributions of various actors and actions towards the milestones and

¹² OECD, *Glossary of Key Terms in Evaluation and Results Based Management*, OECD, Paris, 2002, pp. 21–22.

results achieved, and then assess it. Of particular interest is the adoption of policies, practices and behaviour by relevant State and non-State authorities that contribute to their enhanced compliance with their obligations under international law and to an environment more conducive to protection.

The documentation of multidisciplinary programme design and/or strategies involving the contributions of multiple actors may yield insights into appropriate methods for analysis, planning and coordination and, more generally, into how protection outcomes can be collectively achieved. Evaluations are also essential for determining what long-term and sustained impact, if any, a programme has had, including unintended impact. This may include positive as well as negative impact. Efforts to internalize lessons arising from programmes and to invest in protection evaluations also serve to reinforce informed risk-taking and promote a learning culture within a community of actors involved in protection work.

Evaluating protection strategies is particularly difficult because of the variety of issues that may be addressed, the volatility of all the factors affecting the risk people face, the diversity of the sectors, actors and disciplines that may be involved in efforts to reduce risk, and the range of levels at which activities may need to be carried out. This gives rise to a common challenge encountered in humanitarian and human rights evaluations, namely understanding the relationship between cause and effect, as well as whether and how a result may be attributed to a certain action or actor. Prior to commencing an evaluation it is therefore important to assess whether protection outcomes or impact can be evaluated, i.e. the “evaluability” of an activity or response.

Evaluability is enhanced when a programme has a clearly articulated desired outcome and expected results. This determines what to evaluate and where to look for sources of data to establish evidence or results – positive and negative, intended and unintended.¹³ This evaluability is further enhanced and informed by continual protection analysis and a causal logic setting out the pathways for achieving the outcome. In fact, protection actors should design and manage protection strategies with a view to achieving measurable outcomes or, in other words, with a view to their evaluability.

Evaluation also shares many of the same challenges as monitoring, with regard to determining useful, relevant and measurable indicators. This further underscores the critical importance of protection analysis and of developing such analyses on a continual basis.

Evaluators should be familiar with the professional standards in this document, which may be used to inform the overall approach and methods to be used. In particular, evaluators should pay close attention to Chapter 6 (related to managing data and information for protection outcomes) – for example, in relation to personal data, confidentiality, the collection of information from people affected, and the importance of securing these people’s informed consent.

Evaluation should be conducted professionally – by trained staff – and in accordance with the principles of utility, propriety, feasibility and accuracy (see box).

¹³ F. Bonino, *Evaluating Protection in Humanitarian Action: Issues and Challenges*, ALNAP, London, 2014.

GUIDING PRINCIPLES FOR EVALUATION¹⁴

Utility has to do with making sure that the findings and lessons learnt from the evaluation are used for future actions. Therefore, persons involved in or affected by the evaluation should be identified from the outset and their needs taken into account. The evaluation should be planned and conducted in a way that encourages follow-through by stakeholders. Finally, the findings (and interim findings) should be disseminated to intended users.

Propriety entails ensuring that the evaluation will be conducted legally, ethically and with due regard for the welfare of those involved, and for that of those affected by its results. Evaluations should respect the rights and welfare of people. Evaluators should respect dignity and confidentiality, especially with regard to those who are at risk of recrimination.

Feasibility is intended to ensure that the evaluation is realistic and prudent.

Accuracy concerns method and tries to ensure that an evaluation will reveal and convey technically adequate information and describe purpose and procedures. A detailed analysis of the context is important. Sources of information should be described and triangulated. Reporting should be reliable and impartial and follow the principle of “do no harm”. Conclusions should be justified.

¹⁴ Drawn from 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.

ANNEXES TO CHAPTER 2

ANNEX 1: FROM SMART OBJECTIVES TO INDICATORS OF EXPECTED OUTCOMES AND IMPACT: AN EXAMPLE

Sexual and gender-based violence can involve many different patterns of risk. Assaults may be perpetrated by spouses or other household members, neighbours and community members, people in positions of traditional and formal authority, members of security forces (such as prison guards, police, military forces) or non-State armed groups. Women and girls, and men and boys – as well as some particular minority groups, such as detained men or gay, lesbian and transgender people – may be vulnerable to sexual violence. The pattern of violence may vary greatly from context to context and may be driven by a range of factors present within a given situation.

Understanding the drivers behind sexual and gender-based violence – as well as who is vulnerable and why – is critical to knowing how to reduce the threat, reduce vulnerability to the threat and enhance relevant capacities. The example below is not specific to any context and is intended as a general example for illustrative purposes only. It should not be understood as a response required for all situations of sexual and gender-based violence.

Desired outcome (or impact)

Women and girls are able to carry out daily activities without regular risk of sexual violence in [geographic region] X.

SMART objective

Sexual violence affecting women and girls in [geographic region] X decreases by 75% within the next three years.

Information collection for three types of indicators enables the ongoing protection analysis and programme monitoring necessary for continual adjustment of strategies to achieve the reduction of risk:

- **Risk indicators:** These are indicators (identified in the protection analysis) of threats, vulnerabilities and capacities that are being addressed.

Examples may include a recurring pattern of behaviour by armed groups towards a certain population or the excessive use of force by security forces, or the commitment of duty bearers to comply with their obligations (threat), the extent of a certain population's exposure to this threat (vulnerability), and strategies to address or cope with the threat by the people affected (capacities). Changes in these risk factors contribute to the desired outcome of reduced risk. Perception indicators – vulnerable people's views and perceptions of their risk factors – can be used as proxy indicators of the overall risk.

- **Progress indicators:** These are indicators of milestones that need to be achieved – at different levels – in order to reduce the risk factors. These milestones contribute to the desired outcome of reduced risk.

Examples may include the adoption of disciplinary measures within an armed group to discourage certain behaviour, access to effective remedies for violations, the presence of a deterrent to reduce people's exposure to a threat, and the adoption of a variety of methods by people affected to cope with and address threats.

Programme indicators: These are outputs that correspond to activities to meet the objectives and bring about the desired results. Monitoring outputs can help track the capacities and contributions of the range of actors involved in the strategy and ensure ongoing awareness of whether and how the activities are approaching the milestones that have been defined and yielding the desired results.

For example, building on the desired outcome and objective above:

- **risk indicators** to track the risk factors (threats, vulnerabilities, capacities) that are being addressed to reduce risk could include the following:
 - number/ratio of police personnel who understand the crime of sexual violence
 - number/ratio of police personnel who are familiar with applicable laws and policies and their responsibilities in addressing the crime of sexual violence
 - number/ratio of allegations of incidents of sexual violence received by the police according to place and time
 - number/ratio of alleged incidents that the police have taken measures to investigate effectively, promptly, thoroughly and impartially
 - number/ratio of women and girls reporting confidence in mechanisms to formally report incidents of sexual violence
 - number/ratio of women and girls reporting confidence/lack of confidence in measures taken by the police to investigate sexual violence
 - number/ratio of women and girls reporting feeling safe/unsafe from the threat of sexual violence, disaggregated by age, time, place
 - number/ratio of women and girls reporting confidence/lack of confidence in measures they can take to diminish their exposure to sexual attacks according to place and time (e.g. moving in groups or working in groups in the field)
 - number/ratio of women reporting safety of daily access to resources/services
 - number/ratio of duty bearers acknowledging the problem of sexual violence and of perpetrators being prosecuted and held accountable, according to type of perpetrator

- **progress indicators** to track milestones that need to be achieved – at different levels – in order to reduce the risk factors could include the following:
 - women and girls implement measures within two months to reduce exposure at the highest-risk locations and times
 - access to resources (firewood, water, etc.) and services (clinics, schools, etc.) in highest-risk locations/times is changed within six months to locations/times identified by women and girls as safe
 - community groups engage in regular dialogue with police, express their concerns and seek solutions to address sexual violence
 - comprehensive education and training for the police is mandated by regional authorities and implemented throughout the region
 - the police engage in regular dialogue with community representatives to hear concerns about sexual violence against women and girls
 - the police adopt record-keeping policies and practices that meet human rights standards and address concerns of women and girls about reporting incidents of sexual violence
 - the police establish, within six months, regular patrols in highest-risk areas
 - the police take measures, within one year, to process and investigate alleged incidents of sexual violence effectively, promptly, thoroughly and impartially
 - lawmakers take measures, within two years, to adopt new legislation against sexual offenders
 - legislative, administrative and other measures to prevent sexual violence are in place

- **programme indicators**, or outputs corresponding to the activities being conducted, could include the following:
 - number of community groups, involving women and girls, that address sexual violence
 - number of women and girls who participate in a community group
 - number and frequency of meetings community groups have with police
 - number of police personnel receiving education and training on law and policies, and on their responsibilities, related to sexual violence
 - number of public awareness-raising events/media spots and the estimated numbers of people reached.

ANNEX 2: 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*.



CHAPTER 3

OUTLINING THE PROTECTION ARCHITECTURE

Relating to the primary duty bearers

- S** 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.
- S** 3.2. Protection actors must at all times avoid action that undermines the capacity and will of primary duty bearers to fulfil their obligations.
- S** 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.
- G** 3.4. Protection actors should include some form of communication with the relevant authorities in their overall approach.
- G** 3.5. Protection actors should ensure that, whenever feasible, they establish a protection dialogue with armed non-State actors.
- S** 3.6. All protection actors must specify their roles, protection objectives, institutional priorities and means of action.

Interface with UN peace operations and internationally mandated military forces and police services

- 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.

Engaging UN peace operations and internationally mandated military forces and police services

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

Other actors

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

This chapter outlines what can be referred to broadly as the “global protection architecture”, and how humanitarian and human rights actors doing protection work should relate to it, as well as to each other.

The global protection architecture, comprising various actors at national and international level with protection roles and responsibilities, is based on rights and obligations set out in international humanitarian law (IHL), international human rights law (IHRL) and international refugee law (IRL). These rights and obligations must be incorporated in domestic legislation, which frequently expands and enhances the rights agreed upon internationally, and defines responsibilities to enforce them.

While the State bears primary responsibility to protect the people within its jurisdiction (including those beyond its borders), *de facto* authorities or non-State armed groups that exercise government-like functions and control over territory are increasingly expected to respect international human rights norms and standards when their conduct affects the human rights of individuals under their control.¹⁵

All parties to armed conflicts, including organized non-State armed groups who conduct military operations, are also bound by IHL, which imposes protection responsibilities on them for civilians affected and other persons not or no longer directly participating in hostilities.

Various elements of the State apparatus, such as the police and the courts, are responsible for implementing international obligations – by applying and monitoring domestic laws and policies, and ensuring the protection of the population. In cases where the capacity, or the will, of the authorities to ensure the protection of persons under their jurisdiction is limited – or worse still, when the authorities themselves are actively perpetrating violations against the population – such protection mechanisms are likely to be ineffective or inadequate. A response by other actors is then required to help ensure the protection of those at greatest risk. This can take the form of action by other States, multilateral bodies and civil society organizations. As members of the United Nations, and as parties to the Geneva Conventions, States bear protection duties towards persons at risk, even if these persons are outside their jurisdiction. In the Geneva Conventions this is defined as a duty to respect, and to ensure respect for, the legal norms – thus deliberately keeping the focus on the responsibilities of the primary authorities.

A number of other actors are often involved in a protection response. They include local, national and international, legal, security, human rights and humanitarian actors. States have conferred specific protection mandates on a number of international humanitarian and human rights organizations, including the ICRC, OHCHR, the Office of the United Nations High Commissioner for Refugees (UNHCR) and the United Nations Children’s Fund (UNICEF). Their mandates derive from a variety of sources, including international treaties, the Statutes of the International Red Cross and Red Crescent Movement, the UN Charter, resolutions of the UN General Assembly and Security Council, and UN World Conferences. Some actors have been mandated to assume a specific protection role, such as country-specific peacekeeping operations with protection mandates. Within the protection architecture, all these actors bear certain protection responsibilities; State actors, of course, remain the primary duty bearers. It is therefore essential for humanitarian and human rights actors carrying out

¹⁵ IASC, *Policy on Protection in Humanitarian Action*, 14 October 2016. See also Chapter 4 of this document.

protection work to be familiar with the overall global protection architecture and to situate their own particular position within this overall framework, so that their action may be more effective.

The first section of this chapter emphasizes that protection work undertaken by humanitarian and human rights actors must relate to the existing protection architecture, and aim to improve the way it functions – as opposed to replacing it – especially at local and national levels. The second section draws attention to the importance of each actor articulating its objectives and intentions clearly with respect to its role in protection, as this is vital for working effectively with others. This should also help avoid gaps, unnecessary duplication or undermining the efforts of other actors, and thus serve the overall objective of creating a more effective protection response.

The third section underlines the need to understand the role of UN peacekeeping operations and other internationally mandated military and police forces engaged in protection.¹⁶ This section was added to the second edition of *Professional Standards for Protection Work*. The standards and guidelines capture some commonalities between the very diverse views protection actors can have on how to engage with such military and police forces whose mandate may include the protection of civilians.

RELATING TO THE PRIMARY DUTY BEARERS

S

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.

Although any actor involved in protection work is responsible for its own actions, its work does not exist in isolation. Protection actors must understand the roles of the various actors that have an obligation to respond, particularly the roles and responsibilities of primary duty bearers.

Under international law, authorities at all levels of government hold the primary obligation and responsibility to respect, protect and fulfil the rights of persons on their territory or under their jurisdiction.

Authorities include 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. Establishing an interface with these various actors and efforts is therefore critical in ensuring effective protection.

In addition, all State and non-State parties to conflicts have additional responsibilities under IHL. They must take measures to avoid, and in any event to minimize, harm to civilians and ensure that these people have access to goods and services essential to their survival.

¹⁶ Other internationally mandated military and police forces are those operated by an international or regional organization other than the UN but still acting in accordance with a Security Council mandate.

No effort should be spared to remind duty bearers of their responsibilities and make them fulfil their obligations more fully. In the case of duty bearers that are willing to protect, and possess the capacity to do so, the approach is likely to be one of proactive and supportive engagement. Other modes of action, such as persuasion, mobilization, denunciation and substitution, may be preferred with duty bearers who, by their acts of commission or of omission, are responsible for the violation of rights.

Different protection actors may adopt different approaches, depending on the issues to be addressed, and on their unique capacities and mandate, as well as on whether they are in a position to do so. Protection actors should, therefore, 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.

Rather than attempt to replace a weak national protection apparatus, humanitarian and human rights actors doing protection work in armed conflict and other situations of violence should – to the extent feasible – encourage, support and persuade the relevant authorities to assume their obligations more fully. Protection outcomes may often involve supporting the establishment of and/or strengthening national protection systems.

Whatever their approach, protection actors must always avoid any action that could undermine or remove responsibility from the legally bound authorities. They must also take care not to undermine but rather to support and empower well-functioning national protection agencies, such as ombudsmen and other national human rights institutions.



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 by humanitarian actors can take many forms. It may include evacuating the wounded or the sick from a battle zone, ensuring access to essential services (e.g. food, education or housing), or setting up an information campaign on the risks of unexploded munitions for IDPs returning to an area that was previously a battlefield. Any such action can inadvertently reduce the incentive of authorities to assume these responsibilities themselves. Direct substitution should therefore occur only when humanitarian actors deem that there is no immediate prospect of the authorities assuming their responsibilities, and the gravity of the situation of those at risk demands immediate action.

Similarly, independent human rights monitoring and other protection work by human rights actors supports but does not relieve a State of its responsibility to fulfil its obligations vis-à-vis populations affected, including those related to protection and accountability.

Activities based on direct substitution traditionally focus more on the populations at risk. They can include measures to reduce these people's exposure to risk, such as providing temporary identity documents, or measures to mitigate the consequences of exposure, such as providing medical services following a violation. In all these cases, such activities must be understood as temporary in nature, undertaken because of the failures for the formal system, and lasting only until the authorities have the requisite means and will to resume their roles.

Ideally, substitution activities should be accompanied by efforts aimed at building or strengthening the capacities of the authorities and national protection systems to fully discharge their responsibilities to respect, protect and ensure the fulfilment of everyone's rights. This is especially relevant when the authorities are willing but lack the capacity to do so. Total substitution should occur only in extreme circumstances. Even then, protection actors should constantly seek through persuasion and advocacy to encourage the relevant authorities to better fulfil their obligations and 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.

Formal or informal communication with the authorities should be included in the work of protection actors, aiming at encouraging them to respect, protect and fulfil the rights of all.

Formal communication usually takes the form of evidence-based analysis and recommendations, submitted bilaterally to the authorities by protection actors (often mandated) or made public, calling for improved respect for, or changes to, laws and policies – to which a formal response is expected.

Informal communication can take many forms. It may be conducted through indirect and private channels, such as messages conveyed by influential personalities or leaflets that present the activities of an organization in a given country. At the local level, informal communication might accompany protection work aiming to help individuals reduce their exposure to threats – usually through assistance or services that empower them to claim their rights and/or to cope better.

In all such scenarios, the need for better protection of those at risk, and the responsibility of the primary duty bearer to provide it, should remain central. Transparency with regard to the activities, mandate and/or mission statement of each actor is also vital when establishing communication with the authorities.

Maintaining dialogue with the relevant authorities is even more essential when working in substitution for the formal authorities. The content of the dialogue will be determined by the causes of the protection shortfalls on the part of the primary duty bearers – for instance, a lack of capacity, a lack of will to protect or deliberate violations perpetrated by the authorities. Acting in substitution for the authorities without any form of communication with them, and without their consent, may not create conditions conducive to the sustainability of an actor's presence and may also create additional risks for the beneficiaries of its protection activities.

Some actors may choose not to communicate on protection issues with the authorities, for reasons of security and in order to maintain access for delivery of humanitarian relief, particularly when protection work is not their primary activity. In the long run, however, such a choice can give rise to suspicions among authorities, and to serious misunderstandings with them, that may become increasingly difficult to allay or correct.

Communication with the authorities is not advisable in certain rare cases, such as when a protection action is carried out against the will of the authorities, for individuals or communities who would be at greater risk if the authorities were to learn of this action.

Leaders at the community level may have some varying influence over the dynamics in a given context, even in relation to implementation of certain policies. Such leaders may occupy formal positions; alternatively, their roles may be traditional or informal in character. Their roles may contribute positively to a protective environment or they may be exploitative and abusive. In some contexts, local leaders may in effect become gate-keepers of information and claim to make decisions on behalf of the community as a whole. It is important to understand the relationships between community leaders and formal authorities and between community leaders and the population affected. Engagement with such leaders is likely to be unavoidable and must be carefully managed.

6

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 to achieve protection outcomes for the population, it is often essential for protection actors to establish a dialogue in the field with all key stakeholders. These include armed non-State actors, such as militias, private security companies and rebel or guerrilla movements. They may all have responsibilities under IHL and engaging with them does not affect the legal status of parties to armed conflict. Their actions and *modus operandi* can contribute to increasing or reducing the incidence of violence inflicted on the population. Furthermore, they can often facilitate or impede access to humanitarian assistance in areas they control or in which they operate.

Engaging with armed non-State actors involves a detailed examination of the nature of violations, threats and abuses and their impact on people's lives. Humanitarian and human rights organizations must also seek to understand the motivations and incentives of armed groups, as well as their strategies, in order to influence their behaviour. This can be particularly challenging when facing groups pursuing both political and criminal objectives. The decision on whom to engage with strategically, and how and by whom, should be based on a good understanding and sound analysis of the context and of the relevance/importance of the various key armed non-State actors.

Protection actors who engage in a dialogue with armed non-State actors should remind them of their obligations. The measures they could take to reduce the impact of conflict and other situations of violence on the civilian population should be presented to them and discussed. In order to establish the proper conditions for such a dialogue on protection concerns, implementation of adequate confidence-building measures will be necessary. When dealing with certain groups operating transnationally, protection actors should ensure that their engagement is consistent throughout various geographical regions.

Not all protection actors will choose to engage in such a dialogue; some may prefer to voice their concerns through public communication, or through humanitarian or other stakeholders who have the necessary contacts. Engaging in any form of dialogue with armed non-State actors can indeed be difficult owing to security considerations for their representatives and for the protection actors' personnel in the field. Counter-terrorism measures may pose additional challenges, as they seek to prevent engagement with proscribed groups. Furthermore, any such interaction must be conducted in a manner that does not put populations affected at greater risk and that does not undermine the ability of humanitarian and human rights actors to operate, and to be seen to operate, in accordance with relevant principles.

Interaction with armed non-State actors should be undertaken in close consultation with senior protection and/or management staff, to ensure the coherence of messages. Staff interacting with armed non-State actors should be carefully selected, and never forced to engage against their will, especially if they feel threatened or uncomfortable. When relying on national staff to engage in such negotiations (in particular in situations of remote management), organizations must ensure that they provide adequate security, financial and managerial support. Organizations must also carefully evaluate the potential risk transfer, and put in place protective and mitigatory measures, when relying on community leaders who engage with armed groups on their behalf.

In all instances, such interaction should be undertaken with due consideration to how and by whom it is conducted, and to ensuring respect for the “do no harm” principle, which includes ensuring the safety of staff.

§

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

Cooperation between the various humanitarian and human rights actors working on protection issues requires clarity as to their respective objectives and intended protection roles, and the responsibilities that each can realistically be expected to assume in varying circumstances. Such transparency greatly facilitates interaction and complementarity, and clarifies their relationship with the existing international protection architecture.

For a protection actor with a formal mandate, a mission statement serves to articulate its overall mandate and objectives in a coherent manner. It can outline the specific protection elements on which the actor is authorized and expected to act, as well as clarify any additional elements to which the actor intends to respond.

For actors who only occasionally engage in protection activities, developing policies and corresponding field guidelines can be another way of specifying their roles and means of action, without having to revise their mission statement.

In any given operational context, all protection actors (mandated or otherwise) 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. Institutional clarity on general objectives and the type of activities to be carried out is also necessary for effective communication with individuals at risk – for example, to get them to agree to provide information or to participate in a workshop or training activity.

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

UN PEACE OPERATIONS¹⁷

UN peace operations (UNPOs) are required to respect and protect civilians while conducting their operations, in accordance with IHRL and, where applicable, IHL (in particular as reflected in Article 1 common to the 1949 Geneva Conventions).¹⁸

Beyond these general obligations, in 2000, the *Report of the Panel on United Nations Peace Operations* (the Brahimi Report) underlined that “peacekeepers – troops or police – who witness violence against civilians should be presumed to be authorized to stop it, within their means, in support of basic United Nations principles”.¹⁹

Furthermore, in 2015, the High-Level Independent Panel on Peace Operations²⁰ called the protection of civilians “a moral responsibility for the United Nations” and noted that “[w]herever UN peace operations are deployed with a protection of civilians mandate, they must do everything in their power to protect civilians under threat”.²¹ It also highlighted the “primacy of politics” in addressing and resolving conflict, including the importance of dialogue “to minimize the suffering of civilians, and promote respect by all actors for the human rights of the local people”.²²

In addition, the Secretary-General’s 2015 report on the future of peace operations noted that “[a]ll United Nations peace operations today have the obligation to advocate the protection of civilians”.²³

¹⁷ The term “UN, peace operations” encompasses both **peacekeeping operations** and **special political missions** (see: *United Nations Peacekeeping Operations, Principles and Guidelines*, UNDPKO/DFS, New York, 2008). Peacekeeping operations include “traditional peacekeeping”, preserving the peace where fighting has been halted; “peace enforcement” with coercive measures; and “peace building” efforts to reduce the risk of lapsing or relapsing into conflict. More and more, recent UNPOs mix these various aspects.

¹⁸ When deployed in situations of armed conflict UN peace operations and internationally mandated military and police forces are bound at all times by Article 1 common to the Geneva Conventions to take all feasible measures aimed to induce the belligerents to comply with IHL. When drawn into hostilities, these forces are obliged to respect IHL and IHRL (taking into account the sensitive issue of the extraterritorial application of IHRL) while conducting their military operations.

¹⁹ UN, *Report of the Panel on United Nations Peace Operations (the Brahimi Report)*, [A/55/305-S/2000/809], 21 August 2000

²⁰ UN, *Uniting our Strengths for Peace – Politics, Partnership and People*, Report of the High-Level Independent Panel on Peace Operations [A/70/95, S/2015/446], 17 June 2015.

²¹ *Ibid.* p. 22.

²² *Ibid.* p. 26.

²³ 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, para 17.

As a result, 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**. Security Council resolutions also usually underline that, where UN missions are engaged in hostilities, they have obligations under IHL, and specifically call upon these missions to mitigate risk to civilians in the conduct of military operations.

A “protection of civilians” (PoC) mandate is generally phrased like this:

The UN Security Council,

(...) acting under Chapter VII of the Charter of the United Nations

(...) authorizes [name of peacekeeping operation] to use all necessary means, within the limits of its capabilities and areas of deployment, to protect civilians under threat of physical violence, without prejudice to the responsibility of the host Government.

The mandate may also include a specific focus on particular themes or on vulnerable categories of population.

In 2017, ten UN peacekeeping missions, accounting for more than 90% of all uniformed and civilian personnel in UN peacekeeping, had such PoC mandates. The Security Council has further articulated the role of peacekeeping operations through its country-specific resolutions and thematic resolutions on the protection of civilians.²⁴

While UN special political missions usually do not have explicit PoC mandates, given their lack of military forces,²⁵ the secretary-general has stated, as noted above, that all UN peace operations have an obligation to advocate the protection of civilians. UN Policy also reaffirms that all mission personnel have a responsibility to ensure that human rights are promoted, respected and protected through and within their operations in the field.

Most UN peace operations also have mandates and tools that are relevant to protection. For example, most UN peace operations include human rights components that serve as mission actors, while also representing OHCHR and its human rights protection mandate. They generally monitor, report on and promote human rights and often work to strengthen national institutions involved in law enforcement and protection, with a view to enhancing respect for the rule of law; this, in turn, generates protection outcomes. In addition, UN peace operations and humanitarian organizations often undertake complementary protection activities, such as child protection and preventing and responding to gender-based violence. UN peace operations also frequently lead the implementation of the Security Council-mandated Monitoring, Analysis and Reporting Arrangements (MARA) on conflict-related sexual violence, and of the Monitoring and Reporting Mechanism (MRM) on grave violations of children’s rights in situations of armed conflict.

²⁴ Such as [Security Council Resolution 1894 \[on the protection of civilians in armed conflict\]](#), 11 November 2009, S/RES/1894. Relevant Security Council language can be found in the UN, [Aide-Memoire for the consideration of issues pertaining to the protection of civilians in armed conflict](#), OCHA, 2014. Further information is available in UN, [Security Council Norms and Practice on the Protection of Civilians in Armed Conflict](#), OCHA, 2014.

²⁵ However, some special political missions, such as UNAMA (Afghanistan), have a mandate to coordinate efforts to ensure the protection of civilians. See [Security Council Resolution 2210](#), 16 March 2015, S/RES/2210.

Finally, it is important to note that the UN Human Rights Due Diligence Policy dictates that the UN will not provide support to national security forces when there are substantial grounds for believing that there is a real risk of such forces committing grave violations of IHL, IHRL or IRL and where the relevant authorities fail to take the necessary corrective or mitigatory measures.²⁶

UN PEACEKEEPING AND THE IMPLEMENTATION OF POC MANDATES

In UN peacekeeping operations, PoC is a “whole of mission” responsibility (i.e. involving the military, police and civilian components of a mission) and is implemented on three different/complementary levels, or “tiers”, as defined by the UN Department of Peacekeeping Operations:

- Tier 1: Protection through dialogue and engagement
- Tier 2: Provision of physical protection
- Tier 3: Establishment of a protective environment

Implementing such mandates can therefore include the show or use of force (tier 2) to protect civilians under threat of physical violence, advocacy by civilian and uniformed actors to deter such violence (tier 1) or, longer-term, more structural efforts, such as training, mentoring or supporting national military and security staff (tier 3). The contribution of other mandated tasks, such as in the areas of security sector reform or child protection, may also fall into the category of tier 3. Missions are required to design a “mission-wide protection strategy” generally structured on these three tiers, and to report on its implementation.

The implementation of the PoC mandate may also include a range of activities classifiable into the three tiers, such as:

- conducting medical evacuations
- taking measures to ensure security in and around IDP camps
- ensuring presence in areas where populations are most at risk, as a preventive and early-warning strategy
- contributing to improving the security and rule-of-law environment and making it conducive to the safe, voluntary and dignified return of IDPs and refugees.

OTHER INTERNATIONALLY MANDATED MILITARY FORCES AND POLICE DEPLOYMENTS

The protection of civilians has now become a major issue not only in UN peace operations but also in the context of other internationally mandated deployment of military forces and police services.²⁷

²⁶ UN, *Human Rights Due Diligence Policy on UN Support to non-UN Security Forces* [A/67/775-S/2013/110], 5 March 2013.

²⁷ Forces that receive a mandate from the UN Security Council but operate outside the UN system, usually under a regional organization (African Union, ECOWAS, NATO, etc.) and sometimes under a State.

Over the past decade, UN Security Council mandates provided to some international forces operating outside the UN system have 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. Meanwhile, stabilization approaches adopted by individual States and a few multilateral organizations have evolved into a policy framework for some international military interventions in fragile and conflict-affected States. Several regional organizations have clarified their PoC ambitions by adopting PoC policies or guidelines. Some States have done so, as well.

Stabilization is generally understood as both a short-term and a long-term strategy, involving both military and civilian capacities, aimed at improving security and stability. While the protection of civilians is not always the priority or an explicit objective of stabilization strategies, such strategies may seek to reduce violence and instability.



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.

UN peace operations have a variety of roles and responsibilities that support protection, ranging from their unique peacekeeping capability to enhance physical protection of civilians by projecting or using force, to activities such as monitoring and reporting or advocacy undertaken by all peace operations (i.e. both peacekeeping and political) that may overlap with the activities of protection actors.

It is worth underlining that the UN Department of Peacekeeping Operations, together with troop- and police-contributing countries, has clarified the potential roles and responsibilities of the different components of a peacekeeping mission with regard to the protection of civilians against the threat of violence: that is, the specific responsibilities of the civilian leadership of the mission, the military command of the force, and the role of police- and troop-contributing countries. Missions with explicit PoC mandates are now required to establish protection strategies, which should be developed in consultation with the populations at risk, as well as with humanitarian and human rights organizations involved in protection work.

Protection actors must understand the different roles, responsibilities and mandate of all peace operations in relation to protection. They should familiarize themselves with the structure, components and coordination mechanisms, and with the relevant documents and policies, of UN peace operations and internationally mandated military forces and police services with regard to the protection of civilians – both at the general/policy level (the UN Human Rights Due Diligence Policy, the UN secretary-general's bulletin on sexual exploitation and abuse²⁸) and in-country (structure of the mission, rules of engagement, PoC strategy, role of troop-contributing countries). The depth of understanding that is required may vary, depending on the types of issues a protection actor plans to address, the activities that may be undertaken and their relation to the presence of a peace operation or military force.

²⁸ UN, *Special Measures for Protection from Sexual Exploitation and Sexual Abuse*, Secretary-General's Bulletin, ST/SGB/2003/13, UNSG, 9 October 2003.

ENGAGING UN PEACE OPERATIONS AND INTERNATIONALLY MANDATED MILITARY FORCES AND POLICE SERVICES

Many humanitarian and human rights actors have long expressed concerns about the impact close association with UN peace operations and multinational forces may have on their ability to operate in an independent and impartial manner and to be perceived as doing so. Their principal concern is that, particularly in conflict situations, their access and security may be undermined if they are perceived by belligerents or segments of the population as being aligned with the political objectives of such missions. This becomes especially acute where UN peacekeepers and forces have a peace enforcement posture or engage in offensive military operations. In such high-risk contexts, it can be problematic if at the same time the UN Humanitarian Coordinator is also a deputy of the Special Representative of the Secretary-General and therefore structurally part of the UN peace operation. This situation is especially challenging for humanitarian organizations that rely on their neutrality to gain access to the population and to all armed actors.

However, humanitarian actors have also long recognized that humanitarian action alone cannot protect civilians from the effects of armed conflict. UN peacekeeping operations have a unique capacity to enhance the physical protection of a civilian population in a way that humanitarian actors cannot. They may also be able to contribute to the creation of a security environment conducive to civilian-led provision of humanitarian assistance. UN peace operations, supported by their human rights component, can also support protection through their engagement with the relevant authorities.

Whereas UN peace operations' contributions may be highly valued by many humanitarian and human rights organizations on the ground, in some instances they have been seen as dangerously blurring the roles and responsibilities of different sets of actors, and inadvertently jeopardizing humanitarian access to populations affected.

Thus dialogue, and interaction as appropriate, between humanitarian organizations and UN peace operations is essential for improving and strengthening the roles and activities of each, and the overall protection response; and also for preventing the blurring of their roles and responsibilities, including in the eyes of local authorities or communities.

In this respect, the UN's Policy on Integrated Assessment and Planning (IAP) of April 2013 recognizes the need for humanitarian action to remain distinct and separate from the political objectives of UN missions, while maintaining dialogue and engagement:

While humanitarian action can support peace consolidation, its main purpose remains to address life-saving needs and alleviate suffering. Accordingly, most humanitarian interventions are likely to remain outside the scope of integration, which can, at times, challenge the ability of UN humanitarian actors to deliver according to humanitarian principles. Depending on the context, certain activities related to protection of civilians, return and reintegration and early recovery may be included in the UN's integrated strategic approach. Therefore, in all cases, shared analysis and coordination among humanitarian and peace consolidation actors should be supported in UN integration arrangements.²⁹

²⁹ UN, *Policy on Integrated Assessment and Planning*, UNDG, 9 April 2013, para. 9.

In relation to other internationally mandated deployment of military and police forces, similar concerns apply and are often exacerbated. These forces are usually actively involved in hostilities against some local forces. Interacting with them can therefore be very complex. It is, however, also important to recognize their potential for contributing to the protection of civilians, and to seek some form of engagement with them to promote protection outcomes, while taking care to avoid confusion of roles and responsibilities.

When UN peacekeeping operations or internationally mandated military forces fight alongside domestic forces in situations of armed conflict, or provide them support for their military operations, they must take all feasible steps to ensure that the parties, particular those they are partnering, comply with the relevant IHL obligations.³⁰ Hence, some degree of dialogue and interaction between humanitarian actors and these forces will be important for securing positive protection outcomes, including fulfilment of the latter's obligations and the obligations of their local partners to respect and protect civilians during their military operations.

The extent to which protection actors and UN peace operations and internationally mandated military forces and police services engage in dialogue and interact will depend on their mandate and the context.

Within the framework of peacekeeping operations, UN human rights actors and UN military and police components interact regularly, and in ways that are defined by relevant policies; however, continuous efforts to exchange information and coordinate relevant work are also required. Effective forms of cooperation between UN military and police components and human rights actors to enhance protection have included identifying protection hotspots for the purposes of military deployment and patrolling, coordinated advocacy with national counterparts and human rights monitoring enhanced by appropriate information exchange.

Whatever the context, dialogue and interaction must take place in a manner that neither undermines adherence to the humanitarian principles of independence and impartiality nor exposes 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.

Protection actors should seek and promote a contextual common understanding of the roles and responsibilities of the various actors engaged in enhancing protection in the field.³¹

Protection actors should therefore establish relevant protocols and networks with UN peace operations, and keep communication channels with them open at all times. Proactive engagement of UN military and police components, alongside the mission's civilian component, should facilitate safe sharing of non-confidential information and analysis of protection risks. This will inform the general PoC analysis of the mission and the prioritization of the response. It will also help identify areas of complementarity. Dialogue is indispensable in order to ensure adequate coordination on particular subjects, such as child protection, DDR (disarmament, demobilization and reintegration), prevention of and response to sexual violence, detention and correctional facilities, and humanitarian demining.

³⁰ See also the [Human Rights Due Diligence Policy on UN Support to non-UN Security Forces](#), [A/67/775-S/2013/110], 5 March 2013.

³¹ For further guidance, see, for instance, [Global Protection Cluster, Diagnostic Tool and Guidance on the Interaction between field Protection Clusters and UN Missions, 2013](#).

Important issues that may need to be addressed include:

- the need to engage communities in a safe and respectful manner
- preserving the distinction between neutral and impartial humanitarian action and peace operations
- the harm that may be caused to the civilian population by the uniformed or civilian personnel of the peace operation itself, during the conduct of hostilities or the use of force or in other circumstances
- the measures the mission may be able to take to prevent harm caused by other forces, or to mitigate threats and
- the support provided by the mission to local forces, the contribution of the mission to security sector reform, and possible conflicts or synergies with the efforts of humanitarian agencies.

UN peace operations may also constitute, in certain circumstances, an indirect channel for advocacy efforts with senior representatives of the local government and armed forces officials.

In certain circumstances, it may also be necessary to address some of the issues documented at higher levels, with the UN Secretariat in New York and Geneva, as well as with the military and political authorities in the country of origin of some of the military and/or police components (troop- or police-contributing countries).

Some non-UN protection actors, independent of the UN system, have their own procedures for engaging with UN peace operations. Other humanitarian actors may engage them through humanitarian coordination mechanisms, such as the in-country protection cluster, or via the UN Office for the Coordination of Humanitarian Affairs (OCHA) or national networks.



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.

Notwithstanding the importance of a distinct humanitarian response, a consistent and constructive dialogue with internationally mandated military forces and police services should involve promotion and respect for IHRL and, where applicable, IHL and IRL by such actors; and, where appropriate, other protection concerns and trends, as well. In this respect, internationally mandated military forces and police services working with domestic forces have the obligation to ensure, as far as possible, that these forces respect their obligations under IHL.

Therefore, humanitarian and human rights actors may approach internationally mandated forces on various issues, such as: the precautionary measures they take when engaged in hostilities; the displacement of people; arrest and detention measures; the promotion of proper procedures for the management of mortal remains, including transfer and handover of bodies, and for the management of post-mortem data to prevent disappearances.

Information exchange may relate to the sharing of non-confidential information on general trends and risks facing civilian populations. It requires proper procedures and agreed communication channels. It must be done with full respect for the applicable standards on data management (see Chapter 6). It will require trust and a solid relationship, both of which have to be built up gradually.

A minimum level of dialogue and information sharing is critical to secure improved protection outcomes. All this must be done in a manner that does not pose further risks to civilians (see Standard 3.10). Furthermore, as there is an inherent risk of data being used to advance a security agenda, protection actors must be particularly attentive not to undermine the ability of humanitarian actors to operate, and to be perceived as operating, according to their principles. Protection actors, collectively or individually, should develop a specific review mechanism to avoid these risks.

The interaction between protection actors and internationally mandated military forces and police services may be conducted bilaterally by individual humanitarian organizations or as a joint effort via humanitarian coordination mechanisms, such as the in-country protection cluster or through OCHA.



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.³²

Whether or not they are engaged in the conduct of hostilities or the use of force, these forces – because of their very nature – may not be seen as neutral and impartial by large sectors of the population and by some of the parties engaged in the fighting. UN humanitarian actors will have established contextual protocols that guide their engagement with UN peace operations (see text box above). However, non-UN humanitarian actors may have different views on how appropriate it is for them to openly engage with UN missions, especially with their military and police components. Such actors will need to determine whether their engagement conveys an image of partiality and, if so, whether this could hinder their acceptance in communities or with armed actors and increase the security risk to the humanitarian community.

The risks may well evolve over time. The more tense and conflict-prone the environment is, the greater the risks become. All protection actors must therefore regularly reassess and adapt their engagement in light of these risks and the changing environment.

OTHER ACTORS



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

Actors with responsibilities in other sectors may also play important roles in helping to enhance protection. These may include domestic and international actors in political, judicial and economic realms. While their principles, policies and practices, competencies, resources and priorities are likely to be very different from those of humanitarian and human rights actors, they can play important roles, in particular, to help create an environment conducive to protection and compliance with international law.

³² See also Standard 5.2.

For example, actors that specialize in strengthening the rule of law and security sector reform, or in building long-term institutional capacity and a legislative underpinning for human rights, can play a critical role in helping to reinforce the obligations of primary duty bearers and provide practical support and technical expertise to bring about sustained changes in policy and practice.

Through their policies and programmes, economic actors – for example, those responsible for domestic development policy or international development assistance – may help create an environment conducive to protection, or do the opposite. They might also be in a position to influence primary duty bearers to enhance the protection of vulnerable populations.

Protection actors must therefore take into account the roles, responsibilities and expertise of other actors when planning and implementing activities, with a view to maximizing complementarity while also respecting the principles of humanitarian action.

Assessing which of these actors is best positioned to have a certain desired impact also requires some degree of interaction, and a will to identify and foster positive synergies. But it is critically important that protection actors, while undertaking these activities, maintain their adherence to the humanitarian principles that underpin humanitarian action.

ANNEX TO CHAPTER 3

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.



CHAPTER 4

**BUILDING
ON THE LEGAL
BASE OF
PROTECTION**

Knowing the legal framework

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

Referring to the law with consistency and impartiality

- ④ 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.

Maintaining coherence and accuracy

- ④ 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.

Referring to relevant regional and domestic laws and other relevant standards

- ④ 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.

Upholding existing legal standards

- ④ 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.

This chapter emphasizes that for humanitarian and human rights actors involved in the field of protection, the capacity to understand and refer to applicable law is often essential. Protection is indeed rooted in respect for the rights of persons, and in the obligations of those in a position of authority, as defined in various instruments of IHL, IHRL and IRL, as well as in domestic legislation. To remind the authorities of their obligations, protection actors must first know the applicable laws and standards, and the jurisprudence, as well as the policies for implementing them. This helps protection actors, not only in their operational programming but also when they seek to address accountability issues such as impunity, to urge the authorities to investigate and prosecute perpetrators of violations of IHL and IHRL, and provide effective remedies and prevent recurrence.

KNOWING THE LEGAL FRAMEWORK



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

There are many international standards (treaties, customary law, soft law) that require States and other actors to protect individuals or communities in armed conflict and other situations of violence. Some are specific to certain categories of person, such as refugees, children, women, persons with disabilities, detainees, IDPs, migrant workers, persons belonging to national, ethnic, religious or linguistic minorities. Some concern specific situations – such as IHL treaties (including the four 1949 Geneva Conventions and their 1977 Additional Protocols), which only govern issues related to armed conflict – or specific violations of international norms, like the 1948 Convention on the Prevention and Punishment of the Crime of Genocide. Others concern weapons of specific kinds, such as the Anti-Personnel Mine Ban Convention, and the various Protocols to the 1980 Convention on Certain Conventional Weapons. Further prohibitions and corresponding obligations for individuals flow from international criminal law, with which protection actors should be generally familiar even if they choose not to actively promote its implementation.

While it is understandable that many protection actors may not know, or need to know, the details of all sets of laws, they must nevertheless know which legal frameworks apply to them and to the context in which they are working. Consequently, understanding the essence of IHL, IHRL and IRL (see box below), and being able to understand how they complement each other, is a requirement for all protection staff when planning and implementing protection activities.

Staff working on protection issues must therefore have the required knowledge and understanding (if necessary, by receiving appropriate training) of the basic principles and standards of each body of international law. In addition, protection actors must be clear as to who falls within the personal, temporal and territorial scope of application of each of these bodies of law.

Universal protection norms are to be found in the sets of laws outlined in the box below.

ESSENTIAL FEATURES OF IHL, IHRL AND IRL³³

Universal legal norms ensuring respect and protection for individuals, in particular their protection from the effects of violence and abuse, can be found in three bodies of law:

- international humanitarian law (IHL), or the law of armed conflict
- international human rights law (IHRL) and
- international refugee law (IRL).

These bodies of law create binding international obligations. National authorities are required to ensure that these sets of laws are fully incorporated in domestic legislation and regulations.

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. It recognizes the importance of relief and protection activities by the ICRC and other impartial humanitarian organizations. The humanitarian principles of humanity, impartiality, neutrality and independence, while not sharing the status of legal norms in their entirety, are widely recognized by States, international organizations and international jurisprudence, and can play a significant role in protection dialogue.

IHRL lays down obligations, primarily for States, to respect, protect and fulfil the human rights and fundamental freedoms of individuals and groups in their territory or within their jurisdiction. The obligation to respect means that States and other duty bearers must refrain from interfering with or curtailing people's enjoyment of their human rights. The obligation to protect requires States to protect individuals against threats emanating from armed groups, private individuals or natural hazards. The obligation to fulfil means that States must take positive action to facilitate the enjoyment of basic human rights. IHRL is applicable in all circumstances, including armed conflict. There are, however, exceptional circumstances – such as public emergencies – in which a limited set of rights may be derogated from, but this is subject to stringent conditions.

Both bodies of law (**IHL** and **IHRL**) comprise a large number of treaties and customary rules that came into being at different points in time. Not all States are parties to all treaties. However, all existing States are party to the Geneva Conventions, which are the main instruments of IHL. And all States have ratified at least one of the core international human rights conventions. Regional human rights treaties often reaffirm or even reinforce the obligations set out by international treaties. In many cases, they may be seen as particularly authoritative by local actors.

³³ For more details, see [IASC Protection Policy](#), 2016, Annex I (“Normative framework”).

Customary international law – that is, rules followed in State practice with the understanding that they represent a legal obligation or authorization – is applicable irrespective of the existence of a treaty provision that contains the norm and whether or not a State has ratified any treaty provision that contains the customary norm. That said, where the requirements for the formation of customary international law are met, the norms contained in international treaties may also reflect customary international law. In this regard, the norms contained in the Geneva Conventions of 1949 have attained the status of customary law. Most of the norms laid down in the Universal Declaration of Human Rights, and some of those laid down in Protocols I and II of 8 June 1977 additional to the Geneva Conventions (1977 Additional Protocols), have also attained the status of customary international law.³⁴

These treaties and customary law are complemented by numerous internationally recognized standards (“soft law”), some of them adopted by political bodies such as the UN General Assembly. These instruments are not formally binding as such but they may reflect rules of customary international law or constitute an authoritative interpretation of existing treaty obligations when they are backed by an international consensus. Even where this is not the case, invoking international soft-law standards may strengthen efforts to persuade authorities to assume their responsibilities and provide a basis for action.

A major distinction to be noted between **IHL** and **IHRL** is that the latter provides rights to the individual to be protected, respected and fulfilled by the State and possibly, to some extent, by non-State actors, whereas IHL is formulated in terms of obligations of the parties to an armed conflict (be they States or armed non-State actors).

In times of armed conflict, both bodies of law are applicable, and each informs interpretation of the other. In practice, States may challenge the applicability of IHL or IHRL without good reason. They may wrongly argue that IHL does not apply to operations against “terrorist” or “criminal” groups, even where the organization of such groups and the intensity of the violence in confrontations with them meet the threshold of non-international armed conflict. Or they might wrongly claim that a situation that is actually one of law enforcement is governed by IHL and human rights standards applicable to armed conflict, and their more permissive rules on crucial issues such as the use of lethal force.

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, not enjoying its protection, and is applicable both in conflict and in peacetime. The 1951 Convention relating to the Status of Refugees and its 1967 Protocol are the key legal instruments defining refugees and their rights, and the legal obligations of States. While the Convention’s definition of “refugee” is restricted to persons suffering, or at risk of, persecution on grounds of race, religion, nationality, political opinion or because of their affiliation to a particular social group, other regional instruments and elements of customary law enlarge the definition to persons fleeing armed conflict or other situations of violence.

³⁴ Olivier De Schutter, *International Human Rights Law: Cases, Materials, Commentary*, Cambridge University Press, 2010, p. 5: “The growing consensus is that most, if not all, of the rights enumerated in the Universal Declaration of Human Rights have acquired a customary status in international law.”

REFERRING TO THE LAW WITH CONSISTENCY AND IMPARTIALITY

S

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. Under IHL, all parties to a conflict have obligations and they should all be reminded of them, particularly if they do not fulfil them.

IHL binds not only States but also organized armed non-State actors as parties to armed conflict. Protection actors must therefore engage both State and non-State armed actors on their obligations, while recognizing that there might be practical differences when it comes to the implementation capabilities of the various parties.

Regarding other legal frameworks, it is important to distinguish when they place obligations on the State that are different from those placed on organized armed non-State actors involved in a conflict or in other situations of violence. For instance, IHRL imposes obligations primarily on State authorities. However, *de facto* authorities or non-State armed groups that exercise government-like functions and control over territory are increasingly expected to respect international human rights norms and standards when their conduct affects the human rights of individuals under their control.³⁵

Defending the rights of communities or individuals affected must not be seen by others as an act of partiality favouring one of the parties to the conflict, since rights are universal by nature.

This standard – 4.2. – implies that a protection actor should take a comprehensive approach to analysing the effects on the population of the actions, or the lack of action, of the various perpetrators or parties to the conflict, taking account of all their obligations. In light of this analysis, the protection actor might decide to concentrate efforts on a particular group at risk of repeated violations or abuses by one of the parties involved in the violence, on violations of a particular type or gravity or on a specific region in the larger conflict area. In pursuing this choice, it has to ensure that it is not implicitly weakening the protection available to other rights-holders, either by denying them recognition or by giving a false sense of legitimacy to other parties committing abuses.

³⁵ IASC, *Policy on Protection in Humanitarian Action*, IASC, 2016.

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.

Whenever specific action is envisaged to persuade authorities to assume their responsibilities, the protection actor involved should understand the applicable legal frameworks and know the norms to be quoted. This does not mean that a protection actor must always expressly base its action on the applicable legal frameworks. What it means instead is that 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. Specific issues – such as the rights of children, racial discrimination, the right to adequate housing, obligations pertaining to occupied territory, conditions of detention in prisons, access to justice – require more detailed reference to the applicable laws and standards. Accuracy is essential both when referring to a specific case and when describing a pattern of violations and abuse, and the related responsibilities and obligations of the parties concerned.

Protection actors must be familiar with national and international counter-terrorism laws and the measures applicable in a given context. They must understand their interplay with IHL, IHRL and IRL and how they augment protection concerns or pose an obstacle to principled humanitarian action (see box below).

Different protection actors will regularly use different wording to describe the same concerns, because their primary normative frames of reference might be different. Coherence and accuracy serve both to reinforce credibility and to help avoid creating confusion or even contradictions when addressing the authorities. When making reference to international law, be it treaty or customary law, efforts should also be made to ensure accuracy and consistency by consulting with other protection actors working on the same issue. This helps avoid the risk of confusion and contradiction, which can be particularly damaging when several protection actors speak inconsistently or incorrectly about what they consider to be the laws and standards that apply. While coherence among the different protection actors will mutually reinforce their action and give greater emphasis to the obligations that the authorities must assume, any incoherence will undermine this goal and is likely to be seized upon by the authorities to discredit the authors.

A certain level of consultation is therefore recommended among protection actors that are addressing the authorities on similar patterns of violations or abuse. This is particularly the case for organizations with an international mandate or that have developed widely recognized expertise in some branches or aspects of the law, such as the ICRC in IHL, OHCHR in IHRL or UNHCR in IRL.

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.

Domestic law, relevant standards, and traditions are essential elements of an environment that can foster or reduce the likelihood of abuse in a given society. When addressing local authorities and communities, protection actors may seek to draw parallels between these laws, relevant standards, and traditions and IHL and IHRL. This can serve to emphasize the universal relevance of applicable international legal frameworks and norms.

Domestic laws, in particular constitutional provisions, often implement or complement international law, thereby reinforcing overall protection for people against violations or abuses. The general population and the authorities are usually more familiar with them, and often think of them as having greater normative force. It is therefore important to take them into account when seeking to persuade the authorities to assume their responsibilities.

A number of other relevant standards or sources of law may also exist and can be referred to, if they are consistent with international law or accepted international standards.

These include frameworks of professional ethics (for medical or legal professionals, journalists, academic researchers, etc.). These may protect specific persons with whom protection actors are interacting, and may also endow humanitarian workers (medical professionals, for instance) with certain rights and obligations. For example, codes of medical ethics assure the confidentiality of communications between patients and medical personnel, and protect medical records.

Public declarations made by parties to a conflict to underscore their commitment to comply with their obligations under international and local law, or even to abide by more stringent rules, are also important sources of reference that may be used to increase the protection of people at risk.

These may include provisions inserted in ceasefire and peace agreements concluded by the parties, agreements signed with the UN (“Action Plans”, for instance) or unilateral declarations, such as Geneva Call’s Deeds of Commitments. Political manifestos, codes of conduct³⁶ and orders issued by senior leaders and commanders might also contain relevant protection commitments.

However, national laws and other normative frameworks should only be invoked alongside applicable international law to the extent that they do not contradict or undermine it. Protection actors should be careful not to invoke local standards without first thoroughly assessing their compatibility with different bodies of international law. They

36 See, for instance, Geneva Call’s online [Directory of Armed Non-State Actor Humanitarian Commitments](#).

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. Protection actors should always be prepared to point out that national law cannot be used as an excuse for failing to comply with international obligations.

Protection actors are therefore well advised to invest energy in assessing those domestic laws, standards and traditions relevant and applicable to their work. This often means recruiting or contracting national staff who have an understanding of the legal framework at national and regional levels.

TRADITIONAL, SOCIAL, RELIGIOUS AND CULTURAL NORMS³⁷

The behaviour of people affected and that of duty bearers – national authorities, State and non-State parties to a conflict, and other actors – may be influenced or driven mainly by ideas, beliefs or policies derived from traditional, social, religious or cultural norms rather than by their obligations under international law.

These norms may, to some degree, be consistent with IHL and IHRL and, therefore, have a positive protective effect. For example, in many societies, the idea of a “warrior” is closely linked to the ideals of honourable and ethical conduct on and off the battlefield. Some cultural norms consider involving children in armed conflict to be taboo, and others make a distinction between people who participate in fighting and those who do not and must therefore be protected. Social, cultural and religious norms may recognize entitlements to community resources for people who are displaced from their homes or who have lost the heads of their households. Understanding these norms and their contribution (or potential for contributing) to protection outcomes can be extremely complex and require expert local socio-cultural knowledge.

A society that has been wrecked by war, or one that is suffering the effects of repeated crises and pressure on scarce resources, may see its traditional norms and values come under pressure, particularly when communities are displaced and scattered from their traditional homes and lands, and when traditional leadership is under strain. In addition, some traditional norms may be abusive or harmful rather than protective. For example, beliefs about the role of girls and women in society may result in relying on harmful coping mechanisms, such as forced marriage or unwillingness to challenge gender-based violence. Traditions associated with communal conflict may encourage retaliation for attacks and looting of property.

This means that when seeking to enhance compliance with IHL and IHRL, humanitarian and human rights actors should be mindful of the broader scope of norms that affect behaviour during crises. Traditional, social and cultural norms may not be used as justification for the violation of international law. However, familiarity with the traditions, norms and rules of the society affected by conflict or disaster can open up opportunities to persuade a variety of actors to change their abusive behaviour – whether this means promoting or reviving a positive and protective norm or mitigating or changing an abusive one.

37 [IASC, Policy on Protection in Humanitarian Action, 2016, Annexes I, V.](#)

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 take care, in their actions and relationship with the parties to an armed conflict, or with groups involved in other situations of violence, to avoid creating the impression that international law and standards can be lowered according to existing regional standards, domestic or local laws, and traditions. The norms embodied in international law and standards cannot be adapted or adjusted according to the domestic context.

This does not preclude taking a contextual approach with the authorities by suggesting realistic changes in law and policy that can help them progress towards compliance with international law and standards while improving respect for the population affected.

Such an approach to convincing the authorities may involve providing support to acquire the necessary technical, financial and other means needed to fulfil their international obligations. In addition, it may be necessary to engage in public education or to raise awareness among local constituencies, with a view to securing acceptance for international standards (e.g. on women's rights or reintegration of child soldiers), in particular if these are seen as incompatible with prevailing cultural or religious norms. It can take time, even several years, to make the necessary legislative changes, implement the laws and put in place adequate control mechanisms. Meanwhile, the authorities should not interpret the support provided as reasons or excuses for not meeting their obligations.

Making reference to soft-law standards and suggesting policy adaptations can also improve respect for the population and individuals affected. A good example is that of detention-related issues, for which the UN's Standard Minimum Rules for the Treatment of Prisoners are widely considered to be the source of reference for detention conditions, or the Guiding Principles on Internal Displacement, which are recognized as an important international framework for the protection of IDPs. Soft-law standards – some of which may simply reflect existing international legal obligations, while others may go beyond such obligations – do not give rise to enforceable rights by themselves; to do that, they have to be incorporated in domestic law. Protection actors must, whenever appropriate, convince the authorities of the relevance of these standards, to help them better fulfil their duties to the population and individuals affected.

COUNTERTERRORISM MEASURES AND PROTECTION WORK

Overly broad laws and standards on counterterrorism may have far-reaching protection implications. Such laws may be those of the country where a particular protection actor operates or those of the country where the protection actor's headquarters are; or they may be the laws of multilateral/regional bodies.

They may affect civilian populations not only directly (e.g. by expanding a State's detention powers) but also indirectly where they undermine the capacity of human rights and humanitarian actors to engage in protection and humanitarian assistance work in complex emergencies, particularly in areas under the control of armed groups and especially when these groups are designated as "terrorist groups". National and international measures that aim to curb the provision of financial or other material support to proscribed groups, i.e. groups that have been designated as "terrorist groups" or against whom sanctions have been imposed either by the UN Security Council, regional organizations or individual countries, can be particularly problematic, since the scope of their application might include the activities of impartial humanitarian organizations.

IHL protects the provision of humanitarian assistance without drawing distinctions among victims of war. Yet, certain counterterrorism laws may effectively criminalize medical assistance to injured fighters or the provision of humanitarian assistance to civilian populations; they may even consider IHL training as "material support to terrorism" in areas where proscribed groups may be operating. Human rights and humanitarian actors might also run afoul of counterterrorism laws where they have to directly engage with proscribed groups to carry out their work, e.g. to negotiate safe access to areas under the control of such groups, to provide them with training on international standards or to engage them in a protection dialogue. In some cases, protection actors may also be subjected to prosecution, because they provide legal assistance to "terrorist" suspects and help them assert their rights to due process and a fair trial. National staff employed by protection actors often bear the brunt of the adverse impact of counterterrorism measures. Engaging with a proscribed group may also carry significant reputational and financial risks for protection actors.

The financial sector is subject to regulations related to combating the financing of "terrorist" activities; these can have unintended consequences for aid actors reliant on banking services. To mitigate the risk of breaching such regulations, banks regularly "de-risk" their activities by excluding NGOs and other charities from financial services or by introducing cumbersome due-diligence measures. As a result, bank transfers to finance humanitarian activities or remittances to areas where proscribed groups operate may be delayed or denied altogether.

International standards – reaffirmed in the UN Declaration on Human Rights Defenders – protect human-rights defenders from being subjected to sanctions for doing legitimate protection work. Furthermore, IHL clearly entitles impartial humanitarian organizations to offer their services to all parties to a conflict. Prohibiting humanitarian actors from engaging with certain armed actors and populations living under their control also undermines the core humanitarian principles of humanity and impartiality: such a prohibition would force a humanitarian actor to withhold protection and humanitarian assistance from victims on one side of a conflict (see Standard 3.5).

The idea that certain civilians and those no longer taking part in hostilities are more deserving of aid than others, and that aid to certain civilians should be “de-prioritized” based on their alleged affiliation to certain groups, undermines the principles of humanity and impartiality (for more details on humanitarian principles, see Chapter 1).

Protection actors should be vigilant and insist that States not enact counterterrorism laws that have a detrimental impact on human rights or humanitarian work. Whenever a new measure is envisaged, they should seek to engage with policymakers and legislators on its potential impact on protection actors and populations affected. The laws adopted should consistently be based on precise definitions of prohibited conduct, and must contain appropriate exemption clauses for principled humanitarian and human rights work that requires engagement with non-State armed actors for protection and humanitarian assistance purposes. More broadly, a sustained dialogue with donors, financial institutions, various entities within governments and the public at large is critical in countering the narrative and associated policies that might impede humanitarian work in areas where proscribed groups operate. Knowing and understanding the applicable legal framework ensures that protection actors can push back against or challenge counterterrorism measures that may undermine principled humanitarian action.

ANNEX TO CHAPTER 4

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.



CHAPTER 5

PROMOTING COMPLEMENTARITY

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.

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.

Complementarity of analyses

- 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.

Mobilizing other protection actors

- 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.

Providing information on protection services and facilitating referral to relevant services

- 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.

Responding to harm and violations

- 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.

This chapter is concerned with managing effective interaction among humanitarian and human rights actors – who are increasing in number and diversity – doing protection work in armed conflict and other situations of violence. It recognizes existing capacities and acknowledges the varying approaches of protection actors to their work, and to complementing that of others. Its aim is to establish some minimum standards for complementarity, but not to propose a uniform approach to protection work.

Enhanced synergies among the protection activities of various actors can help optimize the benefits for the populations at risk. Seeking such synergies can also serve to minimize gaps, potential overlaps and duplication, and prevent situations where the activities of one actor disrupt or undermine those of another. For example, the publicity generated by the advocacy efforts of human rights actors can enhance the impact of strategies – quiet persuasion and community organizing – implemented by humanitarian actors to address the same issues.

However, enhancing synergies should never jeopardize the character of any of the protection actors involved. Care must be taken to respect and maintain their distinctive characteristics, to preserve their various identities and principles, and to avoid blurring the individual responsibilities of protection actors for the safety of the populations, and for using the information collected. As far as possible, protection strategies to reduce risk should incorporate the contributions of various actors towards the desired protection outcome (see Chapter 2).

Given the variety of protection actors involved in humanitarian response, concerted efforts should be made to ensure that methods and approaches are used complementarily to obtain optimal protection outcomes.

As shown below, complementary action can take several forms.

FORMS OF COMPLEMENTARY ACTION

Coexistence

When active cooperation among various actors is neither appropriate nor feasible, interactions focus on minimizing competition, to enable the actors to work in the same geographical area, with the same population, or on the same issues, without impeding each other's efforts.

Coordination

Dialogue and interaction among various actors serve to preserve and promote distinct characteristics or principles, to avoid competition, to minimize inconsistency and, when appropriate, to pursue common goals. Coordination is a shared responsibility, facilitated by liaison and common training.

Cooperation or collaboration

Joint work among various actors for a common purpose may include joint analysis and action. It does not necessarily signify common activities, or any merger of identities or characteristics, but rather some form of working together to achieve a common goal.

Contractual partnership

A more formal and legally constraining form of cooperation, this usually takes the form of a contract between organizations, which agree to contribute property, knowledge or activities to a given task. The contract defines the legal obligations and expectations of each partner, and often covers issues such as the transfer of financial resources and the secondment of personnel.³⁸

Establishing effective complementarity among the wide range of humanitarian and human rights actors doing protection work is important and requires specific efforts. While protection actors may share similar objectives with respect to protection – seeking to obtain “full respect for the rights of the individual”³⁹ – they also have different identities, mandates, priorities, approaches and activities that necessitate ongoing dialogue and coordination.

Organizations that subscribe to the principles of neutrality or independence as a means to gain access to all communities and actors in armed conflict and other situations of violence will be especially concerned to maintain their distinct identities and to respect their foundational principles. This can limit the degree to which they are able to engage in formal or visible sector-wide coordination structures. However, every effort should be made to coordinate on specific issues, such as tracing unaccompanied minors or establishing lists of missing persons following a crisis that caused displacement.

Other characteristics can affect interaction: actors may be faith-based or secular, national or international; their mandates may be rooted in IHL, IHRL or IRL; their priorities (refugees, children, IDPs, minorities, etc.) and geographical interests can vary. These various factors influence every protection actor's willingness, interest and ability to coordinate with others. Disparities in capacity

³⁸ Adapted from the IASC reference paper, *Civil-Military Relationship in Complex Emergencies*, Geneva, 2004.

³⁹ See the IASC-endorsed definition of “protection” in the introduction to this document, p. 13.

or resources, or even the distance between locations, can present additional obstacles to complementary action.

Such differences are, however, often the very reason why complementary action is needed. The multi-faceted nature of crises typically demands a variety of solutions. The multiplicity of humanitarian and human-rights protection actors and the diversity of their approaches is thus an asset. Because protection actors may work in different geographical locations and with different sections of the population at risk, their combined efforts can increase the scale and impact of a response.

Cultural, religious, ethnic and linguistic diversity means that local organizations may, in some situations, be better placed to obtain results. International actors may be more effective in other circumstances.

If protection actors want to achieve better results by making their various activities more consistent and coherent, they must – given the differences in their working procedures and approaches – make a conscious effort to coordinate their actions more closely. For instance, a confidential dialogue to persuade primary duty bearers to fulfil their protection responsibilities can be reinforced sometimes by public reports on the humanitarian and human rights consequences of their failure to do so; and a range of different actors raising similar concerns, or taking similar action simultaneously, can have a multiplying and mutually reinforcing effect.

Thematic collaboration among selected actors is frequent, such as inter-agency cooperation in disarmament, demobilization and reintegration or in matters related to gender-based violence. Some protection actors may choose to participate in coordination structures such as the in-country protection cluster, or in its working groups, such as the ones on gender-based violence and child protection.

The actual form of complementarity to be adopted will depend on an assessment by the protection actor of the most effective response to a given context or protection issue, as well as the most appropriate form of interaction. The ICRC, for example, with its concern for maintaining its neutrality and independence, may prefer to liaise on a bilateral rather than a collective basis, in the interest of preserving its confidential dialogue with weapon bearers and authorities.

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.

As outlined in Chapter 3 (on the protection architecture), it is important for actors involved in protection activities to articulate and communicate the nature of their roles so that their intentions and their work can be understood. Liaison with others working in the same geographical areas or on the same issues will help ensure that protection

concerns are addressed and that unnecessary overlaps do not occur. At the operational level, protection actors should share information regarding their general protection strategy and their target areas and populations, so that these elements can be incorporated in other actors' analyses and planning. This can be done through existing multi-lateral coordination mechanisms (e.g. the in-country protection cluster), through bilateral contacts or even through e-newsletters or briefings.

It is especially helpful, when planning or undertaking activities in a new context or with a new population, to consult with those already operating there, in order to identify potential gaps in the response. This will help protection actors avoid concentrating response efforts in the same geographical areas, or on issues that are already adequately addressed, unless they can provide a clear added value, or if the current response is considered to be insufficient in scale or quality. Assessments should be undertaken to clearly identify where the greatest needs exist, in order to determine where actors with specific expertise should focus their efforts.

As noted in Chapter 3 (Standard 3.2), a protection actor must also ensure – while acting in accordance with its mandate or mission statement – that its actions do not undermine the capacity of the authorities to fulfil their protection obligations. If the authorities fall short in discharging their protection duties, this may be due to inadequate capacity or lack of will. If it is a question of capacity rather than will, providing them with support, as opposed to pure substitution, may be the more constructive approach to increasing the chances of their achieving a sustainable impact. Where authorities have the means to respond, but are unwilling to do so, it is essential to avoid undermining other protection actors' efforts to persuade the authorities to respond more comprehensively. For example, if several actors have taken a collective, principled decision not to substitute for authorities who have the means to respond, any protection actor who chooses to do otherwise must act only after giving the matter the most careful consideration. In all events, a protection actor should proactively advise other actors likely to be affected by its actions.

Being able to deliver on commitments made is another crucial requirement for effective complementarity. Protection actors should ensure that they possess the necessary skills and resources to follow through on their intended roles or activities, and should be transparent about their roles and activities, and about their estimated duration (see Chapter 7). If shortfalls occur, or if they have to withdraw unexpectedly, the protection actor should inform others and efforts should be made to ensure an effective handover.

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 remain central to all protection work, some protection actors also maintain the principles of neutrality and/or independence as core values, which also enable them to gain access and proximity to people at risk in armed conflict and other situations of violence. Adherence to these principles

is a working method; it is also a means of facilitating the engagement in protection activities of all parties to a given conflict, and of all sections of the population affected.

Actors that decide not to share, or that cannot implement these additional principles, should acknowledge and respect the commitment of those that seek to do so. In particular, actors that are not neutral in a crisis – or are not perceived to be so – because of their activities or associations, should be careful not to publicly implicate others in their actions. They should also be aware that actors adhering to the principles of independence and/or neutrality may be required to limit the extent of their coordination or complementary action with others, in order to safeguard their commitment to these principles – in actual fact and in terms of public perception.

COMPLEMENTARITY OF ANALYSES



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.

Analysis is critical for the effectiveness of a response. A good understanding of the environment, the changing trends of violations and abuses, and other protection concerns can help reduce gaps or duplication and foresee future risks (see Chapter 2).

The diversity of humanitarian and human rights actors doing protection work helps increase this understanding and contributes to more comprehensive responses. Different actors focus on many different matters: various geographical areas; issues such as gender-based violence, tracing, judicial reform, prison conditions, the role of security forces in emergencies; specific sections of the population affected; and so on. The resulting diversity, of perspective and approach, enriches analysis. Sharing this diversity helps increase the overall understanding of a given context.

The contextual analysis should examine 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. Due attention also needs to be given to age, gender and other relevant features that might increase people's exposure to threats within their environment. This information should be made available with appropriate amounts of detail, while ensuring respect for informed consent and confidentiality. To maintain confidentiality requirements, some actors may limit their information-sharing to general protection concerns.

The sharing of information and analyses does not presuppose a shared perspective on protection issues. Nor does it mean that all analyses should be undertaken jointly. Differences in organizational mandates, priorities and approaches – including the need for independent and confidential action – can make joint assessment and analysis inappropriate in certain cases. Where possible, however, and particularly when common purposes and approaches exist, inter-agency analysis and assessment should be given priority, in order to reduce duplication and to contribute to coherent messaging and advocacy. Drawing upon existing analyses and assessments is often useful, provided they are relevant and of good quality.

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. In terms of the formal protection architecture, the first step is usually to encourage the primary duty bearers to comply with their responsibilities. But in situations where the authorities are failing, humanitarian and human rights actors may be required to help address the most urgent protection concerns. If important gaps persist, they may also need to mobilize others with the requisite expertise and capacities to address critical, unmet protection needs. This is true at both the institutional level, such as for the development of legislative norms or policy, and at the operational level. Encouraging action by others does not imply directing their response, but rather sharing information and analysis of important, unaddressed protection concerns that have been identified.

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.**

Access to information on available services is often critical for the protection of populations affected. In all situations, protection staff should be able to provide information on the services available to those in need, such as: health care, psychosocial services, security measures, tracing of missing people, documentation services for those lacking essential identity documents, and legal services for those in need of legal aid or advice on how to access accountability and redress mechanisms. Services may be provided by State authorities as well as by national and international civil society organizations, other international organizations, humanitarian and human rights actors, etc. Ideally, referral information should be given after due assessment of the quality of these various services and their conformity with professional standards. Protection actors should coordinate with other clusters or sectors in order to obtain relevant information about services and their quality.

Whenever possible, protection actors should proactively facilitate access to such services. For example, after a sexual assault, safe, timely access to emergency contraception and post-exposure prophylaxis is critical. Rapid access to services may also be essential for others with special needs, such as unaccompanied children, elderly persons, individuals with a chronic medical condition, or persons with disabilities. In such situations, rapid and accurate information on how to safely access critical services, in a manner practicable for the person the services are intended for, is of paramount importance. It can be vital for survival, or for preventing further harm, including exploitative abuse in the form of human trafficking, child labour or forced labour.

Facilitating referral in these cases may also involve ensuring that the person can physically reach and obtain access to the necessary services. At a minimum, it requires providing contact information on services of proven reliability. Protection actors should therefore compile this information with a view to its rapid transmission, when required. Other referral actions include calling emergency services, transporting the person(s) in question and providing the financial means required to access services. Whenever possible, a family member should accompany a person in need of medical care. For organizations covering transportation costs for accessing services, it is good practice to also cover the costs for the accompanying person, partly or fully. The informed consent of the person being referred must be obtained (see Chapter 6). In circumstances where this is not possible, owing to the age or incapacity of the person(s), a decision on referral should be taken on the basis of their best interests.

The act of facilitating referrals does not imply a responsibility to ensure access, but rather to take all appropriate and feasible steps in order to facilitate this access, within the capacity and means of the actor in question. This could include: negotiating with authorities or other actors controlling the area, to ensure fair and secure access; or urging specialist service providers to increase their coverage or capacity, or giving them support for doing so, by facilitating the visit of a mobile outreach team, for instance.

These aspects should be taken into consideration and the person in need duly informed of them and of the limits to the assistance the protection actor can provide; however, none of these considerations should prevent immediate action in a critical situation. Adequate follow-up should also be undertaken, according to the actor's competencies and capacities.

Whenever protection actors decide to set up internet platforms to allow individuals and communities in areas affected by a crisis to register directly – as is the case with sites dedicated to the search for missing persons during emergencies – or to send information on unfolding events, they should include information on the functioning services available to these individuals and communities. Protection actors should regularly verify, to the extent possible, that the information they transmit is correct and up to date.

Protection actors should use the ability of specialist service providers, or ask for their support, to ensure that their internet platforms are of good quality, accessible and user-friendly, and that they are complying with the relevant data protection standards, including the confidentiality requirements discussed in Chapter 6.

When such platforms are set up by third parties, protection actors should ask them whether they would be willing to disseminate information on existing protection services that could benefit individuals and communities.

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, whether these are recurrent or isolated instances. 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. Some actors may also document patterns of harm and violations affecting particular populations or geographic areas. When these violations are serious, protection actors have a **duty** to take appropriate action.

The type of action will depend on the circumstances and the mandate, role and capacity of the actor. For example, a UN Humanitarian Coordinator has a direct responsibility to promote respect for IHRL and IHL by all parties, including non-State actors.⁴⁰ Other actors may pursue more indirect methods, such as relaying information with a view to preventing, halting and seeking accountability for violations, which might include effective remedies and access to justice for the population affected.

While some human rights actors typically engage the authorities directly and urge them to fulfil their human rights obligations – and do so on the full range of violations and related cases they have documented – other protection actors may choose to alert organizations that have a responsibility and the ability to take action.

Taking such action does not relieve primary duty bearers of their responsibilities. If violations or abuses have occurred, action can be taken to prevent any recurrence, to reduce the consequences for populations affected and ensure accountability. In the case of violations that are ongoing or imminent, action must aim at stopping or preventing them, and ensuring accountability. The type of action required will also depend on the nature of the violation and on the particular needs and capacities of the victim(s).

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 (see also Chapter 6). Some protection actors may not be able to share detailed information owing to issues of confidentiality.

Protection actors reporting a protection concern should provide sufficient information to allow others to act. Clearly formulated procedures for doing so should be drawn up by every protection actor. All transmission of information should abide by the standards established in Chapter 6 (on managing data and information for protection outcomes).

⁴⁰ IASC, *Terms of Reference for the Humanitarian Coordinator*, 2009.

ANNEX TO CHAPTER 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.

Gioffi 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.



CHAPTER 6

**MANAGING
DATA AND
INFORMATION
FOR
PROTECTION
OUTCOMES**

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

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.

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.

Clearly defined, specific purpose

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

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 persons affected, witnesses and communities.

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.
- 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.
- 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.

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





Compliance with relevant legal frameworks



- S** 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.

Legitimate and fair processing



- S** 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.

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



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 purpose(s) for which they were collected.



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.



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.



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.



Confidentiality

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



Sharing, transferring and publishing

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

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, monitoring of quality and supervisory mechanisms.

SECTION 3 – ASSESSING THE RISKS

-   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 them, and for their families and communities.

INTRODUCTION

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

Collection and analysis of protection data and information is essential for evidence-informed protection work. Striking the right balance while collecting data – between timeliness and depth of detail – is often challenging, and requires a thorough analysis of the most appropriate collection method for achieving the objectives identified. Sharing the information collected and the related analysis with other protection actors, within a reasonable time frame, is often key in achieving the desired protection outcomes.

Given the potential sensitivity of protection data and information, it is essential to ensure that they are handled appropriately at each step of the information management process.

This chapter does not seek to give an exhaustive description of internationally accepted data protection principles (see Annex 2 below) applicable to the processing of personal data; it seeks instead to highlight the most important elements through a broader perspective that encompasses “protection data and information”. For more detailed information and guidance, please refer to the Brussels Privacy Hub/ICRC *Handbook on Data Protection in Humanitarian Action*.⁴¹

The phrase “management of protection data and information” refers to the *processes* of handling data and information (the collection, analysis, storage, sharing, use, destruction or archiving of data and information) that are required to enable evidence-informed action for quality protection outcomes. It comprises multiple systems, methods and tools that serve different and distinct purposes and produce different outputs in terms of data and information. To be safe, meaningful and effective, the management of protection data and information must be done in a principled, systematic and collaborative manner, which is what the standards in this chapter will address.⁴²

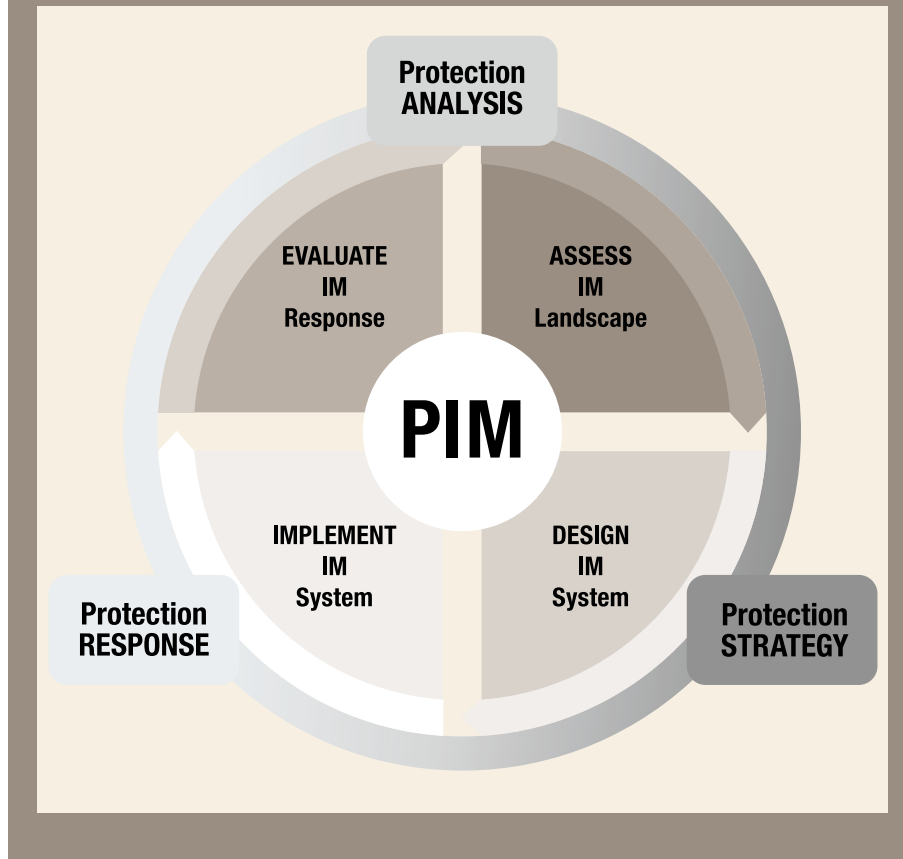
⁴¹ Brussels Privacy Hub/ICRC, *Handbook on Data Protection in Humanitarian Action*, 2017.

⁴² See also the PIM Guide, comprising the definitions, principles, structure, guidance, core competencies and other products of the [Protection Information Management \(PIM\) Initiative](#).



43 Diagrams reproduced from the [PIM guide](#).

The PIM process can also be represented in a circular diagram:



Management of protection information is important because it serves the purpose of informing, facilitating and supporting protection results and outcomes. Proper management of such information yields the evidence needed for the analysis of a particular context and associated protection risks, and for the development of protection strategies and protection responses, including protection programming and advocacy on protection issues. Protection information management activities occur throughout a project/programme cycle.⁴⁴

Safe and responsible management of the data and information collected in the course of protection work, particularly the personal data of individuals and sensitive protection data and information, is an essential aspect of protecting people's lives, their physical and mental integrity, their rights and their dignity.⁴⁵

Management of protection data and information often involves dealing with a number of sensitivities that are in the nature of protection work. Unauthorized disclosure of, or access to, personal data and/or sensitive protection information (for example, those relating to violations of rights or threats of violations, patterns of violence, abuse, coercion and deprivation) may result in harm to the very individuals and communities that protection actors aim to protect. The exceptional circumstances in which protection actors operate, in particular in armed conflict and other situations of violence, create special challenges regarding the management of data and information.

⁴⁴ See Chapter 2 of this document, on managing protection strategies.

⁴⁵ See also [PIM Principles](#).

In an environment that is increasingly digitalized, embracing the fundamental principle of “do no harm” thus requires protection actors to assess and address the impact of their information-processing operations on populations affected. This is why the protection of personal data is of fundamental importance for protection actors.

In practice, risks may range from physical and mental harm or threats of harm, discrimination, social marginalization and stigmatization, and are often not foreseen by the individual soliciting the information or the person providing it. Particularly in armed conflict and other situations of violence, people providing information to protection actors may even face reprisals, regardless of the content of the information shared, for merely participating in the data collection process.

These risks must be mitigated to ensure that the “do no harm” principle is respected throughout the process of managing protection information.

Deciding on the most relevant and appropriate systems and methods requires careful consideration of their purpose and the risks. Competent staff are needed to manage the flow of information, to take into account the possible biases⁴⁶ and to conduct risk analyses. While they clearly have advantages for humanitarian and human rights action, information and communication technologies (ICT) also introduce new challenges with regard to data protection and security.

PURPOSES OF MANAGING PROTECTION DATA AND INFORMATION

Protection work requires the collection, analysis, use and sharing of data and information for various purposes, including as a means to:

- protect people affected by armed conflict and other situations of violence
- trace individuals to restore family links, organize family reunifications or identify human remains
- protect people deprived of their freedom
- build respect for IHL, IHRL and IRL
- provide documentation for establishing the legal status of IDPs, refugees or stateless persons, to determine their entitlement to rights and assistance
- create a basis for advocacy and campaigning on protection, including activities such as media work, and raising of public awareness
- monitor the situation of vulnerable individuals or people at risk of violations or abuses
- report incidents, and refer and follow up the people affected
- identify protection trends and substantiate reporting
- support efforts concerning accountability, remedy and reparation for human rights violations
- inform protection analysis, strategy and response.

N.B. Although not its primary purpose, the collection of protection data and information may also support fundraising. When this is the case, the same standards apply.

⁴⁶ See Standard 1.2.

Structure of the chapter

This chapter is not intended to be comprehensive;⁴⁷ instead, it outlines the key standards for managing protection data and information. It is divided into three parts:

The first section presents the **general standards applicable to the management of all data and information used in protection work**. They apply throughout the data and information life cycle, from their collection and analysis, to their use, sharing, correction, deletion and archiving.

The second section presents the standards applicable specifically to the **management of personal data and sensitive protection data and information**. They too apply throughout the data and information life cycle, from their collection and analysis to their use, sharing, correction, deletion and archiving. These standards *must* be applied when handling personal data. Failure to do so may cause harm to the individuals whose data are processed, and may have legal consequences for the protection actor. Where the practitioner is managing sensitive protection data and information that do *not* contain personal data, these standards must also be applied as a matter of best practice. These standards may also be applied to protection data and information that neither contain personal data nor are sensitive; application of the standards in this context is particularly encouraged, when appropriate.

The third section provides guidance on **assessing the risks associated with the management of protection data and information and on risk mitigation measures**. It includes practical advice for carrying out a data protection impact assessment (DPIA) to identify and mitigate any risks to **personal data and sensitive protection data and information**. More generally, DPIAs may also be used when assessing risks relating to the management of protection data and information that do not contain personal data and/or are not sensitive.

WHO SHOULD APPLY THESE STANDARDS?

This chapter is addressed to all protection actors involved in handling protection data and information, including personal data. “Protection actors” refers to humanitarian and human rights organizations that seek to ensure that obligations under IHL, IHRL and IRL are respected and that the rights enshrined therein are enjoyed without discrimination.

The standards outlined in this chapter should also be applied, when appropriate, by professionals working in humanitarian or human rights responses but not in traditional “protection” work – for instance, people working in assistance, media and communication, fundraising and information communication and systems technology – who may also be processing personal data and protection data and information collected from persons affected, 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 to victims, witnesses or perpetrators of violations, or to incidents and events associated in any way with violations and abuses.

⁴⁷ For further guidance on protection information management resources, see Annex 4 to this chapter.

In fact, most standards linked to protection data and information management presented in this chapter 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, during natural disasters, as well as in armed conflict and other situations of violence.

For instance, information gathered for shelter and livelihoods programmes (composition of average family household for shelter-size requirements, whether and why a family or an individual requires livelihood assistance, other details such as bank account and card numbers for cash-based assistance programmes, etc.) often include personal data and sensitive information that need to be treated with due care.

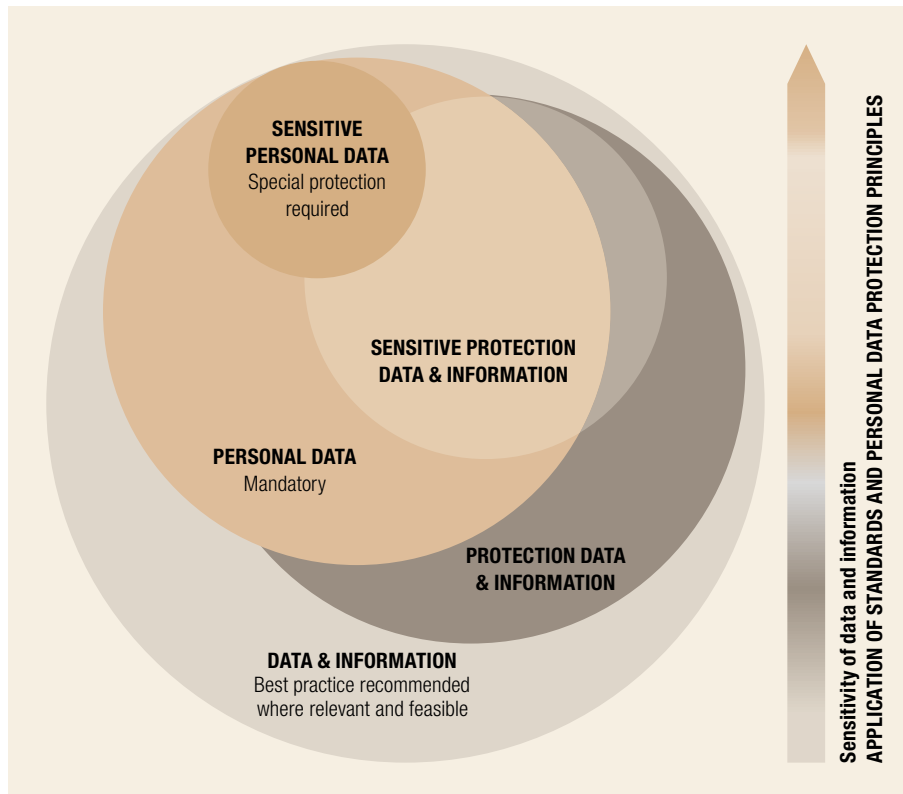
Likewise, actors dealing with aggregated information for the purpose of trend analysis should also be aware of possible risks and sensitivities associated with the information they handle and how to safeguard it.

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. They must also identify the risks and proper safeguards to mitigate them. For this purpose, they should carry out a risk assessment and review it on a regular basis throughout the project or programme cycle.⁴⁸

Several broad categories of data and information can be identified. The more sensitive the data and information, the stricter the data protection rules and standards that will have to be applied, as illustrated in the following diagram (categories of data often overlap).

⁴⁸ See Section 3 below on assessing risks.

Diagram: Relationships between types of data and information**Protection data and information**

This is a collective term to describe 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, and may include personal data and/or “community identifiable information”. It may relate to a specific event or to a general situation or a context.

Information not collected directly for protection purposes may also be relevant for protection work.

Personal data


Personal data, also known as personally identifiable information (PII), are data relating to an identified individual or to a person who can be identified from that data, from other information, or by means reasonably likely to be used related to that data: an identifier such as a name or audio-visual materials, an identification number, location data or an online identifier.

Personal data include biographical data, such as name, sex, marital status, date and place of birth, place of residence, country of origin, country of asylum, individual registration number, occupation, status, religion and ethnicity; biometric data, such as a photograph, fingerprint, facial or iris image; and any expression of opinion about the individual, such as an assessment of their legal status and/or specific needs.

The right to the protection of personal data emerged mainly in the last decades of the 20th century. It is now being enshrined in an increasing number of jurisdictions, at the international, regional and national levels,⁴⁹ and in part arises from the fundamental right to privacy, which is recognized as a human right in various international instruments.⁵⁰

A key element of data protection is that those whose personal data are processed (“data subjects”⁵¹) have rights with respect to the way their data are handled (see Annex 3 below). These rights are not absolute. They should be considered in relation to the overall objective of protecting human dignity, and be balanced with other human rights and fundamental freedoms, in accordance with the principle of proportionality.⁵²

Given the growing importance of data protection legislation around the world,⁵³ and the need for protection actors to apply strict standards in the management of personal data, the professional standards set out here require the application of the principles of data protection⁵⁴ to all personal data. The principles are in line with international best practices and with recent legal and regulatory developments. They should be followed even in places where the legal requirements are weaker or non-existent. Protection actors should always ensure that they are aware of and comply with all applicable laws.

In this chapter, professional standards that are derived from internationally accepted data protection standards, and which therefore *must* be applied when dealing with personal data, are specifically identified by a padlock icon: 

Sensitive protection data and information

Sensitive protection data and information are data or information that, if disclosed or accessed without proper authorization, are likely to cause:

- harm (such as sanctions, discrimination) to any person, including the source of the information or other identifiable persons or groups; or
- a negative impact on an organization’s capacity to carry out its activities or on public perceptions of that organization.

The sensitivity is defined in relation to the particular context, the dynamic of violence and abuse, and the level of aggregation. Therefore, the same types of data may have different levels of sensitivity in different contexts; and sensitivity may change over time.

⁴⁹ E.g. UN Universal Declaration of Human Rights (1948); OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980, updated 2013); Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981); African Union Convention on Cyber Security and Personal Data Protection (“Malabo Convention”, 2014); and the European Union General Data Protection Regulation (GDPR, 2016). Domestic and regional laws usually provide additional specific rules for highly sensitive data, such as genetic data, medical information, religious affiliation, race and ethnicity.

⁵⁰ See Article 12 of the Universal Declaration of Human Rights, and Article 17 of the International Covenant on Civil and Political Rights.

⁵¹ In data protection legislation, the person concerned is usually called the “data subject”.

⁵² The principle of proportionality in this context should not be confused with the principle of proportionality under IHL. The principle of proportionality discussed here requires that protection actors take the least intrusive measures available when limiting the right of data protection and access to personal data, in order to give effect to their mandate and to operate in emergencies.

⁵³ Such as the modernization of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature on 28 January 1981, in force 1 October 1985, ETS 108), and the forthcoming entry into force of the European Union’s General Data Protection Regulation (GDPR) (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.

⁵⁴ See Annex 2 to this chapter.

Protection data and information that do not contain personal data (including information relating to the humanitarian, human rights, political or security situation) may nevertheless be sensitive. They may concern communities and other groups,⁵⁵ anonymous individuals, or specific events or issues.

Data that are aggregated or pseudonymized⁵⁶ may also be sensitive: individuals or groups may be still be identifiable – location and sample size are crucial determinants of this – and thus may be exposed to harm if data about them are disclosed.

It is therefore not possible to propose a definitive list of the types of data or information that constitute sensitive information. However, information about the nature of violations affecting specific individuals or groups, certain details about victims and witnesses, the affiliation of perpetrators, details related to military operations or security, etc. may belong to this category.

The professional standards set out here recognize that the privacy, security and integrity of individuals or groups may be put at risk even if no personal data are collected and processed; therefore, they require – as a matter of best practice – that protection actors apply the standards derived from the principles of data protection to sensitive data and information used for protection purposes, to the extent that it is necessary, given the particular sensitivity of the data.

Sensitive personal data

Sensitive personal data are personal data that, if disclosed, are likely to result in harm (such as discrimination) for the individual concerned. As a result, many of the international instruments on data protection mentioned in this chapter include stricter rules for the processing of sensitive personal data.

Given the specific situations in which protection actors work, and the possibility that some data could give rise to discrimination, setting out a definitive list of categories of sensitive personal data in protection contexts is not meaningful. Sensitivity of data and appropriate safeguards (e.g. technical and organizational security measures) will be context-dependent and may change over time within a given context; therefore, they need to be considered on a case-by-case basis.

Data relating to health, race or ethnicity, religious/political/armed group affiliation, and genetic and biometric data are considered to be sensitive personal data at all times. The nature of violations and abuses affecting specific individuals or groups, and the identity of perpetrators and witnesses, also fall into this category. All sensitive personal data require additional protection, even though different types of data falling within the scope of sensitive data (e.g. different types of biometric data) may present different levels of sensitivity.

⁵⁵ Such data or information may be referred to as “community identifiable information” or “demographically identifiable data (CII/DII)”.

⁵⁶ “Pseudonymization” of data means replacing any identifying characteristics of data with a pseudonym or a value that does not allow the data subject to be directly identified. For example, “Jane Doe” could be pseudonymized to “POC 15364”. But pseudonymization allows identification using indirect means, and should be distinguished from “anonymization”, as it provides only limited protection for the identity of data subjects in many cases. Where a pseudonym is used, it is often possible to identify the data subject by analysing the underlying or related data.

The use of ICT and other technologies

The management of protection data and information is evolving with the growing use of information communication technologies (ICTs). Setting up data collection, combining data sets, cross-checking and analysing data from different sources, and using and archiving data have all become more complex with the multiplication and diversification of digital sources of information. Mobile phone-based applications, digital platforms and social media have made it easier – through surveys and other feedback mechanisms – to communicate with populations affected and to obtain timely information from them about their needs or the abuses and violations they endure. Remote sensing with satellite imagery or unmanned aerial vehicles (UAV) may help establish the destruction of civilian infrastructure, locate mass graves or rapidly map a makeshift camp for IDPs and its surroundings.⁵⁷

ICTs have also enabled the development or expansion of new methodologies – crowd-sourcing, for example, which depends on the participative online activity of volunteer networks. 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 among humanitarian and human rights organizations.

Communities affected are themselves increasingly using the available technologies to communicate while self-organizing during and after crises. In recent years, “Communicating with Affected Communities”⁵⁸ has emerged as an important activity: it focuses on the importance of understanding and learning from the ways in which communities affected communicate with one another and the outside world, and on how protection actors can support both communities in these endeavours and community-based information management systems and tools, including when it comes to protection data and information.

ICTs 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. Notwithstanding their immense potential for protection work, these developments have also increased the risk to individuals’ privacy and safety. This has resulted in legal and regulatory efforts being made throughout the world to respond to these concerns.

It is therefore essential to have a good understanding of the risks that can result from the use of any tool or technology, old or new, before using it. ICTs can help mitigate some existing challenges (using strong encryption against interception of mail, for instance), but may also create new ones and give rise to new risks that must be addressed:

- The risk of interception and then persecution by third parties when persons affected use electronic means of communication (text messages, email, social media, etc.) to rapidly pass on information about problems they face.

⁵⁷ For detailed guidance on drones/UAVs and remote sensing, biometrics, cash transfer programming, cloud services or mobile messaging applications, refer to the Brussels Privacy Hub/ICRC *Handbook on Data Protection in International Humanitarian Action*, 2017; see also the ICRC/Engine Room report, *Humanitarian Futures for Messaging Apps: Understanding the Opportunities and Risks for Humanitarian Action*, 2017.


⁵⁸ “Communicating with Affected Communities refers to communication with, by and between communities and/or community members with the aim of supporting community exchange, access to services, feedback/complaints, transparency, monitoring and evaluation, participation/empowerment, and leadership/community capacities. Communicating with affected communities should be both mainstreamed into other systems and a distinct mechanism to support communities.” (*Second PIM Working Meeting Outcome Document*, Geneva, December 2015).

- Loss of control for individuals over their personal data: once data have been made public on the web, it is nearly impossible for users to reclaim, modify or delete them. Similarly, a lack of feedback loops or accountability mechanisms for persons affected might prevent them from knowing how their data have been used.
- Misuse of personal data by ill-intentioned third parties, including through the capture and use of metadata.
- The risk of raising false hopes that there will be a rapid response, or in fact any response at all, to the concerns expressed by individuals or communities.
- The difficulties associated with obtaining informed consent from people who have had little or no exposure to modern information technology.
- Unequal access to technologies because of differences in location, social class, ethnicity, age and gender.
- Biases, misinformation and manipulation of information, exacerbated by viral loops on the internet that sometimes amplify narratives detrimental to protection outcomes – for example, the erroneous conflation of displaced persons with “terrorists”.
- Lack of in-depth dialogue with populations affected that might be exacerbated by one-way communication from individuals to protection actors and mass communication from protection actors to individuals.

This chapter seeks to ensure that protection actors collect, use and share data in a safe and responsible manner, but it does not provide technical guidance on how to make use of ICTs or specifically address these risks (although some references are provided in Annex 1 below).

Although the need for caution is central to the standards discussed in this chapter, it should not be interpreted as a call to avoid using ICTs or sharing information altogether. The professional standards presented here stress the requirement for protection actors to assess and mitigate risks before taking action.

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. For each of these steps, a number of specific standards apply and certain key considerations must be taken into account.⁵⁹ As elsewhere in this chapter, standards that are denoted with the padlock icon  must be adhered to when dealing with personal data or with sensitive protection data and information (even if the sensitive protection data and information do not contain personal data).

Competencies and capacities⁶⁰



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 therefore particularly important. Practitioners need to understand how data sets are produced, used, presented, connected, aggregated and interpreted. They need to be aware that where multiple data sets exist, covering information about the same individual or group of people, re-identification of a person may be possible – even when the data sets have been pseudonymized.

Given that the responsibility for safeguarding data lies with the actors handling them, 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. This requires people who are aware of the privacy, data protection and security challenges associated with data management in general, and who understand the use of, and the risks associated with, specific technologies before employing them.⁶¹

Inclusive people-centred approach



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.

⁵⁹ See also Chapter 2 on managing protection strategies.

⁶⁰ See also Chapter 7.

⁶¹ For a quick guide to the risks associated with the use of various ICTs and how to mitigate them, see Rahel Dette, *Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts*, Global Public Policy Institute, Berlin, 2016. More detailed information can be found in the Brussels Privacy Hub/ICRC *Handbook on Data Protection in International Humanitarian Action*, 2017.

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.⁶²

Approaches should be systematically adapted to the different categories of age, gender and diversity, to ensure that all persons (including the socially marginalized) are able to participate fully in the decisions that affect their lives and the lives of their relatives and communities.

Clearly defined, specific purpose



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, clearly defined purpose.⁶³ Protection actors must therefore collect and process information only when necessary for the design or implementation of protection activities (see Standard 6.11 on data minimization). The purpose should be communicated to the persons from whom data are collected.

Before collecting data, protection actors must therefore determine and define the specific purpose(s) for which data will be processed, aiming at protection outcomes, and process it only for this/these purpose(s). The protection information and data that are collected should be adequate, relevant and proportionate⁶⁴ to this/these specific purpose(s).

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 those original purposes (in particular, where the processing is necessary for historical, statistical or scientific, or for the accountability of humanitarian actors). Such data might include those collected in order to improve the conditions of detention in a specific place being used for more general advocacy on the issue of overcrowding in prisons. However, further processing is not permissible if the risks to the individual, foreseen by the protection actor, outweigh the benefits.⁶⁵

Protection actors should take care to consider and identify at the outset of data collection, and as much as possible in emergency circumstances, all possible future purposes, in order to be as transparent as possible with the sources of information, and to ensure that the consent obtained covers possible future relevant purposes (see Standard 6.9 on legitimate bases).

Establishing clear objectives and time frames is central to the information collection process. Problems often arise when these objectives are not clearly defined and/or when the reason for collecting information is not made clear to those involved in the process. The data collection process should support a specific protection objective and should be designed to fit this objective. All those involved in the information management process, and those who may handle or use the data at some point, should have a common understanding of this objective.

⁶² For more guidance, see Standards 1.6–1.10.

⁶³ In relation to the collection of personal data, the specific purpose must be **legitimate**, i.e. genuine, appropriate and warranted.

⁶⁴ See Standard 6.11. on data minimization.

⁶⁵ See Standard 6.18 on assessing risks.

Clear objectives are also required to set the scope of the information collection. This can be narrow or broad, according to what is needed to achieve the stated objectives. An example of a narrow scope could be children, in a specific geographical area, who have been separated from their families in the last 12 months. Clarity of objective, precise definition of the scope of the information to be collected, and adequate awareness of these elements among those involved all contribute to determining the core information requirements. In defining the scope of information needed, protection actors should have in mind long-term strategies and objectives related to data collection, and should not miss opportunities to collect data from individuals who may be difficult or impossible to contact again. A broader scope for information collection may be chosen, in view of expected difficulties in re-establishing contact with individuals or communities; but that breadth of scope should not be a reason for failing to contact again, whenever feasible, individuals who have contributed to the information collection.

Without this clarity, field staff may omit valuable information because they do not realize its importance; or they may collect sensitive information that is not relevant to the defined purpose and objectives, and will therefore not be used. In line with Standard 6.11 (data minimization), information that is not necessary for the purpose identified before or during collection should simply not be collected; this is necessary in order to avoid collecting excessive personal data or creating unnecessary risks for, painful questioning of, or false expectations among those providing the information.

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 persons affected, witnesses and communities.

Protection actors should avoid repeatedly asking sources of information the same questions, particularly when they are survivors of abuse or gender-based violence; they should also seek to ensure that the information source does not need to provide the same information to multiple actors. Repetitive questioning may traumatize or retraumatize the information source. The protection actor must be sensitive to such risks, and must ensure, for example, to the degree feasible, the appropriate psychological or psychosocial support both during and after the interview. It is equally important to minimize, as far as possible, the need for multiple interviews and questions.

Protection actors should also carefully consider whether the information collection is essential for fulfilling their protection objectives, and whether its potential positive impact warrants the anxiety that may be generated among those concerned.

In order to limit unnecessary duplication of data collection, protection actors should consult each other to determine who is to collect what type of information and for what purpose; they should also determine how much information is already available, as well as if and how it can be shared.⁶⁶

There can be some degree of incompatibility between the necessity of collecting accurate and comprehensive information, and that of minimizing the trauma and burden for the information provider. When confronted with such dilemmas, protection workers should prioritize the “do no harm” principle.⁶⁷

⁶⁶ See Standard 6.16 on sharing data.

⁶⁷ See Standard 1.4.

Avoiding bias and discrimination



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.

Data and information collected by protection actors may not always be representative and accurate, and may contain gaps as a result of bias⁶⁸ in the data collection or in subsequent steps; this may lead to incorrect analysis and/or discrimination, including of under-represented individuals or groups. Protection actors must be aware of the possible under- or over-representation of some categories, owing to language barriers, political affiliation, educational level, access to means of communication and other factors.

Bias in the process of information gathering and analysis may stem from respondents, intermediaries or the protection actors themselves, and may be due to a range of factors, such as discriminatory practices and power dynamics.

For example, protection actors may reproduce in their information collection the biases of patriarchal societies where people undervalue information and knowledge generated or possessed by women. This could result, for instance, in not reaching out sufficiently to women – or to enough numbers of women – or in choosing information collection methods that are less accessible to women.

Certain segments of the population may also be under-represented because of the inaccessibility of certain areas, which prevents the protection actor from obtaining a representative sample. Bias may also result from communication barriers between the protection actor and the informant, such as the reluctance of female interviewees to share information with male interviewers, or prejudice and assumptions on the part of the interviewer. There are other possibilities as well: an informant may be unable to recall events; other informants may give false or exaggerated testimony because of social pressure, political or ideological convictions; still others may attempt to influence the provision of aid.

Different methodologies used for data collection differ inherently in their potential for bias. For example, crowdsourcing combined with modern technologies can provide for more instant communication and reduce bias linked to the unequal presence on the ground of protection actors. However, crowdsourcing may entail other biases – unequal access to devices, mobile phone networks or internet connections – that can give a distorted picture of the reality on the ground.

Consequently, protection actors must take all reasonable measures not to replicate power dynamics as they exist in a context, and to control possible biases that may result in unintentional discrimination. Even when it does not amount to discrimination, bias hampers an accurate understanding of the situation and distorts the decisions taken, including the resultant protection response.

⁶⁸ “Bias” may be defined as any systematic distortion of information, whether intentional or not. Understanding the potential for bias in information management is the starting point for avoiding it and minimizing or mitigating its effects. For more information on bias, see Standards 1.2 and 1.3.

Bias should be minimized by designing information collection procedures that ensure representative sampling, and by raising awareness during the training and coaching of staff collecting the data and information or processing those collected by others. A combination of methodologies and sources – including crowdsourcing and satellite and aerial imagery, as well as traditional methods such as collecting information and conducting reviews on the ground – will help cross-check information and increase accuracy and minimize the risk of distortion.

The **principle of non-discrimination**⁶⁹ in this context requires protection actors to identify instances of discrimination in any given situation that they are trying to address. To do this, it is important to collect information that 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.

Individuals who have provided information (including personal data) on abuses and violations usually expect that the protection actor gathering the information will take action on their behalf; this may include steps to ensure that the rights of the persons whose data is processed are respected. Return visits, public communication or information campaigns or other forms of follow-up give the protection actor the opportunity to provide an update to the persons affected on the steps taken and on progress achieved.

Furthermore, return visits demonstrate respect for those who took part in the information collection process and increases trust among them that their needs are being taken seriously, which may yield further information; however, any additional personal data of this kind will also be subject to the same principles and standards that applied to the initial information and data collection exercise.

Return visits or follow-up contact also allow for enquiries about possible repercussions and reprisals that informants may have faced following information collection or subsequent actions taken on their behalf. Whenever such consequences are reported, the protection actor should do their utmost to take corrective action. The protection actor should also incorporate the feedback and observations obtained in ongoing risk analyses, and evaluate the need to revise preventive measures and procedures for processing data and information. It must be underlined that in some circumstances, return visits to those who have given information confidentially can be potentially dangerous, notably because they draw further attention to the individuals' contacts with a humanitarian or human rights actor.

In the case of information collected from the general public through the internet and/or via SMS, those who started the crowdsourcing exercise in question should ensure that they regularly update their website and other information channels, including social media, to inform the public on the use made of the information received. They can also keep communities informed through local radio, TV stations and social media. When doing so, protection actors must make sure not to cause harm to the individual sources or to the communities or individuals on whose behalf they are working. For example, they should refrain from sending text messages informing individual persons of actions taken in

⁶⁹ See Standard 1.2.

relation to specific incidents of abuse and violations. This is unless they have assessed the matter and found that there was no particular risk of such text messages being intercepted or read by the wrong person, including a friend or a family member who may not be aware of the fact that someone had provided information.

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.

Before starting to collect data and information, protection actors should define the level of reliability and precision that will be required, and how often the data and information would need to be updated, depending on the use that will be made of them.

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. In a crisis situation, a protection actor may feel under pressure to communicate findings that are not fully verified. When this happens, it is important to avoid reaching firm conclusions based on hasty extrapolation, or being overly affirmative. On the other hand, a lack of fully verified information is no reason for inaction when there are compelling reasons to suspect that violations have been committed and might be repeated.

Any internal or external report should mention the reliability and precision of its contents in general terms. Incidents that have not yet been verified or confirmed can be included in a report, as long as an honest estimate of the reliability and precision of the information is provided. Thus, transparency does not mean providing extensive details about the way information was collected; 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.

Protection data and information should be as detailed and as regularly updated as required; and they should be corroborated by different (primary and secondary) sources as appropriate,⁷⁰ and depending on the purpose of the data collection (see Standard 6.3 on a clearly defined, specific purpose). Tags may be used to identify the different levels of reliability of the information collected (individual incidents and other elements) – for instance, a secondary source report that hasn't been cross-checked yet, or for which no other source of information has been found, should be tagged “unverified” when recording it.

First-hand information provided by a clearly identified and trusted individual or organization during a face-to-face encounter is usually more reliable than that obtained from second- or third-hand sources. However, there is often a trade-off between accuracy and speed. Collecting first-hand and reliable information on the ground is costly, takes time, can be highly risky for everyone involved and is not always possible. Using crowdsourcing or other technologies in an intelligent and careful way to remotely collect and aggregate data from the field can be useful where presence in the field is either not possible at all or restricted. It can draw attention to specific areas, problems or patterns for further exploration. When organizations have established a strong field presence or a network of trusted and reliable sources, crowdsourcing can help corroborate data collected through other means.

⁷⁰ It is essential that the protection actor, when corroborating data, not commit a data breach by disclosing personal data or sensitive protection information.

When gaps in the quality of the information affect the protection response (owing to the limited reliability, precision or currency of the information, or because of other problems), protection actors should take the necessary remedial action. Actions may include redesigning information intake formats, clarifying terms in glossaries, or providing more general coaching and training on fact-finding, interviewing and information collection (see the PIM process above, which emphasizes the importance of evaluating both the data collection system and methods, the risks involved and the protection impact).

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 (see box below). Protection actors must therefore follow them when processing *personal data*. Where they are processing protection data and information that *do not include* personal data, as a matter of best practice, they *must* apply the same standards to the extent required by the particular sensitivity of the data.

Standard 6.3 (clearly defined, specific purpose), derived from the data protection principle of purpose specification, is in Section 1, as it applies to the entire information management process, and not only to personal data and information.

INTERNATIONALLY ACCEPTED BASIC PRINCIPLES OF DATA PROTECTION

Protection actors must apply the internationally accepted basic principles of data protection when processing personal data. These 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

(See Annex 2 below for the definition of each principle).

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.

Data protection legal frameworks must be taken into account by protection actors when processing personal data.⁷¹ Without adequate awareness of the applicable legal framework, protection actors may be prevented from collecting information, compelled to disclose it or face legal action by the State or the individuals concerned.⁷² Prior to collecting or processing data, protection actors must therefore assess the international, regional and national legal frameworks for data protection for their applicability.⁷³

The legal requirements may differ, depending on the protection actor concerned. International organizations usually enjoy diplomatic privileges and functional immunities under international law, which usually provides for the inviolability of the data and information processed by them. On the other hand, NGOs and private companies they contract, and private individuals, remain subject to the national jurisdiction of the country in which they operate and typically do not enjoy such privileges and immunities. They may therefore be required to hand over data to national authorities, in accordance with domestic law. This should be taken into account when assessing the risks associated with the sharing or transference of data and information between an international organization and an entity not enjoying privileges and immunities under international law (see Standard 6.16 on data sharing).

In order to ensure compliance with international law and consistency of practice across their operations, several agencies have adopted comprehensive data protection policies.⁷⁴ These can be useful sources of reference for other actors.

Therefore, before deciding to collect and/or store personal data or sensitive information in any given context, the protection actor must ascertain whether there are any specific contextual factors that might, at any stage, affect the safekeeping of the information collected. For example, it should be clear whether an organization could be forced to hand over information to the authorities – e.g. the police or the judiciary – based on domestic legislation related to, for example, the investigation of serious crimes, or international obligations related to money-laundering, terrorism, etc.

⁷¹ See Chapter 4.

⁷² Domestic or regional laws may contain provisions imposing the disclosure of confidential information, with a view to protecting public order and the rule of law – for example, in criminal cases. In such cases, the protection actor must adopt clear internal guidelines defining the types of data to be collected and the circumstances in which they will be shared, so as to avoid additional risks for both the victim and the actor involved.

⁷³ See also: United Nations, *Guidelines for the Regulation of Computerized Personal Data Files*, A/RES/45/95, 14 December 1990 – especially the “Humanitarian clause”, which calls for particular care and flexibility when applying data protection principles in the humanitarian sector; *International Standards on the Protection of Personal Data and Privacy*; OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 28 January 1981, in force 1 October 1985, ETS 108; 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.

⁷⁴ ICRC, *The ICRC and Data Protection*; UNHCR, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*, May 2015; International Organization for Migration, *Data Protection Manual*, 2010; World Food Programme, *WFP Guide to Personal Data Protection and Privacy*, 2016; Oxfam, *Oxfam Responsible Program Data Policy*, 2015.

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.

As shown in the box below, 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.

LEGITIMATE BASES

Internationally accepted legitimate bases include:

Consent of the person concerned or his/her legal guardian. Consent is the preferred legitimate basis for processing personal data. It must be specific, informed and free. Consent is discussed in further detail below.

Vital interest of the data subject or of another person. This refers to situations where the processing of personal data is necessary to protect the life, physical or mental integrity, health, dignity or security of the data subject or that of another person.

Example: Provision of life-saving assistance, where it may not be practicable to obtain the consent of a beneficiary, such as in the case of an unconscious person requiring urgent medical assistance, whose life and physical or mental integrity may be at stake.

Public interest, in particular in the implementation of protection activities, such as those grounded in the mandates of international organizations granted by the international community of States and enshrined in international law, and in the charters of NGOs.

Example: The right to know the fate of a missing relative is enshrined in IHL and IHRL, and activities to restore family links have been recognized as fulfilling an important public interest. Because it is not possible to obtain the consent of a missing person, protection actors may process personal data about a missing person to enable a relative who is searching for them to restore contact.

Legitimate interest of a protection actor – for example that of international organizations whose mandate is enshrined in international law, or of NGOs whose mandate is derived from national law.

Example: A protection actor may have a legitimate interest in processing personal data to the extent that is strictly necessary for the purpose of preventing or investigating fraud or theft in connection with relief items.

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.

In order for consent to be valid, it must be *informed* and *freely given*. Respect for the individual implies that each person is regarded as autonomous, independent and free to make their own choices. Before providing personal information about themselves or other individuals, or about specific incidents, a person must be given the opportunity to make an informed decision about whether or not to participate in the information collection process. Consent should seek to cover all of the processing activities planned for that data, including, in particular, any data sharing or transfer foreseen.

Protection actors should make sure that individuals have access to enough information on the purpose of the data collection, and the way in which the information they provide will be processed, in order to be able to give their informed consent to the use and possible disclosure of the data.

The person must also be given the opportunity to provide information while remaining anonymous, or to impose limitations on the consent – for example, restricting the sharing of information with certain other actors.

The person may deem some parts of the information provided to be confidential, and others not. For example, an individual may want information about recent violations at an IDP camp to be kept confidential if the perpetrators are still in the vicinity; but the same person may be less concerned if the event occurred some time ago or far from where they now reside. The specific circumstances in which information is provided will need to be assessed to determine the possible risks and mitigation measures to address them.

Informed consent should always be obtained in ways that are culturally appropriate and relevant. Collection of protection information should not take place until staff members have been trained, to ensure that the notion of informed consent is understood and respected. Appropriate efforts should be made to adequately communicate with individuals who may have difficulty in understanding the information that must be provided to them to secure their consent – for example by using different means, such as visual, audio and easy-to-read.

Details of the consent given and the level of confidentiality required should be documented or recorded and accompany the information throughout the information collection process. Where consent has not been requested, or has not been recorded, personal data must not be shared publicly or with a third party. In such instances, it is necessary to contact the person who provided the information and to obtain their consent prior to sharing their personal data.

If transmission⁷⁵ to a third party is intended, the data subject must be informed of the identity of the recipient (another protection actor, national or international judicial bodies, NGOs, National Red Cross or Red Crescent Societies, UN peace operations or other internationally mandated military and police forces, etc.) and when the information may be transmitted (if this can be reasonably determined). In addition, the data subject must be informed of what information will be transmitted and why. Before they are asked to give their consent to the transmission, the person concerned must be given a clear and readily understood explanation of the purpose of the transmission or sharing of information, as well as of the risks thereof and the precautions taken to mitigate them.⁷⁶

⁷⁵ See Standard 6.16 on data sharing.

⁷⁶ Other relevant questions that should be discussed include the following: What controls will be put on access to the information? How long is the information likely to be held and actively used? Is the information going to remain accessible for years or will it be deleted after some time? Finally, those providing information should also know whether they will be able to access the information they have provided, correct or delete it. This is discussed further, below.

INFORMED CONSENT

Informed consent is voluntarily and freely given based upon a clear appreciation and understanding of the facts, risks, implications and future consequences of an action.

“**Consent**” signifies the voluntary and freely given approval of the participant for the information to be used as explained. Consent is often given with limitations. It must therefore be clarified and recorded: for instance, how and which pieces of information can be used, including the identity of the participant, or whether the information may be used on condition that the identity of the participant be kept confidential.

“**Informed**” implies that the data subject must be put in a position to fully appreciate the risks and benefits of what they are consenting to, such as the processing of the personal data or protection information they are providing; consent acquired without doing this may not be considered valid. He or she must be given explanations in simple, jargon-free language. A certain minimum amount of information needs to be communicated to the source of information in order for consent to be regarded as being “informed”:

- The identity of the entity collecting the information, along with a brief explanation of the mandate of the organization collecting it.
- The purpose of the information collection exercise and its scope and method, and the intended use of the information collected (to present cases, to provide assistance, for statistical purposes, etc.).
- Details of the potential risks and benefits of participation in the process.
- Contact information so that the participant can get in touch with the entity collecting the information.
- Details on the duration for which the information will be used or stored, and how and where it will be kept (stored).
- With whom the data will be, or is likely to be, shared (if anyone at all; or when shared, in particular, with authorities: law enforcement authorities, non-State armed groups and *de facto* authorities, etc.) and whether the data will be shared across an international border.
- Reminders that the participant has certain rights: to cease participating at any time, to object to the processing of their data, to demand access to personal data, to demand corrections to data that they have provided and to demand that the information given be destroyed. (Note that these rights are subject to limitations. See Annex 3 below, on the rights of data subjects.)

Consent is therefore given in relation to analysis of the situation at a given moment. When major changes (the emergence of new or significant risks, for example) take place, it may no longer be regarded as valid and should therefore be obtained once again.

Alternative legitimate bases

In the situations in which protection actors usually operate, and within the context of sudden-onset or large-scale emergencies, it can be difficult to obtain informed and freely given consent, especially if consenting to the processing of personal data is a pre-condition for receiving protection assistance. Hence, it may be necessary to rely on alternative legitimate bases for processing personal data.

In some contexts, consent may not be meaningful or sufficient (for example, that of a very young unaccompanied child, a severely traumatized person, or a person whose vulnerability places them in a position where they have no other choice but to consent), or may not be obtainable (that of a missing person or an unconscious person requiring medical assistance, for example).

Consent may also not be meaningful when data processing is characterized by complex data flows using ICTs, when multiple stakeholders are involved, and when the susceptibility of data or information to interception and misuse is unclear or dependent on technical considerations, thus preventing a fully informed appreciation of the risks involved.

In these situations, the protection actor will require another legitimate basis to process personal data, such as the **vital interest** of the source of information or of another person, in case the processing of personal data is necessary to protect the life, physical or mental integrity, health, dignity or security of a person; or pursuant to the **public interest**.

Where consent is obtained from people in positions of authority (community leaders, village elders, etc.), the individual consent of each group member should nevertheless also be sought. If it is not feasible to obtain individual consent from the whole group, another legitimate basis will be required in order to process an individual's personal data.

Finally, obtaining the necessary individual and informed consent does not absolve an actor from his/her responsibility to assess and mitigate the risks for an individual or a given group that are associated with processing personal data or protection information.⁷⁷ If the protection actor determines that the risks are excessive and not warranted by the intended protection outcome, the information should not be processed, even if informed consent has been obtained.

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 moment of the collection, subject to the prevailing security and access conditions and the urgency of the processing. Any information and communication relating to the processing of personal data should be easily accessible and easy to understand; translations should be provided where necessary, and clear and plain language should be used.

Information – for example, in the form of an informed consent form or an information notice – should be provided prior to or at the time of data collection.⁷⁸ See the box above, on informed consent, for guidance on the information to be provided.

⁷⁷ See standard 6.18 on assessing risks.

⁷⁸ See Standard 6.9 on the information that must be provided to obtain informed consent.

Data minimization



6.11. Protection data and information must be adequate and relevant to the clearly defined, specific purposes⁷⁹ for which they are collected and processed. This means that the data processed must not exceed the purpose(s) for which they were 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. This principle is particularly important within the context of inter-agency coordination and of cross-functional needs assessments conducted by humanitarian organizations, where protection actors are at risk of gathering excessive amounts of data (for example, by conducting surveys with up to several hundred data fields, which may or may not be used at a later stage). In these situations, it is important for the protection actor to be able to distinguish between what *might be interesting* and what is *necessary to know* in order to achieve the defined purpose.

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 purposes for which they were collected or for other compatible purposes
- it is found that the purpose for which they were collected can no longer be achieved
- the individuals concerned/their guardians withdraw their consent or object to further use of it
- the individuals concerned object to its use and their objections are upheld by the protection actor or an independent body
- applicable data protection legislation or the regulations of the organization concerned provide for deletion.

⁷⁹ See Standard 6.3 on clearly defined, specific purposes.

However, personal data may not be deleted when there is a legitimate reason for archiving them: for instance, the data may be necessary for ensuring long-term provision of protection services, for historical, statistical or scientific purposes, or for accountability. In some cases, it may be enough to retain only data that have been anonymized.

EXAMPLE: LEGITIMATE REASONS FOR ARCHIVING PERSONAL DATA

The ICRC archives collect and preserve ICRC documents dating from the organization's inception to the present day, and make them available for research. The archives cover a number of important historical events from 1870 on, as well as data on individuals that the ICRC and its tracing agencies have collected in the course of their humanitarian work in armed conflicts and other situations of violence. The data were all collected as part of the ICRC's efforts to restore family links and to protect prisoners of war, civilian internees and victims of war. The ICRC archives are an essential resource for historical and genealogical research in certain areas. Often, enquiries related to this type of research are raised many years after the data were first collected; in addition, requests for personal data are made by the persons concerned or their relatives, either for administrative reasons (obtaining pension rights in some countries, indemnities related to conflict, death certificates, etc.), or purely out of the human need for memory and for coming to terms with history. Therefore, in certain circumstances, the ICRC retains personal data relating to persons to whom it has provided protection and assistance, beyond the time strictly required to provide such protection and assistance.

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.

Security safeguards, appropriate to the sensitivity of the information, must be in place prior to any collection of information – to ensure protection from loss or theft, unauthorized access, disclosure, copying, use or modification – whatever the format in which the data are kept or transferred, paying particular attention to security threats inherent to ICTs.

The primary objective of data security is to mitigate the risk of unintended third parties gaining access to data processed by protection actors, which may result in harm to the persons and communities on whose behalf protection actors are working.

Therefore, the protection actor (and any other responsible entity and processing service provider working on their behalf) must protect the data that is being processed with the appropriate legal, technical and organizational measures and ensure, at all times, their integrity, confidentiality and availability. These measures depend on the existing risk, the possible consequences to the persons concerned, the sensitivity of the data, the context in which the processing is being carried out and, where appropriate, the obligations contained in the applicable national legislation.

The transfer of personal data and sensitive information (from one office to another of the same organization, or to another protection actor, for instance) must also be done by the safest means possible, using the appropriate tools (encryption, for example).

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 it is not able to mitigate the risks to data security.

Data security is thus a crucial component of an effective data protection system. Personal data and sensitive information must be processed in a manner that ensures appropriate security, including the prevention of unauthorized access and use. Data security relates, in particular, to access rights to databases, physical security, computer security or cyber security, the duty of discretion, and the conduct of staff and their awareness of general data security rules. It also entails the secure destruction or anonymization of personal data and backups, when retaining them is no longer necessary.

In order to ensure and maintain appropriate data security, protection actors are required to evaluate the specific risks associated with the processing, and to implement the organizational and technical measures necessary to mitigate those risks and ensure that data are protected from unauthorized access, theft, damage and loss throughout the data and information management process. These measures should ensure an appropriate level of security (taking into account available technology, prevailing security and logistical conditions and the costs of implementation) in relation to the risks and the nature of the data and information to be protected.

These measures may include⁸⁰ the taking of steps related to the following:

- staff training
- office security
- management of individual access rights to databases containing personal data
- safeguards for the intended use of the data/information (e.g. consent)
- clearly defined staff roles and responsibilities
- physical security of databases
- file management
- IT security
- discretion clauses in employment and internship contracts or professional codes of conduct
- quality control mechanisms
- internal procedures for supervising the implementation of security measures
- delays and methods of destruction of personal data.

The objective of these measures is to ensure that personal data and sensitive information are kept secure, both technically and organizationally, and protected by reasonable and appropriate measures against unauthorized modification, copying, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer.

⁸⁰ For more guidance, see the Brussels Privacy Hub/ICRC [Handbook on Data Protection in Humanitarian Action](#), 2017.

Some basic steps can be taken to improve data security. For instance, it may be necessary to blunt the precision of some data (of incidents or of interviews with victims, and concerning time and location) or reduce their granularity⁸¹ (number of persons interviewed, area affected by a certain issue) in order to ensure that a data set does not inadvertently reveal the actual location of at-risk individuals or groups.

Data security measures may vary, depending on the following elements:

- type of protection activity
- nature and sensitivity of the data
- form or format of storage
- environment/location of the specific personal data
- prevailing security and logistical conditions (including the estimated surveillance capabilities of the different parties to a conflict or other situation of violence).

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.

Protection actors may also need to increase their knowledge of digital security and efforts as they digitize more of their data and communications. They should be aware that new technologies are highly susceptible to interception and vulnerable to security breaches; they should also know of the specific risks involved with the tools they use, with regard to both the intrinsic strengths and weaknesses of each tool and in terms of their use in a specific context. If they do not have sufficient knowledge of ICTs to identify such risks, they should seek professional advice from specialists when setting up procedures involving electronic collection, storage or transmission of data. However, they should, for the long term, build up professional capacities in this area within their organizations, thereby also fostering sustained dialogue between protection specialists and ICT and information security staff.

To strengthen compliance with data security procedures within an organization, monitoring mechanisms and corrective measures should be put in place to deal with data security breaches and mitigate their impact. Furthermore, any 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 should be reported, if possible and deemed appropriate, to the persons affected by the data breach, in particular when the data breach puts them at risk.

Confidentiality



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 and as long as the disclosure of the data may place the person or another individual or a community at risk. This obligation to respect the confidentiality of personal data therefore remains, even after the person concerned is no longer receiving specific services or attention from the protection actor.

⁸¹ For more guidance on this subject, see the Brussels Privacy Hub/ICRC [Handbook on Data Protection in Humanitarian Action](#), 2017, section 2.3 on aggregate, pseudonymized and anonymized data sets.

Sharing, transferring and publishing

Protection actors increasingly work in partnership and seek to ensure complementarity with other sectors while avoiding duplication (see Chapter 5). The sharing and transfer⁸² of **personal data** and sensitive information, among protection actors and with third parties (including across borders), is therefore a routine operational requirement in protection activities, essential to ensure an effective, timely and collaborative response to the needs of the populations affected and to the protection threats they face.

However, the need to share information must be balanced with the need to protect the privacy, well-being and security of populations affected, and with the “do no harm” principle. Protection actors should transfer or share information only if it serves a protection purpose and if there is a legitimate basis for doing so.⁸³ Transferring, sharing or publishing personal data and sensitive protection data and information, must be done in a safe and responsible manner. Since data sharing is a form of data processing, it requires paying due regard to all the standards listed in this chapter.

Furthermore, most national data protection laws place restrictions on the sharing of personal data with third parties, in particular across national borders. Some national legislation even restricts the sharing of personal data outside the country where the data were originally collected or processed, even if the data are to be transferred to an office of the same protection actor in another country.⁸⁴

The following steps should be followed when transferring personal data and sensitive information internationally:

- All applicable data protection rules or privacy requirements (including all applicable local legal data protection or privacy requirements⁸⁵) should be satisfied prior to the transfer.
- It must be confirmed or verified that there is a legitimate basis for the transfer.
- A risk assessment (such as a Data Protection Impact Assessment (DPIA – see below)) should be carried out prior to the transfer to confirm that the transfer does not present unacceptable risks for the individual concerned.
- The protection actor initiating the transfer must be able to demonstrate that adequate measures have been undertaken to ensure compliance by the recipient entity with the principles of data protection (outlined in these professional standards) in order to maintain the proper level of protection of data.
- The person whose personal data are being transferred should be informed about the recipient(s) of the transfer and given an opportunity to either consent or object to the transfer.
- The data must be transferred using appropriate safety measures, such as encryption, to protect against interception and unauthorized access.

⁸² The term “data transfer” is to be broadly construed: it includes any act that makes personal data accessible to others or any method used to share data – whether on paper or via electronic means or the internet.

⁸³ See Standard 6.9.

⁸⁴ Further guidance on the conditions for international data sharing may be found in the Brussels Privacy Hub/ICRC *Handbook on Data Protection in Humanitarian Action*, 2017.

⁸⁵ Many countries in all regions of the world have enacted data protection laws that regulate the international transfer of personal data. In order to determine whether any local laws apply to the transfer, the protection actor should consult with its legal and/or data protection departments.



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

As there is a very high risk of causing harm if personal data or sensitive protection data and information are mismanaged, protection actors must ensure that data are transferred to or shared with only those entities that offer the required level of data security and protection. They must also ensure that the actual transfer is done through the safest means possible, using security measures such as encryption, as needed.

When transmitting sensitive data electronically, the security of the system should be evaluated and regularly updated. A risk assessment (such as a DPIA) must be undertaken and mitigating measures put in place prior to deciding whether to share, transfer or publish data. The use of data sharing agreements or information sharing protocols between protection actors is also considered good practice, so as to ensure that all the necessary safeguards have been considered, and that data and information are handled in a confidential manner.

Protection actors must also take measures to ensure that the sharing of personal data and sensitive protection 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.

Organizations using public advocacy and campaigning as a protection activity may feature articles about persons affected and case studies to mobilize public opinion and action, particularly through their websites and in media work. In doing so, their own staff, including photographers and film-makers commissioned to collect such information on the ground, should adhere to the professional standards listed here. They must not publish personal data (including photographs) of individuals, unless the person has given their informed consent or there is some other legitimate basis for doing so.

When sharing non-personal data, such as aggregated or statistical data, or general protection information about a situation, protection actors should also take the following precautions:

- Prioritize protection outcomes, and the safety and well-being of the persons or populations concerned.
- Be transparent about the accuracy and reliability of the information and/or data provided, so as to minimize the risk of presenting an incorrect or incomplete image of the issues they intend to address (see Guideline 6.7).
- Always consider the sensitivities of or the potential risks for the persons (individuals or communities) whose data are shared (even if informed consent has been provided).
- Consider – when sharing aggregate or statistical data – whether the sample is sufficiently large or the granularity of data is sufficient to provide meaningful and accurate statistics and/or descriptions of trends, and whether there is any risk of individuals and communities being identified from the sample alone or in combination with other data/information, and being adversely affected as a consequence.

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, monitoring of quality and supervisory mechanisms.

The principle of accountability is premised on the responsibility of protection actors who process data⁸⁶ to comply with the standards set out in this section, and with the applicable legislation. Protection actors must be in a position to demonstrate that adequate and proportionate measures have been undertaken within their respective organizations to ensure compliance, and to prevent the harm that may result from unauthorized access.

Ensuring accountability for the appropriate processing of personal data and sensitive protection information therefore means ensuring compliance with the professional standards contained in this chapter.

Protection actors may implement various measures that can help them meet this data protection requirement, such as: internal policies, guidelines and instructions, standard operating procedures, supervisory structures, training, monitoring mechanisms, the carrying out of DPIAs. Accountability mechanisms may also include internal data protection policies, codes of conduct, certification schemes, records of processing activities and disciplinary measures.

These procedures are especially useful for ensuring the relevance and quality of information, and accountability in its use, and for defining security rules. As a minimum, they should:

- incorporate, from the outset, key elements linked to preparation for data collection, particularly with respect to informed consent, privacy, transmissibility and restriction of access. This is of critical importance in emergency situations, where staff turnover is often high, and especially when institutional memory is limited
- define access rights and clarify the obligations of staff handling data and what they are authorized to do, and what they are not permitted to do
- set out the conditions for use and onward sharing
- set out the security safeguards
- clarify rules and timelines for archiving and/or destroying data
- clarify how confidential information will be securely stored.

The need for clear procedures applies whatever the tools, methodologies and technologies used to collect data, including crowdsourcing.

A protection actor is also accountable when it subcontracts information collection or processing, including to partners, private companies, research institutions or the communities themselves. The protection actor remains responsible for ensuring that subcontractors apply the required standards at every step of data processing.

⁸⁶ An actor engaged in this task is usually referred to as the data controller: the natural or legal person or the entity, which, alone or jointly with others, determines the purposes and means of processing personal data. When these professional standards are applied, the protection actor will, in most instances, be the data controller.

SECTION 3 – ASSESSING THE RISKS

As emphasized above, protection actors have an obligation to take all feasible measures to reduce the risk of harm to persons from whom or about whom data are collected. This includes making every effort to prevent or mitigate any harm to those persons resulting from third parties' access to data and information. 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; and 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.⁸⁷

While the decision to provide information rests with the person who is being requested to provide it, the protection actor collecting the personal data or sensitive protection data and information is responsible for assessing and mitigating, to the extent possible, all of the associated risks. This means that the protection actor must also regularly review the risks associated with collecting, analysing, sharing, transmitting, releasing or storing data or information. Any residual risk associated with the data processing should be proportionate to the intended protection outcome.

The protection actor also bears responsibility for assessing the risks of using or replicating personal data or sensitive protection information that has been made public by other entities or individuals, including that which is available online, including on social networks and blogging platforms. It is important to note that a protection actor using personal data or sensitive protection data and information from other sources, including online sources, is accountable for the consequences of processing that data and information.

For example, the fact that first-hand accounts from rape survivors or other survivors of abuse, naming victims and/or witnesses, have been made public or circulated to different protection actors does not mean that these accounts can be freely replicated and used. Any protection actor who wants to use this data must, in particular, carry out a risk assessment and ensure that they have a legitimate basis for doing so.

The mere fact of having been in contact with a protection actor can sometimes be a source of risk. Protection actors must therefore, before starting to collect data, identify the risks associated with the different data-collection methodologies and tools (face-to-face interview, focus group, interview via phone or other remote technology, etc.), both for those providing information and those collecting it.

In analysing these risks it is necessary to determine what constitutes particularly sensitive information in a given context, the possible threats to information management, including theft and leakage, and whether sensitive information could be seized by the authorities or others.

⁸⁷ This standard is closely related to various standards set out in Section 2 of the present chapter, such as 6.14 (data security), 6.15 (confidentiality) and 6.16 (which requires that data be transferred to or shared with only those recipients who offer the required level of data security and protection).

Assessing the risks for victims, witnesses and other sources at each stage of the information management process requires dialogue with the persons concerned and raising awareness among them about perceptions of risk.

Having identified potential risks, precautions need to be taken and procedural mechanisms put in place to minimize the risk of adverse outcomes. These measures might include the following:

- conducting interviews in a neutral place, shielded from public curiosity, and in the absence of persons who might exert pressure or intimidation of any kind
- being absolutely transparent about the purpose, the processing procedures and the use of the information (Standard 6.10)
- using methods of transmitting information that conceal the sources of information, the identities of victims and dates and/or places
- deferring interviews with sources and witnesses until they are no longer within reach of those who might seek to harm them, or using alternative methods to collect data
- strictly applying the rules of data protection and confidentiality at all stages of the data processing
- making follow-up visits to or contact with informants, in order to ensure that they have not suffered reprisals or been exposed to additional risks, or been burdened in any other way because they provided information.

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.

ASSESSING THE RISKS – PRELIMINARY ANALYSIS AND DPIAS

In assessing the risks, a preliminary analysis should be done. It should include the following:

1. Evaluating the context and defining what protection data and information are needed for a specific purpose, and identifying the intended benefits.
2. Assessing what data and information already exist/are available, including from other sources. This is often referred to as a “secondary data review”.
3. Assessing the potential and actual risks of collecting, analysing, sharing and using the data and information, and identifying mitigatory measures. This is often referred to as a “risk assessment”, a “risk analysis” or a “data protection impact assessment” (DPIA).
4. Assessing what core competencies are required to implement a specific data processing activity, and proceeding only if those competencies are available.

For stage 3, a DPIA is one of the methodologies that can be used. It provides a structured methodology to identify, assess and evaluate the origin, nature, significance and severity of the data protection risks, the likelihood or probability of the realization of a certain risk, and its consequences (i.e. its impact). It helps the protection actor identify and implement the mitigatory measures necessary to correct, avoid or minimize the adverse consequences foreseen, both to persons concerned and the protection actor, including that actor’s project, policy, programme or service.

A DPIA should be undertaken during the planning and design stages of new data processing initiatives, but it can also be used to assess and mitigate the data protection risks arising from projects already in progress.

The following are some situations where it may be appropriate to consider conducting a DPIA:

- When a protection actor is introducing information communication tools, methodologies or data processing platforms, including interoperable or shared databases with other organizations that involve inherent privacy risks.
- New initiatives or areas of activity that involve the use or transfer of, or access to, personal data or sensitive protection data and information, taking into consideration the local culture and specific operational context. The collection or use of data from a minority group could, for example, expose them to additional risk of harm. Human rights investigations, like commissions of inquiry, also involve the collection of sensitive information that can endanger those providing information.
- The use of a cloud-based storage system to store a protection actor's data and information. The DPIA should consider where the cloud and any backups are located, the risks of unauthorized intrusion into the data stored in the cloud, or of requests for data made by authorities to the cloud service provider.

Examples:

- A local NGO or authority approaches a humanitarian organization, saying that it wants to reunite families separated by violence in the country. It wants the humanitarian organization to supply all the information it has on missing persons in the country. The DPIA should consider whether the information should be shared and, if so, how much personal information should be shared in order to trace missing persons. It should also consider the impact of and possible safeguards for sharing personal data with a host government.
- A tsunami sweeps away dozens of coastal villages. Thousands are reported missing. The DPIA might consider how much personal information the protection actor should collect from the families of persons unaccounted for, whether it should include information, the disclosure of which could cause significant harm to individuals, such as health-related or genetic data, religious affiliation or political views.
- A protection actor is considering publishing pictures of missing unaccompanied children on the internet or releasing the details of emblematic cases of violations of human rights in a public report. A DPIA should consider the respective risks of publishing the pictures online or of circulating them through printed posters (it may be easy for others to copy the online photos and make unauthorized use of them, while printed posters may be less susceptible to replication) and the risk of anonymously given information being easily traced back to their sources owing to small sample size.

Collecting information through the internet: Assessing risks and ensuring compliance with other standards

A DPIA helps identify all the questions that must be answered in order to analyse and manage the risks. In the specific case of collecting information via the internet, questions to ask might include the following:

- Is it possible to trace the information back to its original source?
- Could the information be used for intelligence purposes in military or police operations, or by any ill-intentioned third party?
- Are the means of communication used secure enough to enable the transmission of personal or sensitive data?
- Are there clearly formulated protocols to deal with the sensitive data collected?

- Are non-public parts of a website or offline site secured against loss, theft or misuse of the personal or sensitive data collected or stored on them?
- What data and information can be published or shared with partners without endangering the individuals concerned or showing disregard for their consent?
- Is there a risk to the protection actor itself, especially as regards its capacity to gain or maintain field access?
- Would making some information accessible on the internet result in long-term risk, considering the longevity of online data?

In order to provide individuals with the information necessary to enable them to assess the risks they are taking in providing personal or sensitive protection information through a website, the protection actor should be transparent and explain in simple terms and appropriate language:

- its identity
- the purpose of the website
- how the information will be used/processed and, notably, with whom it may be shared (even partially), and how personal data can be modified or deleted, if required
- the potential risks and the precautions taken to mitigate them.

These steps are necessary to ensure transparency of the purpose of the information collection. They will also help address the issue of informed consent when there is no direct contact between protection actors and the people providing the information.

Although good practices do exist, such as incorporating filters in the information that is openly shared or otherwise rendering data anonymous, when needed, an in-depth contextual understanding of the risks is required. Checking risks with persons or organizations knowledgeable of and, whenever feasible, present in the specific context is therefore essential before deciding to collect information from afar through a website. Protection actors should, in this context, be aware that even anonymized data sets can, in certain situations, put persons or communities at risk. They should understand and manage these risks. For example, they can adapt the way they display information publicly.

Measures to mitigate risks may include technical solutions, operational and/or organizational controls, and/or communication strategies (e.g. to raise awareness and to educate). It is important to stress that risks are context-specific. While it may not be possible to mitigate all of the risks identified through a DPIA, what is important is that the protection actor consider the risks, mitigate these to the extent possible and arrive at an informed decision, in the interest of the persons it is engaging with, as to how best to proceed (or not to proceed at all if the protection actor is not satisfied that the risks involved in the data processing will exceed its intended benefits). A DPIA report should include recommendations on the actions to be taken; it may also be appropriate to provide for a future review or update of the DPIA.

ANNEXES TO CHAPTER 6

ANNEX 1: RISKS AND ADVANTAGES OF DIFFERENT METHODOLOGIES AND TECHNOLOGIES

Use of the internet or mobile-phone networks

Protection actors setting up systematic information collection through the internet or mobile-phone networks (SMS) must analyse the different potential risks linked to the collection, sharing or public display of the information and adapt the way they collect, manage and share or publish the information accordingly.

The information posted on a publicly accessible website can prove extremely sensitive and can result in risks to the provider of the information, or the people mentioned therein. Posting a compilation of text messages online in “real time” may reveal, for instance, the location of a women’s refuge that was previously kept confidential, endangering the women sheltering there. Managing the risks when setting up such systems poses certain challenges that protection actors must incorporate in their risk and mitigation assessments. Similarly, the processing, aggregation and publication of information already in the public domain (e.g. tweets and other social-media posts) can create risks that were not foreseen by the original authors of the posts.

If the information is collected and/or transmitted through mobile-phone networks or the internet, protection actors should evaluate the possibility of the authorities or others being able (legally or otherwise) to intercept the information or to force providers of mobile-phone connections or internet services to hand over some of the data and metadata they manage and store as part of their services.

Aerial and satellite imagery

Access to aerial and satellite imagery for humanitarian and human rights purposes has greatly expanded over the past decade, as the number of providers has risen and costs have fallen, in particular with the rapid expansion of the use of civilian drones (or unmanned aerial vehicles). Aerial and satellite imagery can contribute to a better understanding of a particular situation on the ground, provide photographic evidence to corroborate witness accounts of violations, provide indications of the extent of protection needs, monitor displacement trends, estimate the extent of the destruction of civilian infrastructure and housing, confirm the presence of mass graves and detention centres, and identify the precise location of armed actors. Sequenced, time-stamped images can also provide a timeline of events, which may be of use in establishing a chronology of events.

Protection actors should take particular care when using, sharing and making aerial or satellite imagery publicly available, in particular during periods of ongoing violence or in the context of armed conflict, as it may be used to target particular populations or otherwise put them at risk.

Crowdsourcing and crisis-mapping platforms

Crowdsourcing, which has been made possible by the wide availability of internet services and mobile-phone data networks, relies on a participative approach that allows an organization to call on the general public or members of a volunteer community to contribute to the collection or analysis and processing of data and information, without

direct face-to-face contact. Since 2008, crowdsourcing has been used to monitor trends of incidents and abuses in a number of crises, as it can be an extremely efficient way to collect data on ongoing violence, violations and abuse, and their consequences for individuals and communities. Numerous crowdsourcing and crisis-mapping initiatives are accessible via the internet.

The remote nature of crowdsourcing may give rise to particular challenges. The volunteers, or those managing the network, may not be fully aware of the situation on the ground and of the possible risks for the population. Nevertheless, it is essential to ensure compliance with the standards outlined in this chapter. In particular, whenever a crowdsourcing initiative is launched, identifying and limiting the risks faced by those participating in it, or by those about whom data are collected and processed, is an imperative. Those involved should also pay special attention to protecting data and information concerning children and other vulnerable persons, including their identities and details about their location.

Photographs and other visual data

Visual data include photographs and video footage as well as other recognizable visual representations of individuals (e.g. courtroom sketches). Visual data are particularly compelling and can be used in a wide variety of ways for protection outcomes. Many protection actors collect and retain visual data for several years on databases for use on their websites, in fundraising materials and reports, and on social media. Given the power of visual images, photographs and other images may also be specifically collected by a protection actor to draw attention to their protection work, including for public advocacy and campaigning, and to raise public awareness of the situation, in specific contexts, of populations affected.

When collecting and processing visual data, protection actors remain responsible for assessing and managing the risks to the individuals and communities portrayed in or identifiable from them, and must process the visual data in line with the standards presented here; they must also ensure that all those collecting visual data on their behalf do so as well. This means that protection actors must have a specific purpose and a legitimate basis for processing the data, and should seek the informed consent of individuals depicted in them prior to using them. People who are unfamiliar with digital technology and the internet may not fully appreciate how their images may be used and transmitted, and may also fail to appreciate how little control a protection actor has over such content once it is published or placed online.

Visual data take many forms and the level of risk to individuals portrayed may vary. For example, a photograph of a crowd differs from the portrait of an individual; likewise, video footage of a specific individual speaking on camera about their situation may require higher levels of vigilance and risk management.

Particular care should be taken when recording images on an electronic device such as a smartphone or a digital camera, as metadata embedded in images may be retrieved by third parties. Such metadata could include GPS data identifying the specific location where the picture was taken.

The risks resulting from the juxtaposition of images of individuals or groups with text (including captions) should also be assessed in an appropriate manner. Images must be stored securely in line with procedures for other sensitive personal data. Images and other visual data must not be edited in a misleading manner. Once an image is associated with a specific narrative or type of information, that narrative will define how those portrayed in the images are viewed. For example, using an image of a child

alongside an article about child soldiers will imply that the child is or has been a child soldier. Women whose images are used to illustrate a campaign about sexual violence will be assumed to be survivors of such abuses themselves.

Stock images used for protection purposes – to illustrate a story about the protection situation of individuals, for example – should also be treated with the same due diligence and the same safeguards must be applied as for those images collected specifically for protection purposes.

In addition to complying with the professional standards presented here, protection actors collecting visual data from people in armed conflict and crisis situations should develop internal guidelines on ethical and safety standards, and efforts should be made to foster a culture of responsible data use among humanitarian and human rights actors.

ANNEX 2: INTERNATIONALLY ACCEPTED BASIC PRINCIPLES OF DATA PROTECTION

Protection actors must apply the internationally accepted basic principles of data protection when processing personal data. These principles, adapted from the Madrid Resolution, may be summarized as follows:

Lawful and fair processing

Fair processing of personal data entails respecting the applicable legislation as well as the rights and freedoms of individuals, in conformity with the purposes and principles of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. In particular, processing of personal data that gives rise to discrimination is unfair.

Purpose specification

The processing of personal data must be limited to the fulfilment of a specific, explicit and legitimate purpose. Processing that is not compatible with the purposes for which the personal data were collected must not be carried out, unless the unambiguous consent of the person concerned is obtained.

General principle of legitimacy

Personal data must be processed only after obtaining the free, unambiguous and informed consent of the person concerned, or if there is another legitimate basis that justifies the processing.

Data minimization and proportionality

The processing of personal data must be limited to such processing as is adequate, relevant and not excessive in relation to the specific purpose for which the data were collected. In particular, the amount of personal data processed must be limited to the minimum necessary.

Data quality

The person in charge should ensure at all times that personal data are accurate, as well as sufficiently detailed, and kept up to date in such a way as to fulfil the purposes for which they are being processed. Personal data must be as accurate and up-to-date as possible; inaccurate personal data must be corrected or deleted without undue delay. To ensure that personal data are not kept longer than necessary, a minimum retention period must be set, at the end of which a review should be carried out to determine whether the retention period should be extended or the data destroyed, anonymized or archived.

Transparency and information

Protection actors must have transparent policies with regard to the processing of personal data. They must provide to the data subjects, as a minimum, information about their identity and mandate, the intended purpose of the processing, the recipients to whom their personal data will be disclosed and how data subjects may exercise their rights, as well as any further information necessary to guarantee fair processing of such personal data. When personal data are collected directly from the data subject, this information must be provided at the time of collection.

Data security

The person in charge, and any processing service provider involved, must protect the personal data that are subject to processing with the appropriate technical and organizational measures to ensure, at all times, their integrity, confidentiality and availability. The nature of these measures will be determined by the existing risk, the possible

consequences to data subjects, the sensitive nature of the personal data, the state of the art, the context in which the processing is carried out and, where appropriate, the obligations contained in the applicable national legislation. Data subjects should be informed of any security breach that could significantly affect their pecuniary or non-pecuniary rights, as well as the measures taken for its resolution; this information should be provided in good time – by those involved in processing the data – in order to enable data subjects to seek the protection of their rights.

Duty of confidentiality

The person in charge, and those with any degree of involvement in the processing, should maintain the confidentiality of personal data. This obligation will remain even after the relationship with the data subject – or, when that is the case, with the person in charge – has ended.

International transfers and sharing of data

As a general rule, international transfers of personal data may be carried out when the recipient entity affords, as a minimum, the level of protection provided for in the data protection principles mentioned previously. It will be possible to carry out international transfers of personal data to entities that do not afford the level of protection provided for in these data protection principles where those who expect to transmit such data guarantee that the recipient will afford such level of protection; such guarantees may, for example, take the form of contractual clauses. Where the transfer is carried out within an organization, such guarantees may be contained in internal privacy rules, compliance with which is mandatory. Moreover, national legislation applicable to those who expect to transmit data may permit an international transfer of personal data to entities that do not afford the requisite level of protection, where necessary and in the interest of the data subject within the framework of a contractual relationship, to protect the vital interests of the data subject or of another person, or when legally required on important public-interest grounds.

Applicable national legislation may confer powers on the supervisory authorities to authorize some or all of the international transfers falling within their jurisdiction, before they are carried out. In any case, those who expect to carry out an international transfer of personal data should be capable of demonstrating that the transfer complies with the requisite guarantees, particularly where this is required by the supervisory authorities.

Accountability

The principle of accountability requires observance of the principles mentioned above, and of the pertinent obligations and applicable legislation; it also requires parties concerned to demonstrate that adequate and proportionate measures have been undertaken to ensure compliance with these principles, obligations and laws.

Rights of data subjects

The data subject has the right to demand, from the protection actor concerned, **information** on and **access** to the specific personal data subject to processing, as well as the source of such data, the purposes of processing and the recipients or categories of recipient to whom such data are or will be disclosed. Any information to be furnished to the data subject must be provided in an intelligible form, using clear and simple language.

In addition, the data subject has the right to demand that the person in charge **delete** or **correct** personal data that might be incomplete, inaccurate, unnecessary or excessive. Where justified, the person in charge should carry out the correction or deletion requested. In this connection, the person in charge should also notify third parties to whom personal data had been disclosed, where they are known. Deletion of per-

sonal data is not justified where such data must be retained for meeting an obligation imposed on the person in charge by the applicable national legislation, or by the contractual relationship between the person in charge and the data subject.

The data subject may also **object** to the processing of personal data where there is a legitimate reason related to their personal situation. The exercise of this right to object is not justified where the processing is necessary for the performance of a duty imposed on the person in charge by the applicable national legislation. Data subjects may also object to those decisions that produce legal effects based solely on automated processing of personal data, except when such decisions have been specifically requested by them or when it is necessary for the establishment, maintenance or conduct of a legal relationship between the person in charge and the data subject. In the latter case, the data subject must be able to explain and defend their position, to have some kind of fair hearing, in order to defend their right or interest.

For further detailed information, please refer to the Brussels Privacy Hub/ICRC *Handbook on Data Protection in Humanitarian Action*.

ANNEX 3: RIGHTS OF DATA SUBJECTS

In addition to the principles, a key element of data protection is respecting the rights of data subjects. These rights include the following:

- The right to **be informed** about key aspects of the processing of personal data, including the purpose for which data are processed.
- The right to **object**, on compelling legitimate grounds relating to their particular situation, at any time, to the processing of personal data concerning them.
- The right to **access** and verify their personal data, which they can ask to do through an oral or written request, to the relevant protection actor.
- The right to **correct** personal data relating to them that are inaccurate or incomplete, including by means of providing supplementary information.
- The right to have their personal data **erased** from the relevant actor's databases when:
 - the data are no longer necessary in relation to the purposes for which they were collected or further processed
 - the data subject has withdrawn their consent for processing, and there
 - is no other basis for the processing of the data or
 - the processing does not comply with the applicable data protection and privacy laws, regulations and policies.

It should be possible for an individual to exercise these rights using the internal procedures of the relevant organization, such as by lodging an enquiry or complaint with the relevant staff/office. Depending on the applicable law, the individual may also have the right to bring a claim in court or with a national data protection authority. In the case of international organizations enjoying privileges and immunities from jurisdiction, claims may be brought before an equivalent body responsible for independent review of cases involving the organization.

Notwithstanding the above, the exercise of these rights is subject to certain conditions and may be limited. In particular, an organization with a mandate enshrined in international law may restrict the right to access personal data in order to implement its mandate and operate in emergencies.

ANNEX 4: 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.

Detle, 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).



CHAPTER 7

ENSURING PROFESSIONAL CAPACITIES

Ensuring relevant capacities and competencies

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

Staff training

- S** 7.3. Protection actors must ensure that their staff are adequately trained and have the requisite expertise and capacities.
- S** 7.4. Protection actors must keep themselves informed of and adopt, as appropriate, current practices and guidelines of relevance to their protection activities.

Managing staff safety

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

Ensuring professional and ethical conduct by staff

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

This chapter deals with the internal processes, competencies and capacities necessary for humanitarian and human rights actors doing protection work in armed conflict and other situations of violence.

Its first part underscores the importance of ensuring congruence between the stated intentions of a protection actor and its capacity to deliver. To achieve that, a protection actor must be able to define intentions and plans for their realization, ensure the requisite means and then implement the plans. While the mandates and mission statements of protection actors articulate broad organizational goals, operational objectives and plans of action define more specific commitments in a given operational context. However, for these planning tools to be relevant, the protection actor must have the capacity and expertise to deliver – in real terms – on the commitments they make. This chapter insists on the necessity of ensuring adequate human resources.

Increasingly, protection actors operate using transnational structures. This requires them to ensure consistency of approach and coherence across these structures in all the locations where they operate, and implement protection activities.

The second part of this chapter looks at the possible implications for staff management when engaging in protection work. It outlines the essential support any organization must provide to its staff, including training, developing best practices, managing security and clarifying the conduct expected.

ENSURING RELEVANT CAPACITIES AND COMPETENCIES

S

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. Seeking to persuade the authorities to fulfil their responsibilities, through advocacy or bilateral dialogue, can be a sensitive matter and technically demanding. The results of protection work frequently depend on the accuracy of the problem analysis, the precision of subsequent evidence-based advocacy and the consistency of the particular organization's practice. Those responsible for providing technical advice, or for implementing protection activities, must be versed in the relevant concepts, approaches and methodologies of protection work, and familiar with the applicable legal frameworks, including IHRL and IHL. They must also have the capacity to work under various operational and security constraints.

Protection work is becoming increasingly diversified, with evolving specializations. Accurate analysis and effective response to the particular protection needs of populations at risk requires different types of expertise – for instance, in: penal and judicial sector reform; preventing and responding to sexual and gender-based violence and other human rights violations or abuses; tracing people unaccounted for and restoring family links; protecting personal data; addressing housing, land and property claims and ensuring effective remedies. A range of skills in the following fields is required: communication; fact-finding; interviewing; intercultural dialogue; writing, editing and formatting reports; negotiation; advocacy; contextual and political analysis; law; data protection; security management; statistics; coordination.

It is important for protection actors to undertake regular and systematic assessments of their professional competencies, and those of their teams carrying out specific tasks.⁸⁸ This should enable timely identification of gaps and allow for action to be taken to adjust activities or fill gaps in knowledge and skills as required.

G

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.

Protection actors should analyse the resources required, in relation to the objectives and strategy they have defined, in order to achieve protection outcomes (see Chapter 2). They should endeavour to secure resources for an adequate period of time, before undertaking a response.

While avoiding resource-driven programming, protection actors should work with donors to ensure that funding for their activities is flexible enough to avoid having to curtail programmes or projects while there are ongoing protection needs. There are, however, obvious limitations to this effort. For example, multi-annual funding is seldom obtainable, while seemingly secure funding can quite suddenly and unexpectedly dry up.

To the extent possible, such shortfalls should be foreseen, along with efforts to analyse the potential impact on the population affected. When the risk of a shortfall is high, pre-emptive measures and contingency planning must be put in place. In cases where an interruption is inevitable, all relevant stakeholders should be alerted as rapidly as possible. Operational adjustments must be implemented swiftly, including in concert with other actors. In the likely event of a handover of activities to actors with the means and capacity to continue, all efforts must be made to minimize negative consequences for the people at risk, caused by the shortfalls and ensuing interruption of programme.

STAFF TRAINING

S

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

As already emphasized, protection work can be sensitive, and often takes place in complex and fluctuating circumstances. It is the responsibility of each protection actor to ensure that its staff acquire the knowledge, and develop and maintain the skills and attitudes, required to perform satisfactorily in such environments. The risk of having an adverse impact, on the people for whom this work is conducted, is ever present. Hence the vital need for protection activities to be carried out by staff with appropriate expertise and competencies, and for protection actors to maintain adequate in-house capacities.

The demanding technical complexities and the rapid evolution of the protection sector as a whole have led to a shortage of the highly skilled protection staff needed to meet operational demands. In addition to trying to recruit new staff with the requisite knowledge and skills, protection actors must therefore develop other strategies to cope

⁸⁸ See, for instance, the tools for [Cluster Coordination Performance Monitoring](#).

with this development, with training as a core feature. For those actors who do not have the means or the desire to develop their own comprehensive training programmes, facilitating access for their staff to other available opportunities should be a priority. Partnerships in the design and delivery of training programmes should be explored, as a means of also facilitating cooperation in operations. Other options, such as induction courses, on-the-job coaching, communities of practice and mentoring programmes, may also be useful.



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: gender-based violence, child protection, housing, land and property rights, access to justice, mine action, protection of persons in the context of natural disasters, protection of the elderly and persons with disabilities, etc.

The proliferation of protection references is expected to continue. In the absence of a centralized quality control process, and with no body formally tasked to guide, manage or judge the quality of the reference materials produced across the humanitarian system, it is up to the users to assume this task, exercising their own judgement as to the quality of what they use. It is in the interest of protection actors to draw from collective experience, and to keep themselves informed of the evolution of protection work, adapting and adopting new policies, approaches and practices, as appropriate. They must also take measures to ensure that their field staff are informed of useful new materials relevant to their mandates and activities. This includes disseminating and understanding these professional standards and other relevant guidance, to ensure response of adequate and consistent quality across all operations.

By documenting their own activities, lessons learnt and good practices, individually and/or in cooperation with other partners – by establishing communities of practice, for instance – protection actors can also actively contribute to the evolution of concepts, policies and practices, and to the development of their sector.

MANAGING STAFF SAFETY



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

Protection work is inherently dangerous since it often challenges the status quo of the operational environment, and may pose a threat to long-standing practices of violating human rights. While this work may be particularly welcomed by populations affected, there is always a risk of an aggressive response (overt or otherwise) by some duty bearers. Protection work also usually leads to an accumulation of stress, the result of having to regularly confront violations and abuse, and interact with victims, survivors and witnesses.

Protection actors, at the organizational level, have a duty of care towards their staff. To that end, adequate measures must be put in place, to help minimize the risk to staff members' health and mitigate the physical and mental consequences of their work.

The actual risks and vulnerabilities that protection staff might be exposed to obviously vary according to the context. The specific threats that their activities might generate must be carefully analysed regularly. Understanding these threats – their nature, the perpetrators/sources and their motives and intentions, the people at risk of being targeted and the reasons for that – is essential in order to manage them effectively.

The distinction between the risks faced by national and international staff is of particular importance in this analysis. The value of the knowledge, insights and analysis that a national perspective can offer in shaping an effective protection response must be weighed against the potential risks that national staff might face, owing to their association with protection activities. That is because, in many cases, national staff face different – and often greater – security risks in this work, as they are often, along with their friends and families, part of the communities in which they work.

It can happen that national staff are perceived by various stakeholders as having a personal interest in the dynamics of the conflict. Their mere involvement in protection activities may implicate them in the eyes of those stakeholders, if only in terms of perception. To address these issues, the role of national staff must be defined more clearly, which will also help minimize their exposure to risk.

Whenever risks – either in terms of security or of public perception – have been identified, the exposure of national staff to matters of a sensitive nature – circumstances, processes, people or information – must be reduced, and the distinct roles of national and international staff made clear to all stakeholders.

In all circumstances, staff at all levels must be informed of the risks they may face. No staff should be forced to participate in an activity presenting risks they are not willing to take: the option of declining to participate must be kept open to all.

An organizational culture that encourages staff to report their distress and seek assistance to cope with accumulated stress or following traumatic events (originating within or outside the organization) is essential. Such openness is critical for managing these risks and equipping staff to keep themselves safe in sensitive environments.

All protection actors should also develop clear management policies and guidelines consistent with their duty of care to staff. These guidelines should help management/senior staff mitigate and respond to risks faced by protection staff, including workplace safety and the consequences of accumulated stress and vicarious trauma. They should be made available to and discussed with all staff – national as well as international. 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.

All 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. Codes of personal conduct are essential to ensure that no individual action by protection staff causes harm, intentionally or unintentionally, or generates additional risks for communities and individuals affected (or for staff members). They are also critical in clearly defining the parameters of acceptable practice, behaviour and personal conduct.

While not necessarily specific to protection work, a number of policy documents aimed at regulating the behaviour of staff towards beneficiary populations have been widely endorsed by humanitarian and human rights actors. They include important policies to prevent and eradicate harassment and abuse in the workplace, sexual exploitation and abuse of beneficiary populations, with particular attention being paid to the heightened risk of exploitation that can arise when working with persons in situations of vulnerability.

Once a protection actor has adopted a code of conduct, concrete measures to ensure compliance must be put in place. As a minimum, such measures must include: making the policies available to all staff; briefing staff on their content and incorporating the policies in relevant staff training; allowing access by the public (at least to those parts that relate to interaction between staff and communities or individuals affected); ensuring clear reporting lines that are safe and confidential both for staff and for beneficiaries on potential breaches of the policies; and establishing accessible monitoring and complaints mechanisms. Such codes should also feature in the terms of reference of positions, unit/individual work plans and in performance appraisals.

ETHICS BOARD

Ethical dilemmas may arise when handling sensitive personal information, the solution of which may be beyond the competence or responsibility of a single individual. In such instances, guidance may be provided – for example, by an ethics board, though this may be only one entity within a broader set of mechanisms and procedures. These mechanisms and procedures should be in a position not only to respond to specific requests but also to regularly review whether an organization possesses support mechanisms for staff and the tools necessary for risk analysis. It should be made clear that working on the basis of standards and ethical considerations is as much an individual as an institutional responsibility.

ANNEX TO CHAPTER 7

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.

 facebook.com/icrc
 twitter.com/icrc
 instagram.com/icrc



ICRC

International Committee of the Red Cross
19, avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01
shop.icrc.org
© ICRC, April 2018