



PROFESSIONAL STANDARDS FOR PROTECTION WORK

BY HUMANITARIAN AND HUMAN RIGHTS ACTORS DURING ARMED
CONFLICT AND OTHER VIOLENCE

FOURTH EDITION, 2024



A GLOBAL NGO NETWORK
FOR PRINCIPLED AND EFFECTIVE
HUMANITARIAN ACTION



PROFESSIONAL STANDARDS FOR PROTECTION WORK

**BY HUMANITARIAN AND HUMAN RIGHTS ACTORS DURING ARMED
CONFLICT AND OTHER VIOLENCE**

FOURTH EDITION, 2024

ACKNOWLEDGEMENTS

The Advisory Group extends its appreciation to all those who took part in this revision, which is the result of an interactive process. The Standards reflect contemporary concerns and are of direct relevance to those involved in protection work.

The ICRC would like to thank the members of the Advisory Group. They were asked 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), Joanne Mariner, Tirana Hassan (2015–2017), Anne Fitzgerald (2015 onwards)

Danish Refugee Council (DRC): Kathrine Starup (2011–2024)

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

Global Protection Cluster (GPC): Francesco Michele (2023–2024), Simon Russell, Eva Garcia Bouzas (2015–2017), Samuel Cheung (2023–2024)

Human Rights Watch: Michael Bochenek (2015–2024)

Humanitarian Policy Group (HPG): Sorcha O’Callaghan (2008–2009), Victoria Metcalfe (2011–2012), Eva Svoboda (2012–2017), Gemma Davies (2023–2024)

Humanity & Inclusion: Sarah Rizk (2011–2012), Nathalie Herlemont Zoritchak (2011–2017)

InterAction: Ray Lynch (2008–2009), Jenny McAvoy (2011–2017), Erin Weir (2023–2024)

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), Romain Bircher (2011–2013), Guilhem Ravier (Project Manager, 2012–2017), Pilar Gimeno Sarciada (2018–2022), Aribani Ibachi Witanene (2022–2024), Sean Cordey (2023–2024), Clara Deniz Buelhoff (Project Manager, 2023 onwards)

International Council of Voluntary Agencies (ICVA): Ed Schenkenberg van Mierop (2008–2012), Nan Buzard (2012–2017), Mirela Shuteriqi (2023–2024)

International Federation of Red Cross and Red Crescent Societies (IFRC): Stephen Wainwright (2023–2024)

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

Médecins sans Frontières (MSF): Kate Mackintosh (2008–2009), Sean Healy (2011–2013), Judith Fisher (2011–2012), Gabriela Baraldi (2023–2024)

Norwegian Refugee Council: Anthony Nolan, Elise Rech (2023–2024)

Office for the Coordination of Humanitarian Affairs (OCHA): Simon Bagshaw (2011–2013), Dina Abou Samra (2014–2024)

Office of the United Nations High Commissioner for Human Rights (OHCHR): Matthias Behnke (2007–2009), Francesca Marotta, Mara Steccazzini (2015–2024)

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), Nicholas Hart, Houda Chalchoul, Bernadette Raymonde Castel (2023–2024)

Oxfam: Rachel Hastie (2011–2024)

Thanks are also due to:

- Jumana Shafiq, Mohammad Jameel (ABS Development Organization for Woman & Child), Kalungero Lusenge (Groupe d'Associations de Défense des Droits de l'Homme et de la Paix), Regis Zoungrana (Association pour la Gestion de l'Environnement et le Développement), Paluku Isamura, Me D'Alzon Syamasamba (Ceprossan) and Cathy Huser (ICRC) for their contributions on community-based protection in Chapter 2.
- Marlies Bull (OCHA) for her contributions to Chapter 6.
- Jacek Saffell, Justinas Sukaitis, Vincent Graf Narbel, Joelle Rizk (ICRC), Alice Proby, Megan Mcguire, Ondine Ripka (MSF), Nicholas Oakeshott, Rachelle Cloutier, Dogu Han Buyukyagcioglu (UNHCR), Fanny Weicherding and Jos Berens (OCHA) for their contributions to Chapter 7.
- Joelle Rizk, Pierrick Devidal, Konrad Bark, Samit D. Cunha (ICRC), Alice Proby, Megan Mcguire, Ondine Ripka (MSF), Nicholas Oakeshott, Katie Drew, Charles Hornsby, John Warnes, Norbert Trosien, Rachelle Cloutier, Dogu Han Buyukyagcioglu (UNHCR), Anna Bacciarelli, Tamir Israel and Amos Toh (HRW) for their contributions to Chapter 8.
- Anne Quintin, Ahmed Aldawoody, Alexander Breitegger, Cathy Huser, Chiara Debenedetti, David Kaelin, Eva Svoboda, Joelle Rizk, Maria Carolina Aissa de Figueredo, Samar Al-Attar, Sylvie Van Lammeren, Tilman Rodenhäuser, Siobhan Sparkes McNamara and Chiara Traverso de Souza (ICRC) for their contributions to various chapters.

The ICRC would like to thank all others who participated in the preparation of this fourth edition (2022–2024), including:

- Steve Bonaventure Ako Tanga, Cristian Rivier, Rachel Bernard, Claire Meytraud and Sophie Orr (ICRC) for their help in organizing consultations on protection leadership.
- The Protection Donor Group.
- Ruth del Pino Bleijerveld (ICRC), who contributed to the revision and supported the work of the Advisory Group during the revision process.
- Melanie Kesmaecker-Wissing (Oxfam), Carolina Franceschini (NRC) and Tamar Suzanne Joanian (UNHCR) for their help in liaising with L/NNGO members of the Community-Led Protection Task Team.
- Hala El Khoury (CCHN) for her help in organizing a survey of local and national organizations.
- Ameline Peterschmitt Nussbaumer for her help in the development of the app and the e-learning tool that accompany this document.

The ICRC would like to thank the Swedish International Development Cooperation Agency for financially supporting the revision of the Professional Standards and the Norwegian Red Cross for financially supporting a study on the evolution of the protection environment.

TABLE OF CONTENTS

| | |
|---|-----------|
| Acknowledgements | 2 |
| Abbreviations | 8 |
| Glossary | 9 |
| Introduction | 11 |
| Why protection standards are still necessary | 11 |
| Background | 12 |
| Scope and limitations of the document | 13 |
| Purpose and target audience | 14 |
| Applicability of the standards during disasters | 14 |
| Structure of the document | 15 |
| What has been updated? | 16 |
| 1. The role of leadership in addressing protection risks | 18 |
| Introduction | 20 |
| The role of organizational leadership | 22 |
| The role of individual leadership | 24 |
| The roles of donors and states | 28 |
| Reference material for Chapter 1 | 30 |
| 2. Principles in protection work | 32 |
| Introduction | 34 |
| Respecting the principles of humanity and impartiality (including non-discrimination) | 35 |
| Avoiding harm | 37 |
| Putting affected people at the centre of protection activities | 39 |
| Annexes to Chapter 2 | 44 |
| <i>Annex 1: Protection work for people with disabilities</i> | 44 |
| <i>Annex 2: Reference material for Chapter 2</i> | 46 |
| 3. Managing protection strategies | 48 |
| Protection analysis and identification of critical protection risks | 50 |
| <i>People-centric protection</i> | 50 |
| <i>A multidisciplinary approach</i> | 51 |
| <i>A dynamic approach</i> | 51 |
| Response planning and implementation | 52 |
| <i>An outcome-oriented approach</i> | 52 |
| <i>A coordinated and complementary approach</i> | 52 |
| Monitoring, evaluation and learning | 53 |
| <i>Monitoring</i> | 53 |
| <i>Evaluation and learning</i> | 55 |
| Reference material for Chapter 3 | 57 |
| 4. Building on the legal base of protection | 58 |
| Introduction | 60 |
| Knowing the legal framework | 60 |
| Referring to the law with consistency | 63 |
| Maintaining coherence and accuracy | 63 |
| Referring to domestic law and other standards | 64 |
| Upholding international legal standards | 66 |
| Reference material for Chapter 4 | 69 |

| | |
|--|------------|
| 5. Promoting complementarity | 70 |
| Introduction..... | 72 |
| Complementarity of action among protection actors..... | 74 |
| Complementarity of principles among protection actors | 74 |
| Complementarity of analyses..... | 75 |
| Mobilizing other protection actors | 76 |
| Providing information on protection services and facilitating referral to services..... | 76 |
| <i>Ensuring a survivor/victim-centred approach when establishing a referral pathway</i> | 76 |
| <i>Facilitating face-to-face referrals</i> | 77 |
| <i>Facilitating digital referrals</i> | 77 |
| Responding to harm and violations..... | 78 |
| Reference material for Chapter 5..... | 79 |
| 6. The protection architecture | 80 |
| Introduction..... | 82 |
| Relating to the primary duty bearers..... | 83 |
| Interface with UN peace operations and internationally mandated military forces and police services | 88 |
| Engaging UN peace operations and internationally mandated military forces and police services..... | 92 |
| Communities, civil society and other actors | 96 |
| Reference material for Chapter 6 | 98 |
| 7. Managing data and information for protection outcomes..... | 100 |
| Introduction..... | 103 |
| <i>Structure of the chapter</i> | 103 |
| <i>What is protection data and information management and why is it important?</i> | 103 |
| <i>Protection information management</i> | 104 |
| <i>Protection data and information: types of data, sensitivity and requirements</i> | 106 |
| Section 1 – General standards for the management of protection data and information..... | 108 |
| <i>Lawful, legitimate and fair management</i> | 108 |
| <i>Defined and specific purpose, necessity and proportionality</i> | 112 |
| <i>Data quality</i> | 113 |
| <i>Data retention</i> | 114 |
| <i>Data security</i> | 114 |
| <i>Confidentiality</i> | 116 |
| <i>Assessing risks and benefits</i> | 116 |
| <i>Avoiding bias and discrimination</i> | 119 |
| <i>Transparency</i> | 120 |
| <i>Coordination and collaboration</i> | 121 |
| <i>Data sharing and transfer</i> | 122 |
| <i>Accountability</i> | 124 |
| Section 2 – Additional standards for the processing of personal data | 125 |
| <i>Compliance with legal frameworks</i> | 125 |
| <i>Main actors of personal data processing</i> | 126 |
| <i>Data protection by design and default</i> | 128 |
| <i>Data subject rights</i> | 128 |
| Annexes to Chapter 7 | 130 |
| <i>Annex 1: The data-related risks and benefits of various processes and technologies</i> | 130 |
| <i>Annex 2: Glossary</i> | 138 |
| <i>Annex 3: Reference material for Chapter 7</i> | 140 |

| | |
|---|------------|
| 8. A protection approach to digital risk and digital technologies | 142 |
| Introduction..... | 144 |
| <i>Digital realities</i> | 144 |
| <i>A framework for protection in the digital space</i> | 145 |
| <i>Aim, scope and structure of the chapter</i> | 146 |
| Protection work in the digital age..... | 146 |
| <i>Digital risks as protection risks</i> | 146 |
| A principled protection approach to digital technologies..... | 148 |
| <i>Respecting the principles of humanity, impartiality and non-discrimination</i> | 148 |
| <i>Digital “do no harm”</i> | 149 |
| <i>People-centric and inclusive digital technologies</i> | 150 |
| <i>Further ethical and operational implications</i> | 151 |
| Enhancing protection outcomes in the digital age | 152 |
| <i>Integrating digital risks in protection strategies</i> | 152 |
| <i>Referring to and developing protective frameworks</i> | 152 |
| <i>Engaging in protection dialogue on digital risks</i> | 154 |
| <i>Strengthening affected people’s self-protection capacity and their resilience to digital risks</i> | 154 |
| <i>Ensuring complementarity of protection action in the digital age</i> | 155 |
| <i>Building preparedness of protection actors</i> | 156 |
| Annexes to Chapter 8..... | 156 |
| <i>Annex 1: Reference material for Chapter 8</i> | 156 |
| <i>Annex 2: Examples of protection risks enabled through the use of digital technology</i> | 158 |
| <i>Annex 3: Glossary for Chapter 8</i> | 163 |
| | |
| 9. Ensuring professional capacity..... | 164 |
| Introduction..... | 166 |
| Ensuring relevant capacities and competencies | 166 |
| Staff training..... | 168 |
| Managing staff safety | 169 |
| Ensuring professional and ethical conduct by staff | 170 |
| Reference material for Chapter 9 | 171 |

ABBREVIATIONS


| | |
|----------|---|
| ALNAP | Active Learning Network for Accountability and Performance (in humanitarian work) |
| DFS | UN Department of Field Support |
| DIA | data impact assessment |
| DPIA | data protection impact assessment |
| DPKO | UN Department of Peacekeeping Operations |
| GPC | Global Protection Cluster |
| HPG | Humanitarian Policy Group |
| IASC | Inter-Agency Standing Committee |
| ICRC | International Committee of the Red Cross |
| IDP | internally displaced people |
| IHL | international humanitarian law |
| IHRL | international human rights law |
| IRL | international refugee law |
| L/NA | local/national actor |
| LGBTQ+ | lesbian, gay, bisexual, transgender, queer and other identities |
| NGO | non-governmental organization |
| OCHA | Office for the Coordination of Humanitarian Affairs |
| OECD/DAC | Organisation for Economic Co-operation and Development/the Development Assistance Committee |
| OHCHR | Office of the High Commissioner for Human Rights |
| PIM | protection information management |
| PoC | protection of civilians |
| SMART | specific, measurable, achievable, relevant, time-bound |
| SMS | Short Message Service |
| UN | United Nations |
| UNHCR | United Nations High Commissioner for Refugees |
| UNICEF | United Nations Children's Fund |
| UNSG | United Nations Secretary-General |

GLOSSARY

Some of the terminology in this document may differ from that used by other organizations.¹ Additionally, Chapters 7 and 8 include glossaries covering the concepts in those chapters.

| TERM | DEFINITION |
|----------------------------|---|
| authority | <ol style="list-style-type: none"> 1. A military, police or other state security force, judicial entity or ministry with specific responsibilities, such as ensuring access to justice and effective remedies, emergency medical assistance or other services essential to the safety and well-being of the population. 2. Any kind of weapon bearer – state entity, armed force, peacekeeping force, other multinational force, armed group or other non-state actor – that is able to launch hostile action against individuals or a population and is responsible for protecting those who fall under its control. |
| capacity | <p>Any of the resources and capabilities that are available to individuals, households and communities to cope with a threat or to resist or mitigate the impact of a threat.</p> <p>Resources can be material or may derive from the way a community is organized. A capacity can include skill sets or the ability to access certain services or move freely to a safer place.</p> |
| causal logic | <p>The pathways and milestones for achieving a particular outcome, including the sequence of actions to be undertaken (and the assumptions inherent in them), the sectors and disciplines that will contribute to the desired outcome and the roles of various actors.</p> <p>The causal logic identified should underlie all actions taken to achieve the planned outcome. It is sometimes referred to as the theory of change.</p> |
| critical service | <p>A service that addresses people's fundamental needs after their life-saving needs have been met.</p> <p>Critical services include:</p> <ul style="list-style-type: none"> • health care • psychosocial services • security measures • tracing services for missing people • documentation services for people lacking essential identity documents • legal services for people in need of legal aid • advice on how to access accountability and redress mechanisms. |
| primary duty bearer | <p>An entity that holds the primary obligation and responsibility to respect, protect and fulfil the rights of people on its territory or under its jurisdiction or control.</p> <p>Under international law, authorities at all levels of government are primary duty bearers. In addition, state and non-state parties to conflicts have additional responsibilities under IHL.</p> |
| protection actor | <p>Humanitarian or human rights entity engaging in protection activities or pursuing protection strategies. This includes protection-mandated and specialist organizations/agencies.</p> <p>Humanitarian actors not mandated for or specialized in protection are also expected to contribute to protection outcomes.</p> |

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 Terminology](#), June 2016; [Privacy International website](#); UNHCR, [Policy on the Protection of Personal Data of People of Concern to UNHCR](#), May 2015.

| TERM | DEFINITION |
|------------------------------|---|
| protection analysis | A process undertaken to identify protection risks with the aim of guiding strategies and responses. |
| protection monitoring | The process of systematically and regularly collecting, verifying and analysing information over an extended period of time in order to identify violations of rights and/or protection risks for populations of concern, for the purpose of responding effectively. |
| protection outcome | <p>A reduction in protection risk.</p> <p>Protection risk will be reduced when threats and vulnerability are minimized and the capacity of affected people and primary duty bearers is enhanced. Protection outcomes are the result of changes in behaviour, attitudes, policies, knowledge and practices.</p> |
| protection risk | <p>Actual or potential exposure to violence, coercion or deprivation (deliberate or otherwise).</p> <p>Violence, coercion or deprivation may harm people's physical or mental well-being, place them in physical danger and/or violate their rights. The activity causing the risk may be a direct act, measure or policy, but a protection risk may also stem from inaction by a primary duty bearer. Reducing risk involves reducing the level of a threat, reducing relative vulnerability to that threat and/or increasing the capacity of a person or group to resist and/or rebound from a given threat.</p> <p>A reduction in risk is also referred to as a <i>protection outcome</i>.</p> <p>PROTECTION RISK EQUATION</p>  |
| threat | <p>A human activity or a product of human activity that results in violence, coercion or deprivation (deliberate or otherwise).</p> <p>A threat can be the perpetrator of such activity (the agent of the threat) or a policy or ethnicity norm (source of threat) that is causing harm.</p> |
| vulnerability | <p>Characteristics or circumstances of an individual or group or their surrounding physical environment that diminish their ability to anticipate, cope with, resist or recover from the impact of a threat.</p> <p>People differ in their exposure to a threat depending on their social group, gender, ethnicity, age and other factors. Vulnerability is not a fixed or static criterion attached to specific categories of people and no one is born vulnerable.</p> |

INTRODUCTION

Protecting people caught up in armed conflict and other violence is a critical challenge. In many armed conflicts, the distinction between civilians and combatants is deliberately blurred. Parties to conflict often subject civilians to attacks, systematic violations of their rights and other abuses. States and other duty bearers frequently lack the will – or the capacity – to protect people at risk. Duty bearers may themselves perpetrate violence or other abuse against civilians. The proliferation of armed actors and the high intensity of conflicts present additional challenges to protection actors. This is compounded by hateful speech and attitudes, misinformation and disinformation, which can spread increasingly rapidly in the digital realm and can put both affected populations and protection actors at new or increased risk of harm.

Debates on localization and decolonization have challenged the status quo of protection action and led to a re-evaluation of practices that reflected unequal power dynamics and outdated mindsets. The centrality of affected people, their priorities and their expertise in all protection action has been reaffirmed and the role of local actors has gained increased recognition. Externally imposed approaches lacking appreciation for local expertise and mechanisms are meeting increased resistance, as are dishonest partnership models.

The increased number and diversity of actors in protection work requires a greater level of complementarity between them. Despite the challenge of remotely connecting with affected people at times during the COVID pandemic, a strengthened operational presence has brought closer proximity between humanitarian and human rights actors engaged in protection work. These protection actors 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 persist. This document recognizes the 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 violence, and that it is possible to maximize complementarity to provide more effective protection.

WHY PROTECTION STANDARDS ARE STILL NECESSARY

A complementary protection response delivered by a wide array of actors needs a common foundation. These standards are a set of common professional ethics that aim to make protection work safer and more effective. They define a baseline that guarantees a high level of professionalism, in the interests of both the affected civilian populations and the community of protection actors.

The absence of common professional standards can lead to situations where protection work harms the very people and communities we seek to protect. A concerted effort is therefore required to ensure that protection work by humanitarian and human rights actors meets commonly agreed minimum professional standards, 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 ICRC between 1996 and 2000 initiated a collaborative project to create professional standards that would strengthen protection during armed conflict and other violence. Besides agreement on a common understanding from which to create common minimum standards, the project resulted in a generally accepted definition of protection that remains in effect:²

² 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.

Definition of protection

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).

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.

Since then, there have been several efforts to define professional standards in protection work, including the Sphere Project³ and various UN and NGO initiatives.⁴ However, these efforts were based on a specific approach to protection or a specific operational context. There were no principles or fundamental elements on which to base safe and effective protection work. 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 conducting protection work during conflict or other violence.

BACKGROUND

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

From the outset, publication of *Professional Standards* was intended to be an evolutionary process, involving regular revisions. A second edition was published in 2013 and a third in 2018. In 2022, the ICRC, together with the Advisory Group composed of experienced humanitarian and human rights practitioners and researchers, agreed to undertake a fourth revision. This enabled us to take stock of important developments in the area of protection and of our views and evolving practice with regard to major issues and challenges.

Based on these discussions, members of the Advisory Group began working on draft proposals. These were discussed throughout late 2023 and early 2024 and then circulated to the wider community of practitioners.

The broader consultative process, which began in May 2023, sought to ensure that the standards reflected both the challenges faced by actors in the field and the consensus of the protection community. This process entailed a series of workshops, the mobilization of local and national organizations, and an online survey. 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 dissemination of the standards and to ensure more effective capacity-building measures and 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 remains difficult.

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 partners and the broader humanitarian and human rights community.

³ See: The Sphere Project, *Humanitarian Charter and Minimum Standards in Disaster Response*, 2011.

⁴ See, for example: World Vision UK, *Minimum Inter-Agency Standards for Protection Mainstreaming*, 2012.

SCOPE AND LIMITATIONS OF THE DOCUMENT

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

They are not intended as operational guidance. Rather, 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 other duty bearer with protection responsibilities (such as a state, non-state actor, or peace operation). A “protection worker” is a person engaged in 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. It is recognized that actors not engaging in specialized protection work may nonetheless contribute to protection outcomes. These actors may also find that the *Professional Standards* provide valuable guidance for their work.

The scope of this project is broad, but it makes no claim to be exhaustive. Moreover, the Standards reflect the view that people at risk must themselves be at the centre of any action taken on their behalf. The contents of this document are equally applicable to humanitarian and to 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.

The standards outlined in this document supplement and do not replace other standards used by protection actors, such as:

- 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 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.

All these efforts to set protection standards are complementary, rather than duplicative or contradictory.

PURPOSE AND TARGET AUDIENCE

These standards are addressed to all humanitarian and human rights actors working to protect people who experience or are at risk of violations and other abuse during armed conflict and other violence. Action to protect such people includes persuading duty bearers to meet their obligations and enhancing people's capacity to reduce or eliminate their exposure to threats and to cope with the consequences of protection failures.

Other organizations may also find them useful, such as those involved in development or peacebuilding and those that interact with humanitarian and human rights organizations in these situations.

The standards in this document provide a reliable source of reference for organizations writing or reviewing internal policies, guidelines and training materials and for practitioners in the field who design and implement protection strategies.

They can also serve as a point of reference for other actors that have an interest in protection or contribute to protection outcomes, even if they do not regard themselves as specialized protection actors. In addition, protection actors can use them to explain to 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 fourth edition – such as the e-learning course and the summary version – to disseminate the standards and guidelines to their colleagues and partners. Those tools are designed to make the standards more accessible and user-friendly.

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 violence, i.e. those that have protection at the centre of their efforts. Organizations that simply need to consider protection risks in their daily activities can certainly gain inspiration from these standards, but they are likely to find more practical guidance in the latest version of the *Sphere Standards* and in *Minimum Standards for Protection Mainstreaming*.

APPLICABILITY OF THE STANDARDS DURING DISASTERS

These standards focus on armed conflict and other violence, but many of them are equally applicable during disasters. Certain standards or guidelines may not apply or might apply in a less stringent manner during disasters, as they are intended to cover 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. There have to be people in the area concerned, and even then, the determining factors will be the degree to which those people are exposed to natural disasters and their resilience. These questions can be addressed by human action, including action by states. When governments and others fail to reduce people's exposure and vulnerability, strengthen their resilience or take effective mitigation measures, their failure is a human rights issue.⁵

5 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.

Human rights principles must be at the centre of all efforts undertaken at every phase of disaster response – risk reduction, prevention, preparedness, response, recovery and reconstruction. International human rights norms should guide all measures taken immediately after a disaster to ensure that survivors are safe, are treated for their injuries and are clothed, fed, and sheltered. Full respect for human rights is essential at all stages of a crisis; it should not be regarded as a luxury 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 dignity of the people affected, is wholly compatible with that of the present standards.

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 of or 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 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 and human rights actors engaged in protection work must pay close attention to the following:

- the principles of humanity (Standard 2.1)
- non-discrimination and impartiality (Standards 2.2 and 2.3)
- human dignity (Standard 2.6)
- the duty to do no harm (Standards 2.4 and 2.5)
- the need to ensure the active participation of people at risk (Standard 1.7).

As in the case of armed conflict and other violence, protection actors responding to disasters must analyse protection needs in their areas of competence (Standard 3.1) and must monitor and evaluate protection outcomes and impact (Standards 3.3 and 3.4).

STRUCTURE OF THE DOCUMENT

Standards, guidelines and explanatory text

This document presents a series of standards and guidelines, each accompanied by explanatory text.

Standards

These constitute the minimum obligations that all humanitarian and human rights actors doing protection work must fulfil. In certain 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 takes precedence.

Guidelines

Guidelines are useful and sometimes essential reference criteria. Applying them is likely to require more flexibility than in the case of standards, as they cannot be applied at all times by all actors. Certain guidelines could even be adopted as standards by some organizations, whereas other organizations might find the same guidelines to be unrealistic, impracticable, or irrelevant, depending on the nature of their work, the approaches they adopt and the activities they undertake.

Explanatory notes

Explanatory notes delineate the main elements that underpin 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, and 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 decide 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.

- The Standards now take a more inclusive and community-based approach to protection, in response to an advanced understanding of the role of affected people in their own lives and their own protection.
- The importance of prevention and preparedness actions carried out by duty bearers or at the community level and supported by protection actors, has been embedded throughout the Standards.

New Chapter 1 on the role of leadership in addressing protection risks

The humanitarian sector is faced with an inter-related set of problems:

- the growing perception of a leadership gap or leadership weakness with respect to commitment to protection
- a sense that a commitment to “principled humanitarian action” is being lost
- persistent failures of advocacy for protection.

Accountability for protection outcomes is situated at various levels along a chain of actors, ranging from the protection professional working directly with communities, to mid- and senior-level humanitarian leadership at country or regional level, to organizational-level leadership and ultimately to donors and states. The Standards seize the opportunity to present a sector-wide consensus on the accountability of senior leadership at various levels and to set standards and guidelines for senior leadership to successfully contribute to protection outcomes.

While the Professional Standards are mainly directed at protection professionals, this chapter addresses the role and responsibilities of senior managers, protection leaders and donors. Based on consultations with donors, the chapter also provides guidelines for donors, to create an enabling environment for principled decision-making and prioritizing protection.

Significant updates to Chapter 2: Principles in protection work

The community-based protection textbox in Chapter 2 has been re-written on the basis of contributions from local and national organizations, with the aim of taking a more inclusive and community-based approach to protection.

A definition of protection outcomes has been added, recognizing that specialized protection actors should work together with other actors that contribute to protection outcomes.

Significant updates to Chapter 3: Managing protection strategies

Chapter 3 now places greater emphasis on protection as an outcome, with success being measured by the extent to which risks have been reduced. The 2009, 2013 and 2018 editions had already recognized the need to adopt a strategy based on sound analysis of the situation and to monitor and evaluate its implementation regularly. The changes to this chapter draw on discussions still in progress among protection practitioners about the challenges of measuring protection outcomes.

The chapter explains the importance of establishing the causal logic of action to achieve a protection outcome and of monitoring and evaluation.

Significant updates to Chapter 6: The protection architecture

Dialogue and interaction between humanitarian and human rights actors and UN peacekeeping operations and other internationally mandated military and police forces are necessary to achieve protection outcomes while upholding a principled approach to protection work.

The revised version of Chapter 6 emphasizes the role that UN peacekeeping operations and other internationally mandated military and police forces can play in supporting duty bearers, not only in their response to protection risks, but also in their prevention efforts with duty bearers and affected communities.

This edition of the Professional Standards recognizes communities themselves as part of the protection architecture and includes guidelines for engaging local/national actors (L/NAs), which provide an invaluable understanding of local challenges and potential solutions, can mobilize local networks and contribute to more effective, efficient and sustainable humanitarian prevention and response action with enhanced accountability to affected populations.

Significant updates to Chapter 7: Managing data and information for protection outcomes

The revised chapter reflects the insights and best practices of humanitarian and human rights organizations and the experiences of actors in data management.

It now clarifies the principles and considerations specific to the processing of personal data and information.

Annex 1 to this chapter has been updated to provide further guidance on a wide range of technologies and their data-related risks.

The Advisory Group has reviewed the scope and language of the standards and guidelines for protection data and information management. That review was prompted by the rapid proliferation of initiatives to safely and efficiently manage data and information in protection action and the expanding body of law on data protection.

New Chapter 8 on a protection approach to digital risk and digital technologies

This chapter has been written in response to the digital realities underpinning modern crises, armed conflicts and other violence, and provides a set of emerging standards and guidelines for “protection work in the digital age”.

It focuses on how protection actors should address digital risks and their impact on the rights, safety and dignity of affected people, stipulating that protection actors should address the harm emerging from the use of digital technologies by states, non-state actors and individuals.

Protection actors must also address the risks created by their own use of digital technologies for protection work. This means they must uphold the principles laid out in Chapter 2 and follow other ethical and rights-promoting approaches to digital technologies.

The chapter also provides guidance to help protection actors understand digital risks and integrate consideration of them in their work, so they can achieve protection outcomes more effectively.

Chapter 8 is complementary to Chapter 7 on data-related risks and the management of protection data and information.



1. THE ROLE OF LEADERSHIP IN ADDRESSING PROTECTION RISKS

The role of organizational leadership

- S** 1.1 Humanitarian and human rights actors must foster an organizational culture that enables their organizations to fulfil their commitments to achieving protection outcomes. This encompasses internal policies, capacity-building and incentives for robust protection leadership.
- S** 1.2 Humanitarian and human rights actors must ensure strategic alignment between organizational leadership and country contexts by establishing common protection priorities, ensuring coherence in positioning, allocating adequate resources and fostering informed risk tolerance.
- S** 1.3 Humanitarian and human rights actors must strive for complementary approaches to protection, coordinated between the leaders of the various organizations.
- G** 1.4 Humanitarian and human rights actors should ensure organization-wide coherence in their positioning, through public communication and by other means, to promote protection outcomes.

The role of individual leadership

- S** 1.5 Humanitarian and human rights leaders must prioritize amplifying the voices of affected people regarding protection risks at all levels. Where appropriate, protection dialogues and advocacy efforts must be complementary to and coordinated with the actions of affected people.
- S** 1.6 Humanitarian and human rights leaders must promote a common understanding and complementary action regarding protection among multidisciplinary teams.
- G** 1.7 Humanitarian and human rights leaders should reinforce each other in the application of humanitarian and human rights principles and the pursuit of protection outcomes. This may include adopting coordinated approaches to navigating operational dilemmas.
- S** 1.8 Humanitarian and human rights leaders must ensure that risk analyses are communicated to their donors and that local partners and mitigation measures are adequately financed. When working with local partners, humanitarian and human rights leaders must ensure that partnerships are equitable and risks are shared.
- S** 1.9 Humanitarian and human rights leaders must be predictable in their actions, in accordance with their organization's role and guided by a continuous commitment to achieving protection outcomes.
- G** 1.10 Humanitarian and human rights leaders should document their rationale for decision-making on protection action, to ensure internal accountability and external continuity.

The roles of donors and states

- G** 1.11 Donors and states should use their bilateral diplomatic relations to ensure respect for humanitarian principles and legal frameworks and advocate for the reduction of protection risks.
- G** 1.12 Donors and states should provide political backing to protection priorities, aligned with humanitarian principles and legal frameworks.
- G** 1.13 Donors and states should use their diplomatic capital to build an environment conducive to preventing violations or abuses. Donors should therefore fund prevention actions, while encouraging collaboration between humanitarian and human rights actors and other stakeholders such as peace and development actors.
- G** 1.14 Donors should factor in risks borne by their partners and intermediaries, and by front-line responders, when funding protection work. When working with local or national organizations through international partners, donors should engage in open dialogue with their partners on risks and mitigation measures and ensure that such measures are adequately funded.
- G** 1.15 Donors should require the organizations they fund to demonstrate how projects will contribute to protection outcomes, based on an analysis of protection risks, while recognizing the limitations to measuring outcomes when working to minimize threats to people at risk.

INTRODUCTION

This chapter outlines the roles and responsibilities of different levels of leadership and loci of decision-making in pursuing protection objectives and achieving protection outcomes.

Accountability for these outcomes is situated at various levels along a chain of actors, ranging from the protection professional working directly with communities, to mid- and senior-level humanitarian and human rights leadership at country or regional level, to organizational-level leadership⁶ and ultimately to donors and states. While the Standards are mainly directed at protection professionals, this chapter addresses the role and responsibilities of senior managers, humanitarian and human rights leaders and donors.⁷

Leadership can and must be found at all levels of an organization; demonstrating leadership in addressing protection risks to affected people is not reserved to senior management. This chapter, however, does address the senior leadership of humanitarian and human rights organizations, as it emphasizes their responsibility for creating an environment where leadership on protection can be demonstrated at all levels. While many of the standards and guidelines in the chapter are equally applicable to protection specialists and mid-level management, the primary target audience of the chapter is the senior leadership of humanitarian and human rights organizations – be they UN organizations, NGOs at local, national or international level, the International Red Cross and Red Crescent Movement or others.

The chapter mentions two broad categories of risk:⁸

- protection risks as experienced by people affected by conflict and other violence
- risks borne by actors working towards protection outcomes.

This second risk category can be divided into:

- safety
- security
- operational
- ethical
- reputational
- legal/compliance
- fiduciary
- information/data/digital.

Advocating for the protection and rights of affected people, publicly or through bilateral dialogue, may incur some of the above-mentioned risks. However – and perhaps more importantly – inaction entails risks that are often not adequately factored in. These may include negating the voice and experiences of affected people or generating the perception that an organization is complicit in abuses.

The chapter is divided into three parts.

It starts by laying out leadership responsibility for protection at organizational level. To provide a foundation and frame of reference for leadership at country level, organizations must provide clear direction and guidance for operations. This means ensuring that HQ and country contexts have the same priorities as regards addressing protection risks, and resolving ethical dilemmas, and agree on how outspoken or assertive the organization can and should be in a given context. Decisions in a country context should not be taken in a vacuum nor should they be solely the result of the bold moral leadership of an individual; they should be taken and implemented by a broader leadership team. Organizations must therefore foster an organizational

⁶ Organizational leadership includes the senior leadership of local and national humanitarian and human rights actors.

⁷ In this context, “donors” are state donors, including multi-state bodies such as the EU. Protection actors and humanitarian and human rights organizations may have a variety of funding sources including private donors, foundations, etc.

⁸ Risk Sharing Platform, [Risk Sharing Framework](#), 2023.

culture that incentivizes people in leadership positions to act decisively and unequivocally in prioritizing protection risks and conducting dialogue and engagement efforts accordingly. Where this approach is not followed, organizations should create tangible disincentives, linking promotion to performance on protection.

The second part details the role of individual leaders at country level, starting from their role in creating a common understanding of protection within their organization and a common understanding of priority protection risks on which to take action. It then explains that prioritizing protection must be a core leadership responsibility for humanitarian and human rights organizations operating in conflicts or other violence.⁹ It discusses improving accountability in decision-making processes, before emphasizing the importance of collective or complementary action between an ever-growing number of humanitarian and human rights actors in a context of assertive states and varying levels of acceptance of humanitarian and human rights actors' roles. Finally, it calls on leaders of humanitarian and human rights organizations to use their platforms to magnify local voices wherever possible, especially where access is difficult. Communities and local protection actors must be supported in their protection dialogues, and the leaders of humanitarian and human rights organizations have a responsibility in this area.

The third part of the chapter is directed at donors and states, including states funding protection action.

A donor not only funds protection action but is also an actor in their own right. At the same time, within the same government, agencies in charge of humanitarian funding, foreign policy or security policy operate at different levels of harmonization with each other.

States should use their diplomatic relations to support protection outcomes and contribute to building an environment conducive to preventing violations and abuses. Similarly, states that finance protection should provide political backing to protection priorities and outcomes, viewing protection and respect for legal frameworks as a strategic interest and ensuring that political, peace, security, humanitarian, and other dimensions do not take contradictory approaches.

When working with partners, donors should consider directly funding and incentivizing greater risk-sharing between local organizations and intermediary partners¹⁰ financed by the donor. The underlying risk analysis should be conducted jointly and openly, and mitigation measures should be adequately financed; all of this should be traceable for the donor.

9 The 2016 IASC Protection Policy states that humanitarian and human rights organizations “must be encouraged, supported and incentivized by all levels of leadership to consider protection in all their actions; adhere consistently to a principled approach to humanitarian action, regardless of the political dynamics driving or influencing a crisis; and contribute to preventing, stopping, reporting on and remedying risks, violations and harm experienced by affected people in crisis”.

10 Intermediary partners are usually organizations that receive funds from a back donor and pass them on wholly or in part to one or more other organizations. These deliver the proposed assistance themselves, either wholly or in part, or act as an intermediary donor to other downstream partners (e.g. UN agencies, pooled funds, National Societies to National Societies, NGO consortia, etc.).

THE ROLE OF ORGANIZATIONAL LEADERSHIP

Humanitarian and human rights actors may have operations in multiple countries, with headquarters at national or global levels, possibly supplemented by regional offices. Decision-making may be more or less decentralized depending on the organizational structure. Organizations must provide an enabling environment for decision-making at local, national, or country level in order to pursue protection outcomes. The common understanding and prioritization of protection outlined in Standard 1.6 must form part of an organizational culture in which protection is central to all humanitarian and human rights action and the organization's mandate or role is translated into actionable strategic priorities that guide organizational leadership.

S

1.1 Humanitarian and human rights actors must foster an organizational culture that enables their organizations to fulfil their commitments to achieving protection outcomes. This encompasses internal policies, capacity-building and incentives for robust protection leadership.

Putting protection at the centre starts with an organizational culture that creates incentives and builds the capacity among staff to do so. There must be incentives for leaders at all levels to work towards protection outcomes. Disincentives must be removed. Responsibilities for fulfilling commitments to putting protection at the centre need to be clearly laid out, making it clear who is accountable for what. This could include the achievement of protection outcomes among a person's performance objectives or requiring protection-relevant experience or expertise for senior leadership positions. Conversely, where performance does not meet expectations or senior staff demonstrably fail to act on stated protection objectives, the organization should take this into account when assessing their performance, and it should have a negative effect on their career progression.

Trust is a vital element for principled decision-making, risk-taking and sharing. Diversity and inclusion policies can empower leaders, increase their trust in the organization and help them use their skills.

S

1.2 Humanitarian and human rights actors must ensure strategic alignment between organizational leadership and country contexts by establishing common protection priorities, ensuring coherence in positioning, allocating adequate resources and fostering informed risk tolerance.

Alignment between organizational leadership and a specific country context enables humanitarian and human rights leaders on the ground to act, trusting that the organization will support their decisions. Such alignment also enables organizational leadership to defend contextual decisions in the light of their role or mandate, if required.

Documentation on decision-making (see Guideline 1.10) should extend to the organizational level, to enhance accountability, ensure continuity and share the responsibility associated with a decision taken, complementing documentation at country or local level.

Risk tolerance means acceptance by an organization of the following categories of residual risk:¹¹

- safety
- security
- operations
- ethics
- reputation

¹¹ Residual risk is the risk that remains after mitigation measures have been applied to reduce the likelihood or expected impact of a risk materializing.

- legal/compliance
- fiduciary
- information/data.

If individual leaders receive no clear guidance from their organization regarding its risk profile, i.e. on how accepting of residual risks the organization wishes them to be, it is possible or even likely that leadership at country or local level will err on the side of conservative, risk-averse decision-making, even where the protection needs are grave and call for a more decisive, bold response.

The protection risks prioritized by country or local-level leadership must be communicated upward and ultimately result in common priorities at all levels of the organization. This underscores the importance of ensuring consistency of strategy between local and central levels within an organization.

S

1.3 Humanitarian and human rights actors must strive for complementary approaches to protection, coordinated between the leaders of the various organizations.

As outlined later in Chapter 5 on complementarity, humanitarian and human rights actors must situate their efforts on protection in the wider landscape of actors. They must operate in a coordinated and complementary fashion, and collectively where possible and appropriate. Each actor must use its mandate and role in a way that complements the work of others. Complementary approaches to protection in operational contexts require that humanitarian and human rights actors also exchange at organizational level, build synergies, and disambiguate their efforts.

G

1.4 Humanitarian and human rights actors should ensure organization-wide coherence in their positioning, through public communication and by other means, to promote protection outcomes.

How an organization positions itself externally at global or national level and communicates on protection will affect how it is perceived at country or local level. Public communication by a protection actor influences the perception of a broader audience, which in turn means that its communication at global level and in other contexts will influence perceptions of that actor at local level.

External positioning includes diplomatic relations and non-public engagement with stakeholders. Here too, consistency within an organization is important. Even though the operating environments of humanitarian and human rights actors may differ in terms of access, acceptance, and space to act, the overall external positioning of an organization should be clear, should reflect the organization's role or mandate and should strengthen the protection of civilians and other people protected under relevant legal frameworks.

THE ROLE OF INDIVIDUAL LEADERSHIP

It is where humanitarian and human rights organizations are operationally active that strong leadership is most important. Individual leadership is the leadership exercised by the person heading a humanitarian or human rights organization in a specific context, such as a humanitarian coordinator, a head of delegation or the country director of an INGO or an L/NA.

S

- 1.5 Humanitarian and human rights leaders must prioritize amplifying the voices of affected people regarding protection risks at all levels. Where appropriate, protection dialogues and advocacy efforts should be complementary to and coordinated with the actions of affected people.**

Affected people must be at the centre of protection action. Communities, local humanitarian and human rights actors and civil society more broadly may be conducting bilateral dialogue, advocacy, or other influencing strategies to strengthen protection. Humanitarian and human rights leaders must build on these efforts (see also Guideline 2.8, Standard 6.13 and Standard 6.14 on promoting local capacity).

Local actors will often have the contextual knowledge and networks to help community members with protection needs. However, they may also face barriers to effectively influencing key duty bearers when the protection concerns to be raised are too sensitive (e.g. dialogue with weapon bearers on violations of international law). In such cases, international humanitarian and human rights actors should work in complementarity with local actors and reinforce them.

For instance, a local organization might be undertaking prevention work on sexual violence using its relationships with other actors and with weapon bearers, and might also be providing safe shelter, food and non-food assistance to victims and survivors. However, security constraints might complicate their efforts to reduce the civilian population's vulnerability to such violations. An international actor can address this gap by capitalizing on its mandate and access to directly engage with weapon bearers on the prevention of sexual violence.

The complementarity of protection dialogue between local, national, and international actors is all the more important in areas where access is difficult and much of the risk associated with protection work can land on the shoulders of local actors alone.

Proximity to affected people is a pillar of people-centric protection. Humanitarian and human rights leaders should seek proximity to affected people, including marginalized groups, to ensure that local perspectives guide their decision-making.

S

- 1.6 Humanitarian and human rights leaders must promote a common understanding and complementary action regarding protection among multidisciplinary teams.**

Senior leaders have a crucial influence on ensuring that protection is central to their organization's response strategy. Based on analysis, evidence and consultations with colleagues, they decide how the organization will position itself as a protection actor in a given context, which in turn affects how their colleagues at all levels understand their roles.

A common understanding of protection results from:

- a common appreciation of protection risks in the context
- the organization's identity and role as a protection actor
- the operational environment
- the organization's capacity to achieve protection outcomes.

Many organizations, especially those with a broader array of activities, struggle with siloed ways of working. For those organizations in particular, it is essential that senior leaders provide a unifying vision and ensure a common direction and an integrated way of working.

Leadership support for adopting a “protection lens” is crucial, to ensure that everyone analyses a given problem in the same manner and that all departments take the same approach. To ensure continuity in this, senior leaders can use existing analysis, planning, monitoring, evaluation and coordination mechanisms. Those mechanisms should ensure that everyone in the organization agrees as to which protection risks are the top priorities, that the organization deals with those risks in an integrated fashion and that it adapts its analysis and response as needed over time.

Ultimate responsibility for protection response lies with the head of an organization. However, other senior leaders should also prioritize the creation of staff capacity and expertise on protection (see also Chapter 9), since only staff confident in their knowledge and ability will be able to carry forward a protection-centric response.

G

- 1.7 Humanitarian and human rights leaders should reinforce each other in the application of humanitarian and human rights principles and the pursuit of protection outcomes. This may include adopting coordinated approaches to navigating operational dilemmas.**

It is necessary to find coordinated approaches to the implementation of humanitarian principles, regardless of whether humanitarian and human rights actors come together through formal coordination mechanisms. Effective protection action hinges on respect for humanitarian and human rights principles and is therefore undermined where these principles are not respected.

Decision-making in disregard of collective efforts can also weaken protection action. Humanitarian and human rights leaders do not operate in a vacuum and should reinforce each other in pursuing protection outcomes. How operational and ethical dilemmas are navigated may vary between organizations and contexts, but within the same context, alignment can magnify the impact of each actor’s protection efforts. Where organizations pursue collective or coordinated approaches to applying humanitarian and human rights principles and arbitrating dilemmas, it is equally important that exchanges between leaders reflect the roles and mandates of their organizations, leveraging a diversity of perspectives to achieve the best possible outcome.

As leaders of different organizations will often be negotiating with the same counterparts, it may be possible to draw up common messages and agree on the minimum outcomes leaders are willing to accept in negotiations.

S

- 1.8 Humanitarian and human rights leaders must ensure that risk analyses are communicated to their donors and that local partners and mitigation measures are adequately financed. When working with local partners, humanitarian and human rights leaders must ensure that partnerships are equitable and risks are shared.**

Local organizations must be supported to make informed decisions about the risks they take. International partners need to acknowledge the risks that local organizations face and respect their decisions. Sharing decision-making power is a key step towards sharing risks. If partners are inflexible or threaten to remove funding, local organizations may be compelled to accept unreasonable risks in order to continue their operations and to sustain their livelihoods. Risk-sharing implies a conscious – rather than coerced – acceptance of risks. To accomplish that, partners need to discuss on an equal footing how to best approach risks. Risk-sharing applies to all partnerships along the delivery chain.

S**1.9 Humanitarian and human rights leaders must be predictable in their actions, in accordance with their organization's role and guided by a continuous commitment to achieving protection outcomes.**

It is especially important that humanitarian leaders be predictable in their actions with regard to protection. Standard 6.7 states that protection actors, including humanitarian and human rights actors, must clearly communicate their roles and mandates. Leaders must be clear and open from the outset when communicating with authorities and others about the organization's mission and intended contributions to achieving protection outcomes, and the methods it uses to do so. This is particularly true for international organizations, to avoid confusion or the conflation of political interests and protection priorities.

Humanitarian and human rights leaders must balance priorities, often requiring them to make difficult decisions as to what to address, how and when. As explained in Guideline 1.3, this decision-making should be documented and should follow a justifiable rationale. Humanitarian and human rights leaders must use their leverage, expertise and relationships strategically: a leader who works to create a platform with stakeholders but does not use it to promote adherence to IHL and other legal frameworks, nor to promote the reduction of protection risks, loses credibility in the long run. Relationship-building with stakeholders in the conflict or other violence will further their acceptance of humanitarian and human rights actors. Predictability builds a foundation of trust upon which to develop a protection dialogue or broader influencing strategy.

Failure to advocate for protection may also jeopardize relationships of trust with stakeholders who expect organizations (especially those with a mandate) to discharge their obligations, e.g. those towards duty bearers or affected communities. Even authorities or duty bearers who fully accept the role of humanitarian or human rights actors may not always be receptive to their messages. Nevertheless, humanitarian and human rights leaders are expected to remind authorities of their obligations under IHL, human rights and other legal frameworks, and to advocate for protection.

Predictability and coherence in projecting an organization's role and obligations are essential to a protection dialogue that is underpinned by trust from all sides. This, in turn, may reduce the threats to affected people.

G**1.10 Humanitarian and human rights leaders should document their rationale for decision-making on protection action, to ensure internal accountability and external continuity.**

The leaders of humanitarian and human rights organizations should assess a variety of factors when deciding how to address protection threats through protection dialogue and other means of engagement with stakeholders, and should document their decision-making rationale as they do so. Documenting decision-making is especially important when organizations face protection dilemmas, and should be carried out contemporaneously.

Decision-making processes in times of crisis are complex. Psychological factors such as stress or fatigue, group dynamics when working collaboratively, and changing conditions within an organization can contribute in ways that it may be difficult to trace afterwards, even after just a few months. Articulating the reasoning behind a decision as to whether or not to take a certain protection action helps individuals and organizations to assess the same factors over time or review a past decision in the light of new developments. Equally, sharing this documentation appropriately internally enables risk-sharing between individual and organizational leaders. The leaders of organizations should endorse not only the success or failure of a protection dialogue, or a position taken on an ethical dilemma, but more importantly the analysis on which they based their decisions, the way they carried them out and how they worked through the consequences of their decisions, including the steps they took to mitigate any negative consequences.

Documenting decision-making processes helps leaders respond to new situations in a manner that is predictable to duty bearers and others. Personnel turn-over within humanitarian and human rights actors and duty bearers makes it even more important to be able to refer to past interactions with clarity on why decisions were taken and what considerations underlay them. During a protracted conflict where authorities and duty bearers can draw on a wide range of experiences with a protection actor, this may seem less critical. But if the organization itself or humanitarian and human rights actors in general are not well known or accepted, continuity in external engagement is an essential building block for effective protection action.

Decision-making on protection dilemmas

Humanitarian and human rights leaders should start their analysis from the desired outcome of a protection dialogue and the stated priorities of affected people. The principle of humanity must underpin their decision-making, and this implies giving priority to protecting the lives and dignity of people at risk.

Navigating ethical dilemmas may entail weighing the potentially positive outcome for a smaller group (for instance the families of people who are missing or detainees) against the potentially negative outcome for other groups of affected people if a protection dialogue is not only received negatively but leads to retaliation, such as loss of access to certain areas of the country or certain groups of people. However, this analysis should also take into account the potential results of inaction by the humanitarian and human rights actor, short-term and long-term. Doing nothing may be seen as tacitly condoning certain behaviour and may embolden perpetrators of violations.

A protection dialogue or advocacy approach should also be based on informed stakeholder mapping. Complementarity between international and national actors involves seeking out the advice of local actors, who may be well-placed to advise on how to engage with duty bearers. Understanding the stakeholders allows leaders to make informed choices as to how and when to engage duty bearers in dialogue on protection.

Leaders must thoroughly understand the dynamics of the conflict or violence, allowing them to time their interventions carefully and to choose the right angle. Duty bearers may have their own interpretation as to why a protection actor is approaching them at a given time; understanding conflict dynamics allows leaders to frame their interventions in a way that avoids misperceptions.

Leaders should also consider other protection actors and how they may be affected. In some circumstances, a principled, well-timed intervention by an international actor may support efforts by local actors to advocate for protection. In other circumstances, the opposite may be true. Leaders should assess their organization's positioning in the operational environment and the potential consequences for affected communities and other actors.

THE ROLES OF DONORS AND STATES

Donors and states not only fund protection action but are also actors in their own right. However, the different donor agencies in charge of humanitarian funding, foreign policy and security policy may not always be entirely harmonized with each other.

Under Article 1 common to the Geneva Conventions, states must “respect and ensure respect for” the Geneva Conventions. This means they must ensure that all entities under their jurisdiction comply with the rules they contain. Whether engaged in a conflict or not, states must take all possible steps to ensure that everyone complies with the rules.¹² This includes states that are supporting parties to an armed conflict and can influence those parties in such a way as to enhance the protection of civilians (PoC) and can use their influence to promote compliance with international humanitarian and human rights law.¹³

G

1.11 Donors and states should use their bilateral diplomatic relations to ensure respect for humanitarian principles and legal frameworks and advocate for the reduction of protection risks.

A state may engage in operational contexts not only by funding protection action through donor departments, but also in its capacity as a state with diplomatic ties to duty bearers. States have a responsibility to influence the environment in which humanitarian and human rights actors operate. Donors and states should use their diplomatic relations with duty bearers to ensure respect for humanitarian principles and to uphold relevant legal frameworks for reducing protection risks. Donors and states may also play a role in facilitating access for engagement between humanitarian and human rights actors and duty bearers, or may support their efforts directly by aligning key messages on protection.

G

1.12 Donors and states should provide political backing to protection priorities, aligned with humanitarian principles and legal frameworks.

States funding protection action operate in multiple spheres. They may engage with other states and stakeholders in such areas as diplomacy, security, humanitarian, development and peace action. Furthermore, they may support protection action for people affected by conflict or other violence.

States should adopt a coherent approach that allows them to provide political backing to protection priorities.

They should not instrumentalize protection risks for political purposes. For instance, they should not attempt to achieve political advantage by accusing each other of violations or abuses. Rather, they have an obligation to create an environment of genuine commitment to humanitarian principles, together with conditions conducive to reducing risks.

Similarly, where the interests of states run counter to protection priorities, humanitarian and human rights actors cannot respond effectively to protection risks nor can accountability to affected people be upheld. Donors and states should ensure their accountability for protection outcomes by supporting the application of humanitarian principles and relevant legal frameworks.

¹² The ICRC’s interpretation of Common Article I of the Geneva Conventions.

¹³ ICRC, [Allies, Partners and Proxies: Support Relationships in Armed Conflicts](#).

G

1.13 Donors and states should use their diplomatic capital to build an environment conducive to preventing violations or abuses. Donors should therefore fund prevention actions, while encouraging collaboration between humanitarian and human rights actors and other stakeholders such as peace and development actors.

States should use their diplomatic relations to support duty bearers in creating robust systems to prevent protection risks, in articulation with protection actors where appropriate (see Guideline 6.4, Chapter 6). They should engage with duty bearers on relevant legal frameworks prior to an outbreak or escalation of conflict or violence.

Donor agencies should therefore fund prevention action and encourage collaboration between humanitarian, human rights, peace and development actors and others.

G

1.14 Donors should factor in risks borne by their partners and intermediaries, and by front-line responders, when funding protection work. When working with local or national organizations through international partners, donors should engage in open dialogue with their partners on risks and mitigation measures and ensure that such measures are adequately funded.

Local humanitarian and human rights actors are essential to a protection response. Donors often engage with local or national actors through intermediary partners such as UN organizations or INGOs. This creates a gap between the donor and the organization implementing a protection activity and means that donors risk not being sufficiently aware of the risks that front-line responders face.

The constraining effects of power inequalities and uneven access to resources and funding may make it more difficult for local and national actors to secure funding consistently. This in turn may render them more inclined to accept higher levels of risk than international actors. Donors need to share risks with their intermediary partners and ensure that they in turn share risks with their local partners.

Perception of what constitutes acceptable levels of risk may differ, given that local actors are embedded in contexts affected by conflict or other violence. Where access is limited, risk may be transferred to local actors without the donor being fully aware of this. Donors should hence require their partners to communicate openly and systematically regarding the risk analysis and the mitigation measures they have undertaken with their local partners. It is essential to fund these measures adequately, along with the associated support and capacity-strengthening costs.¹⁴

G

1.15 Donors should require the organizations they fund to demonstrate how projects will contribute to protection outcomes, based on an analysis of protection risks, while recognizing the limitations to measuring outcomes when working to minimize threats to people at risk.

Putting protection at the centre of humanitarian response in areas of conflict and other violence requires donor agencies to be more aware of how the projects, programmes or response plans they fund will contribute to protection outcomes. At the same time, humanitarian and human rights actors who work towards reducing threats may not be able to disclose their reports on activities and their outcomes, such as confidential representations to perpetrators of IHL violations. The desired threat reduction may not materialize over the agreed reporting period, given that behaviour change is a long-term process and is difficult to measure causally.

¹⁴ See also IASC, [Risk Sharing Framework](#).

REFERENCE MATERIAL FOR CHAPTER 1

ALNAP, [State of the Humanitarian System Report 2022](#)

Centre for Competence on Humanitarian Negotiation, [CCHN Field Manual](#)

Centre for Competence on Humanitarian Negotiation, [Negotiating with Beneficiaries and Communities](#)

Chatham House, [Rethinking the Role of Humanitarian Principles in Armed Conflict, a Challenge for Humanitarian Action](#), 2023

ICRC, [Support Relationships in Armed Conflict](#)

IASC, [Independent Review of the Implementation of the IASC Protection Policy](#)

ODI, [Leadership of Protection in the Humanitarian Sector](#)

Risk Sharing Platform, [Risk Sharing Framework](#), 2023

UNOCHA, [Handbook for the UN Resident and Humanitarian Coordinator](#)

Laurence Boisson de Chazournes, Luigi Condorelli, [Common Article 1 of the Geneva Conventions revisited: Protecting collective interests](#), *International Review of the Red Cross*, No. 837, 31 March 2000.



2. PRINCIPLES IN PROTECTION WORK

Respecting the principles of humanity and impartiality (including non-discrimination)

- S** 2.1 Protection actors must ensure that the principle of humanity is at the core of their work.
- S** 2.2 Impartiality must guide protection work.
- S** 2.3 Protection actors must ensure that their activities do not have a discriminatory effect.

Avoiding harm

- S** 2.4 Protection actors must ensure that their work does not cause harm.
- S** 2.5 Protection actors must contribute to the capacity of other actors to ensure that their actions do not cause harm.

Putting affected people at the centre of protection activities

- S** 2.6 Protection work must be carried out with due respect for people's dignity.
- S** 2.7 Protection actors must base their work on meaningful engagement with people at risk and ensure they are engaged throughout the design and implementation of any protection action.
- G** 2.8 Protection actors should learn from and build on the capacities of individuals and communities, to strengthen their resilience.
- G** 2.9 Protection actors should assist affected people in accessing information that can help them avoid or mitigate risk.
- G** 2.10 Protection actors working with affected people should inform them of their rights and of the obligations of duty bearers to respect them.

INTRODUCTION

This chapter describes the main principles that are central to protection work by humanitarian¹⁵ and human rights actors and are common to all protection work.

The first section underlines the principles of humanity and impartiality, highlighting the aspect of non-discrimination. It also emphasizes that it is concern for people at risk that drives protection work. These are the principles that underlie international humanitarian law and form an indispensable part of efforts to establish and maintain humanitarian access and to protect people at risk.

The principles of neutrality and independence are often crucial for gaining access to and maintaining proximity with the victims of armed conflict and other 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 or practical reasons), they may not be so for all organizations, and the importance an organization attaches to these principles may vary according to its identity, mandate and operational realities. So while the principles of humanity and impartiality are fundamental to the protection work of all humanitarian and human rights actors, the principles of neutrality and independence are not. Protection actors should nevertheless aim for openness 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 actions that could aggravate the situation of those they seek to help. It explains that protection work can be extremely sensitive and can have severe consequences for the population. Responsibility for managing and mitigating these risks lies with the actor doing the work.

The last section explains 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 physical well-being is essential to the effectiveness of this work. This in turn entails ensuring that they play a key role, influencing decisions and making practical recommendations based on their intimate understanding of the threats, violations and abuses to which they are exposed. It is also important to strengthen the capacities and coping mechanisms of communities and individuals.

¹⁵ Both the present 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-centric approach.

A principled approach to protection work

Practitioners will face challenges that require them to take tough decisions guided by the principles mentioned above and to find and maintain the right balance between them. Challenges such as lack of access to affected people, lack of security or logistical constraints often limit protection actors' ability to deliver an impartial, non-discriminatory response. Prioritizing one principle over another may sometimes be appropriate, provided this is based on a thorough analysis of the challenges and aimed at achieving effective protection outcomes. The principle of "do no harm" must remain central, however, and must not be compromised.

These constraints and choices need to be identified, explained and discussed with other humanitarian and human rights actors, donors, the population concerned and others.

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, armed conflict or a lack of security 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 areas – 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 AND IMPARTIALITY (INCLUDING NON-DISCRIMINATION)

S

2.1 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 – is 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 dignity, alleviating suffering and ensuring respect for the rights, dignity and psychological and physical well-being of anybody at risk.

S

2.2 Impartiality must guide protection work.

The non-discrimination aspect of the principle of impartiality guards against adverse distinction in the treatment of 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 aim of impartiality is to ensure that protection activities address all relevant rights and obligations, together with the most urgent protection needs of communities and individuals affected that are experiencing or are at risk of violations and abuses.

The principle of impartiality – when linked with that of neutrality – also implies consistency in 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 protection risks using objective criteria.

The application of these principles also entails the inclusion of diversity factors such as gender or age and as indicated in Standard 2.3 below. For example, 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 necessary skills. Some groups may have heightened vulnerabilities related to particular situations, such as ethnic, religious or tribal minority groups and LGBTQ+ people. Protection actors must take such vulnerabilities or risk factors into account in order to analyse protection risks, to ensure that critical protection risks are prioritized and addressed and to ensure that protection responses do not cause or exacerbate marginalization or discrimination.

Prioritizing protection risks is the means by which non-discrimination is applied. This means that if a protection actor has to prioritize which protection risks to address, the criteria guiding such choices must be non-discriminatory and based on the urgency and severity of the risks.

The challenge of respecting the principle of impartiality is often compounded by the complex operating environment in which protection work takes place. Protection actors must make difficult choices regarding the protection risks to prioritize in their response. Focusing on specific groups within a community (e.g. children associated with armed groups/armed forces or people in detention), may run counter to what the majority of the community perceives as their priorities. While these groups may genuinely be the most vulnerable or the most exposed to protection risks, other sections of the community may perceive the protection actor as biased or unresponsive if it prioritizes those groups. Protection actors hence need to ensure effective two-way communication with the affected community at all stages and factor the mitigation of potential challenges to social cohesion within or between communities into their response.

Bias may also result from unequal access to information by affected people or the collection of information by protection actors in a way that excludes segments of the population (e.g. conducting assessments via phone or digitally). If remote information collection is the only option, any access limitations need to be factored into the data analysis, as that analysis may otherwise result in discriminatory or exclusionary advocacy and programming choices. This is developed further in Chapters 7 and 8.

Finally, problems such as inaccessibility owing to denial of access, lack of security or infrastructure constraints may limit the ability of protection actors to respond in an impartial and non-discriminatory manner. Humanitarian leaders must monitor and mitigate these constraints, so that protection actors can do their work. Equally, two-way communication with crisis-affected people is crucial, to communicate the scope and limitations of protection actors' activities and to ensure that the response meets people's needs.

S

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

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, a protection risk analysis must not discriminate between people with similar needs or vulnerabilities, based solely on their status. The response may take into account a particular status, but must also ensure that risks 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 needs of particular groups within any population at risk, so all can assert their rights. For example, population groups with recognized vulnerabilities, such as children (or multiple vulnerabilities, such as children with disabilities), may need targeted protection activities conducted by protection actors with the necessary skills. Some groups may have heightened vulnerabilities related to particular situations, such as ethnic, religious or tribal minority groups and LGBTQ+ people. However, protection activities should not be focused on one group with particular needs, if this would be to the detriment of another portion of the affected population that is suffering particular abuse or violations. This could be the case, for example, when abuses causing displacement of a certain population focus attention on internally displaced people (IDPs) to the exclusion of people exposed to similar protection risks within the host community.

It is the collective responsibility of all actors engaging in protection work to ensure that no high-risk group is overlooked and that the overall response of the many protection actors involved in a given context is non-discriminatory. Please see Chapter 5 regarding effective complementarity among actors responding to the needs of diverse segments of the affected population.

Impartiality and people with disabilities

In armed conflict and other violence, people with disabilities may be extremely vulnerable and have specific protection concerns. The principle of impartiality requires that protection actors address the rights and needs of people with disabilities, take into account the specific risks that they face and treat their needs as a matter of priority.

As people with disabilities are often among the least visible members of communities affected, protection assessments are likely to overlook them. Protection workers should therefore identify people with disabilities, to analyse and address their needs.

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

AVOIDING HARM

S

2.4 Protection actors must ensure that their work does not cause harm.

Poorly conceived or carelessly implemented protection activities can exacerbate protection risks or even generate new ones (see Chapter 3 and 8 regarding protection risks related to digital technologies). Although it is often extremely difficult to foresee the consequences of activities or to know when an action could cause harm, 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 information gathering and use – are being designed, analysed, implemented or monitored.

Protection activities can inadvertently expose individuals or groups to further risk, which is one reason why it is essential to involve affected people in the analysis of protection risks and in response planning. Where communities are taking the lead on activities for their own protection, protection actors must conduct a thorough analysis to ensure that their support for community-led efforts respects this standard (see the textbox on community-based protection).



2.5 Protection actors must contribute to the capacity of other actors to ensure that their actions do not cause harm.

Staff involved in protection activities are expected to have particular expertise in 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 and ensuring the centrality of protection throughout the overall humanitarian response. 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.

All humanitarian actors should contribute to protection outcomes, meaning they should consider protection risks at the basis of their humanitarian activities. They must use a “protection lens” in their analysis and incorporate protection risks in their response, for example in the context of “protection mainstreaming” or “good quality programming” or in the application of the “do no harm” principle. Protection actors must encourage and contribute to discussion of these concerns among non-protection experts and suggest measures they could take to reduce such protection risks.

In extreme cases, an authority¹⁶ can manipulate the mere presence of humanitarian actors as part of its strategy of continuing to violate 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”. Many humanitarian actors that are not mandated or specialized protection actors have recognized the need to ensure a minimum protection capacity within their organization.

¹⁶ In this document, the expression “authority” covers all primary duty bearers as defined in Chapter 6, 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 people or a population and who are responsible for protecting those who fall under their control.

Protection outcomes

A response or activity is considered to have a *protection outcome* when the risk to affected persons is reduced. The reduction of risks occurs when threats and vulnerability are minimized and, at the same time, the capacity of affected persons is enhanced. (*IASC Protection Policy*)

Factors contributing to protection risks are the actual or potential exposure of affected people to protection risks, i.e. human action or the effect of human action resulting in violence, coercion or deprivation, deliberate or otherwise. Reducing protection risks includes changing the behaviour of perpetrators, primary duty bearers and other authorities that have the duty to protect people, to prevent or reduce the threats civilians face and their vulnerability to those threats.

Reducing protection risks also includes

- helping affected people strengthen their capacities
- providing them with opportunities to avoid harm
- restoring their dignity and living conditions
- strengthening the shock-resilience of systems on which people rely for critical services.

All these activities involve reducing risk through improved respect for the rights of victims and restitution for the abuse they have suffered. They aim to diminish threats and vulnerabilities and to enhance capacities. Protection actors can also enhance the environmental conditions that influence behaviour, policy and practice.

PUTTING AFFECTED PEOPLE AT THE CENTRE OF PROTECTION ACTIVITIES

S

2.6 Protection work must be carried out with due respect for people's dignity.

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

Measures to respect, safeguard and promote the dignity of people at risk also include ensuring their inclusion and meaningful participation in decision-making processes that affect them, facilitating their access to accurate and reliable information and supporting their independent capacities, notably those of making free and informed choices and of asserting their rights.

S

2.7 Protection actors must base their work on engagement with people at risk and ensure they are meaningfully engaged throughout the design and implementation of any protection action.

Recognizing that crisis-affected people are the primary experts regarding their lives, even under the most difficult circumstances, protection actors should at the very least seek out the experiences, analysis and recommendations of affected people. The distribution of roles and responsibilities between affected people and protection actors in protection activities may differ, with more or less involvement of affected people depending on their preferences and the operational environment. Protection programming must be as inclusive as possible and involve affected people throughout the entire programme cycle. In addition to formal community representatives, it is useful to identify forums and associations, which may represent the

interests of diverse groups within the community, such as youth or women's groups or associations for people with disabilities. The inclusion of people facing protection risks is also crucial to ensure that protection activities support self-protective actions and enhance capacity.

Affected people or their families, groups and communities might be able to document violations and abuses that they have suffered or witnessed. Communities can compile lists of missing people and 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 apply the standards regarding evidence and other aspects of good practice for documenting violations and abuses and do so without placing people at risk. This is particularly important if there is a possibility that the information gathered will be referred to during a formal inquiry.

Trust needs to be built, to ensure open and constructive dialogue with affected people. Special sensitivity and training are needed to engage in dialogue with affected people, especially when interviewing children, the families of missing people and victims/survivors of sexual abuse, and their families.

Other barriers may also exist. Engaging selectively with people on specific issues may render their diversity factors more visible and thus put them at risk (e.g. families of known political opponents, HIV-positive detainees, etc.). Protection actors must provide safe spaces where people can express themselves freely without fearing negative repercussions. Examples include providing emergency health care for survivors/victims of sexual violence in general health-care centres and not asking sensitive questions in group discussions with affected people. In other instances, protection action may rely on maintaining confidential dialogue with the authorities, and it may only be possible to involve the community to a limited extent if that confidentiality is to be respected. In such cases, protection actors should nevertheless obtain informed consent when collecting information, and discuss the purpose, potential risks and benefits of the protection activity with the community, without divulging confidential information.

Even in the case of protection dialogue or advocacy, once implementation of a protection activity has begun, protection actors should, where possible, re-visit the affected population to inform them of progress made or problems encountered. Protection actors should take this opportunity to enquire about and monitor any positive or negative consequences for the population. If the protection response is of long duration, e.g. when tracing missing people, the protection actor should consult the community periodically to gather any new information and report on progress.

The relationship between affected people and protection actors is characterized by a marked imbalance of power and access to resources. The rapid spread of communication technologies has enabled many individuals and communities to mobilize public opinion when abuses and violations are being committed and – directly or indirectly – to mobilize humanitarian and human rights organizations. This is also true during armed conflict and other violence. People may therefore be able to collectively influence the agendas of these organizations. Furthermore, unequal access to information technology means that some voices will be magnified over others.

Although some communities might use social media to publicize their dissatisfaction, they 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 they should address the underlying issues raised.

Protection actors are often formally accountable to some form of oversight body, such as member states, boards of directors or donors. However, these bodies may have only a limited relationship with affected people at best. In many cases, protection actors also work with local operational or implementing partners, further removing the relationship between the oversight body and the affected people, to both of whom the protection actor is accountable. They must mitigate this structural deficiency and establish a reasonable level of accountability to people at the centre of protection activities. Two-way communication with affected people, for instance through formal complaints mechanisms or hotlines available in local languages, is one way of ensuring that people's concerns are adequately integrated in programmes that affect their lives. Protection actors need to ensure that such mechanisms are as accessible as possible and do not exclude certain segments of affected communities, such as people who are elderly, illiterate, or have visual or hearing impairments.

Accountability of humanitarian actors

The *Core Humanitarian Standard* glossary defines “accountability” as:

“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

2.8 Protection actors should learn from and build on the capacities of individuals and communities, to strengthen their resilience.

Those at risk usually have the clearest understanding of the risks they face (types of threat, potential perpetrators, times when risks are higher, etc.). They often know some of the most effective means of mitigating these risks. Protection actors should work with affected communities to assess the individual and collective capacities for protection that exist within those communities. At a minimum, protection actors must ensure that their own actions do not diminish these capacities. More ambitiously, they should try to reinforce these capacities and to strengthen the resilience of communities over time.¹⁷ The textbox on community-based protection below explains this in more detail.

When supporting community-based protection mechanisms, protection actors must nevertheless be aware of the limits to this strategy, as it is the responsibility of the authorities to protect people. Whenever feasible, protection actors should thus favour a longer-term strategy that builds on the capacity of affected populations to organize themselves and engages with the authorities at all levels to safeguard their rights. See Chapter 6

¹⁷ For considerations related to digital technologies and risk, see Chapter 8, particularly Standard 8.9.

Community-based protection

Community-based or community-led approaches to protection adopt a “people-centric” intent, which aims at helping people affected by crisis to better navigate the difficult circumstances they face.

In recognizing that crisis-affected people are the primary experts regarding their lives, even under the most difficult circumstances, protection actors should, at the very least, seek out the experiences, analysis and recommendations of the affected community and build on those communities’ capacities and agency. Community-based protection comprises a spectrum of approaches ranging from more agency-led responses to interventions led by the communities themselves and supported by protection actors.

- Community-based protection entails collaborating with the community on all aspects of the programme cycle, conducting assessment, analysis, design and implementation together and combining first-hand insights with the protection actors’ technical expertise to guide prevention and response activities.
- Community-led protection responses are initiated by communities themselves, with or without the support of external protection actors.

Crisis-affected people are often forced to take independent action to prevent and respond to protection risks. They are often the first responders to the protection risks in their contexts. The role of the protection actor is therefore to help them find long-term solutions to the challenges they face, devising more feasible strategies to better tolerate, absorb, cope with, avoid or confront the primary threats they face.

In community-based protection programmes, the communities themselves control the decision-making. The protection actor takes a supportive role, contributing logistics and materials support, brokering relationships and facilitating access to duty bearers, while offering technical expertise and coaching as needed.

To build acceptance and trust from the affected community and mitigate any harm, protection actors must understand the composition of the community, its culture and the social attitudes that fuel social power dynamics (e.g. leadership and inclusion and exclusion dynamics). This analysis will help the protection actor identify those people who are most affected, vulnerable and at risk, along with the power dynamics within and between communities.

Affected people are often those who are most marginalized, with the least voice and influence. They may therefore be relatively invisible. This type of analysis is essential, to provide spaces in which community members can express themselves freely and their voices be heard. The absence of such analysis exacerbates the risk that protection actors will reinforce exploitative and/or abusive social power dynamics and further marginalize those who are already on the margins.

Protection actors and communities should jointly analyse protection risks facing the community, by unpacking threats, vulnerability factors and existing capacities. While affected people themselves typically have a better understanding of the threats they face than external actors, protection actors may possess information and insights that can help nuance their understanding of the risks. For example, without disclosing sensitive information, protection actors can communicate their reading of the protection context to communities if doing so may help the community draw up better protection strategies. A protection actor may be able to provide information on the risks posed by mines and explosive remnants of war, for instance.

In line with the principle of “do no harm”, the protection actor and the community should jointly identify and manage the risks to which community-based protection programming can expose communities, community protection actors and external protection actors.

In working collaboratively with communities, the protection actor should promote specific principles. By emphasizing the spirit of the principles of impartiality and humanity (i.e. response according to urgency of need), protection actors can promote inclusiveness. This presents empathy and compassion as essential resources on which the community can draw in difficult times. The protection actor can also support the will and capacity of affected communities to work together to find collective solutions by fostering the spirit of these principles.

Fragmentation of the social fabric owing to the socio-political dynamics and implications of conflict can exacerbate social stigma and discrimination, e.g. against victims/survivors of sexual violence, people associated with armed groups and minority groups. Collaborative approaches supported by protection actors can help communities boost individual and collective resilience, enhancing coping capacities and self-protection mechanisms.

Community-based efforts should be seen as part of a larger collaborative protection strategy, with efforts by other actors being designed to complement these community-based efforts. The protection actor should also address the root causes of the threats, either collaboratively with the community or in consultation with them.

G

2.9 Protection actors should assist affected people in accessing information that can help them avoid or mitigate risk.

While affected people typically have a better understanding of the threats than external actors, protection actors may possess information and insights that can help nuance their understanding of the risks. To make informed choices and develop resilience, self-protection and coping mechanisms, communities and individuals at risk need a nuanced understanding of the threats to which they might be exposed. Without disclosing sensitive information, protection actors can communicate their reading of the protection context to communities if doing so may help them draw up better protection strategies.

Protection actors should communicate their analysis of abuses, violations and related trends to affected individuals and communities if doing so will help them enhance their own protection strategies. One area where this is typically done in a coordinated manner is with regard to the risks posed by mines and explosive remnants of war. Nevertheless, 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 locations of mobile checkpoints along roads they have just travelled, movements of troops they have witnessed or the presence of a local rebel group commander in a village they have recently visited. What local authorities and armed actors perceive as military intelligence may vary from one context to another. Protection actors should be attentive to the way armed actors perceive them and should communicate about their activities, to avoid misperceptions. People who have already been affected by abuses and violations also need to receive adequate and timely information on the services and support they can obtain (see Guideline 5.5).

G

2.10 Protection actors working with affected people should inform them of their rights and of 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 duty bearers. That may involve working with various associations – such as those of families of missing people – women’s groups, representatives of indigenous peoples and minority groups, disabled people’s organizations or LGBTQ+ organizations. This may take time, especially when working with people who are not well informed regarding their rights under domestic and international law.

ANNEXES TO CHAPTER 2

ANNEX 1: PROTECTION WORK FOR PEOPLE WITH DISABILITIES

According to the *Convention on the Rights of People with Disabilities*, “disability results from the interaction between people with impairments [physical, visual, hearing, speech, psychosocial and intellectual] and barriers [attitudinal, communication, physical and institutional] that hinder their full and effective participation in society on an equal basis with others”.¹⁸

According to the World Health Organization, about 16% 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, people with disabilities are often overlooked in humanitarian emergencies and lack access to adequate protection and support.

People with disabilities are not a homogeneous group. They are diverse in their experience, in the ways that barriers impede their participation and inclusion in humanitarian action and in their identity, including their age, gender, ethnicity, location and race. Owing to the intersectionality of these factors, people with disabilities face greater marginalization and discrimination in humanitarian action.¹⁹ At the same time, the principles of humanity, non-discrimination and impartiality require that protection actors respond to the needs and rights of people with disabilities. They are among the most at-risk groups in armed conflict and other violence and experience particular threats and challenges.

When populations affected by conflict flee to safety, people 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, making them even more susceptible to threats. People with disabilities are also often excluded from social networks, which provide much-needed support during 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.

To address the protection needs of people with disabilities and the specific barriers and threats they face, protection actors must collect data and disaggregate those data not only by gender and age but also by disability.²⁰

¹⁸ United Nations, [Convention on the Rights of Persons with Disabilities](#), Preamble, para. e.

¹⁹ IASC, [IASC Guidelines, Inclusion of People with Disabilities in Humanitarian Action](#), 2019.

²⁰ Disability data should be collected in accordance with the [guidelines set out by the Washington Group on Disability Statistics](#). See also DFID, [Guide to Disaggregating Programme Data by Disability](#) and ICRC, [Sex, Age and Disability Data Disaggregation Framework](#).

However, biases in the collection and/or assessment of information often prevent protection actors from addressing the risks that people with disabilities face. For example, protection workers conducting an assessment may not immediately notice large numbers of people with disabilities because these people may be confined to their homes. This may cause them to wrongly infer that there is no one with a disability among the affected population. Protection workers should therefore actively look for people with disabilities.

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

The failure to include people with disabilities in protection activities and in other sectors of the humanitarian response may harm them and their families and exacerbate their marginalization. For example, if food distributions or sanitation and hygiene facilities are inaccessible to people 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 to protection concerns affecting people with disabilities and on how to mitigate them.

Upholding the rights and dignity of people with disabilities must guide all protection activities, so protection workers should always consult people with disabilities and their representative organizations and involve them in the planning, implementation, monitoring and evaluation of all activities affecting them. People 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 people with disabilities, protection actors should pay particular attention to confidentiality and privacy – which may include privacy from their families or caregivers – and support the right of people with disabilities to make their own informed choices. That support may include using alternative means of communication, such as sign language.

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

Humanitarian organizations increasingly acknowledge the challenges faced by people with disabilities in emergencies and the need to better include them in humanitarian response. The *Humanitarian Disability Charter* was launched in May 2016 at the World Humanitarian Summit in Istanbul.²¹ In the Charter, states, humanitarian NGOs, UN agencies and disabled people's organizations committed to removing barriers to relief, protection and recovery support for people with disabilities and ensuring their participation in humanitarian programming.

²¹ [The Humanitarian Disability Charter](#), 2016.

ANNEX 2: REFERENCE MATERIAL FOR CHAPTER 2

[Charter on Inclusion of People with Disabilities in Humanitarian Action](#)

[Core Humanitarian Standard](#)

DFID, [Guide to Disaggregating Programme Data by Disability](#), 2015

GPC, Explanatory Note on Protection Risks, 2023

IASC, [IASC AAP Framework](#), 2023

IASC, The Centrality of Protection in Humanitarian Action, IASC Principals' statement, 2013

ICRC, [Enhancing Protection for Civilians in Armed Conflict and Other Situations of Violence](#), 2013

ICRC, [Sex, Age and Disability Data Disaggregation Framework](#), April 2023

Save the Children, [Minimum Inter-Agency Standards for Protection Mainstreaming](#), 2012

The Sphere Project, [Humanitarian Charter and Minimum Standards in Disaster Response](#), 2011

[Washington Group on Disability Statistics](#)

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

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

Mahony, Liam, [Proactive Presence: Field Strategies for Civilian Protection](#), Centre for Humanitarian Dialogue, Geneva, 2006

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



3. MANAGING PROTECTION STRATEGIES

Protection analysis and identification of critical protection risks

- S** 3.1 Based on the experience and input of affected communities, protection actors must undertake a context-specific analysis of protection risks, including the prevailing threats and vulnerabilities related to those threats. They must also analyse the capacity of primary duty bearers to prevent and mitigate those threats, and of people's capacity to recover from them. Humanitarian and human rights actors must meaningfully engage with the affected population and with others to conduct and update analysis and to identify priority critical protection risks.

Response planning and implementation

- S** 3.2 Protection actors must work in a coordinated and complementary manner and with other key actors to identify the main drivers of protection risks – the sources of threats, vulnerabilities and capacities – and the ways in which those drivers can be positively addressed. This “causal logic” must be developed with affected communities and must describe both the desired outcome and the intermediate points at which the drivers of specific protection risks can be addressed.
- G** 3.3 This “causal logic” should serve as the basis for developing the protection strategy, which includes defining the roles of the sectors and/or actors contributing to the desired outcome and identifying assumptions inherent in the strategy.

Monitoring, evaluation and learning

- G** 3.4 Protection actors should take an iterative approach to the monitoring, evaluation and modification of the strategy. They should carry out regular analysis of changes in patterns of protection risk and the monitoring and evaluation of outcomes – or lack thereof – of ongoing or completed actions, with a view to evaluating progress towards the achievement of protection outcomes and ensuring accountability for the actions taken. Changes in patterns of protection risk and lessons learned should be incorporated into protection strategies periodically, as required.

The standards and guidelines in this chapter refer to the main stages of the project management cycle that most organizations use. They highlight elements particular to protection work that should be taken into account, such as context-specific analysis, development of strategies and monitoring and evaluation.

Revision of these standards was driven by the growing understanding that “protection” needs to achieve measurable protection outcomes, i.e. reductions in protection risk. “Protection risk” is the probability of violence, coercion and deprivation, deliberate or otherwise. To analyse protection risk, one must assess the threat and its underlying factors, the relative vulnerability of those exposed to it and their capacity to prevent, mitigate or recover from those threats. Actors that contribute to reducing protection risks include not only humanitarian and human rights organizations with specialized protection activities, but also humanitarian actors that focus on reducing vulnerabilities or increasing the capacity of affected people through assistance activities. This chapter is for all these actors, and in this chapter “protection actor” includes all actors that help to reduce protection risk.

The terminology in this chapter may differ from that used by certain organizations regarding analysis, strategy, objectives, outcomes, etc.

PROTECTION ANALYSIS AND IDENTIFICATION OF CRITICAL PROTECTION RISKS



- 3.1 Based on the experience and input of affected communities, protection actors must undertake a context-specific analysis of protection risks, including the prevailing threats and vulnerabilities related to those threats. They must also analyse the capacity of primary duty bearers to prevent and mitigate those threats, and of people’s capacity to recover from them. Humanitarian and human rights actors must meaningfully engage with the affected population and with others to conduct and update analysis and to identify priority critical protection risks.

“Protection analysis is a process undertaken to identify protection risks with the aim of guiding protection strategies and responses.”²² A thorough protection risk analysis should include identification and understanding of:

- the sources, perpetrators and drivers of prevailing threats
- the characteristics or combinations of characteristics that make people or communities vulnerable to those threats
- the capacities of primary duty bearers to prevent or mitigate those threats and/or the capacity of affected people to prevent, mitigate or recover from them.

PEOPLE-CENTRIC PROTECTION

The agency, interests and well-being of the population must guide the process. The population must participate in context analysis and in conceptualizing, developing and implementing the reduction of protection risks. People in dangerous areas often have very clear ideas about the drivers of protection risks and the types of action that will most effectively reduce the risks they are experiencing. Analysis should be co-developed with the population that is subject to violations or abuses. Affected people should be central to all aspects of the development, implementation and evaluation of protection strategy, including the identification and prioritization of protection risks, together with the identification of primary drivers of protection risk and how to positively affect them.

²² GPC, [Protection Analytical Framework](#).

Humanitarian actors should facilitate two-way information flow with affected people; this includes engaging them in interpreting the results of the protection analysis. Humanitarian actors should be mindful of gatekeepers of information, as they are capable of both supporting the flow of information to and from affected people and acting as barriers to this flow.

Even during the acute phases of conflict, violence or other emergencies, protection analysis should be co-conducted with a broad cross-section of the population experiencing or at risk of violations or abuses, wherever practicable and safe. Care should be taken to include people and groups that may experience marginalization or discrimination, as they may otherwise be prevented from voicing their concerns.

A MULTIDISCIPLINARY APPROACH

Protection analysis requires the involvement of various disciplines, sectors and actors – including human rights, peacebuilding, peacekeeping and development actors, academics and local civil society. This is necessary in order to fully understand the factors driving certain protection risks – including the root causes – and to identify the possible means of reducing those factors, even if some of those means fall outside the scope of humanitarian action. Collaboration and coordination are essential, both within teams and organizations and with others, to build upon existing efforts to identify and understand protection risks and to avoid duplication of effort.

The voice and knowledge of the affected population, local staff, partners on the ground and front-line workers are essential. The actor leading on the protection analysis must ensure this happens, through direct participation in preparation meetings, bilateral conversations or joint analysis sessions. Participation in a protection analysis process must be broad, to ensure that its development and interpretation include rights holders, who are best placed to identify the risks they experience and guide the analysis of what those risks mean for their lives.

The protection analysis process must also include the following:

- Data experts: People and actors able to guide and support the collection, understanding and technical interpretation of data.
- Subject matter experts: People and actors with protection and other specific thematic or sector knowledge in the context who can help interpret the results and can guide collective decision-making.
- Context/cultural experts: People and actors with the context knowledge to guide the acquisition of qualitative and quantitative information and provide regular interpretation of information.
- Decision makers, when possible: People and actors in charge of strategic, programmatic and operational decision-making, including local leaders and others with a high social or cultural profile.

A DYNAMIC APPROACH

Protection analysis should not be treated as a one-off exercise, but should take place regularly 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 stakeholders, to clarify assumptions, develop partnerships and formulate strategies to address risks more comprehensively.

While it may not have a specific starting point, the protection analysis may be triggered by a specific occurrence, shock or event and once triggered, it should be an iterative and regular process so it can reflect the evolving context. When defining the protection analysis timeframe, it is important to consider contextually relevant events or seasonal dynamics that affect the population.

It is essential to identify an individual protection threat and build from there. Data and information should include the locations at which the threat is present, the population groups affected, the consequences of the threat and the capacities available to address it. There may be several protection threats in a single context, which may need to be prioritized to ensure the analysis is appropriately focused.²³

²³ *Ibid.*

RESPONSE PLANNING AND IMPLEMENTATION

S

3.2 Protection actors must work in a coordinated and complementary manner and with other key actors to identify the main drivers of protection risks – the sources of threats, vulnerabilities and capacities – and the ways in which those drivers can be positively addressed. This “causal logic” must be developed with affected communities and must describe both the desired outcome and the intermediate points at which the drivers of specific protection risks can be addressed.

G

3.3 This “causal logic” should serve as the basis for developing the protection strategy, which includes defining the roles of the sectors and/or actors contributing to the desired outcome and identifying assumptions inherent in the strategy.

AN OUTCOME-ORIENTED APPROACH

Reducing protection risks means addressing their main drivers.

This requires the following actions:

- Directly reducing the threat (e.g. through direct or indirect engagement with armed actors to influence their behaviour towards civilians).
- Reducing the vulnerabilities of people exposed to the threat (e.g. by providing assistance so as to reduce exposure to violence).
- Strengthening the capacities of crisis-affected people and other local/national actors to prevent and respond to the threat (e.g. by supporting communities’ engagement with duty bearers to claim their rights).

It is unlikely that a single type of activity will comprehensively reduce protection risk. Even within a single organization, reducing protection risk is likely to require a variety of disciplines and sectors working towards a common strategic outcome.

Pulling all actions together into a collective strategy will be greatly aided by the development of a context-specific “causal logic” (or theory of change), which identifies key drivers of protection risks and the action needed to positively affect those and make progress towards a chosen outcome. This causal logic should describe the key indicators – such as changes in behaviour, attitudes, policy or practice – linking protection risks and a reduction in those risks. It should also describe the sequence of actions required and the sectors and disciplines that need to be mobilized to achieve the desired outcomes.

The process of developing this “causal logic” can serve as the basis for establishing a collective vision, which can then be combined with SMART objectives and specific activities to form a comprehensive strategy.

A COORDINATED AND COMPLEMENTARY APPROACH

Clearly identifying the drivers of protection risk and the interventions most likely to effectively counter those drivers enables humanitarian and non-humanitarian actors to identify the unique role that each can play.

Roles and contributions are potentially very diverse. In addition to specialist protection inputs, these can include the following:

- 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.
- Instances where “traditional” humanitarian sectors can and should play an active role in reducing protection threats and vulnerability to those threats, and in increasing people’s capacity to withstand them. For example, food assistance can constitute a protection intervention when food distributions are prioritized for communities where food insecurity is driving child recruitment into armed groups.

The findings of the protection analysis should lead to identification of the most critical protection risks. This in turn will provide the basis for joint prioritization exercises.

Once the protection risks have been prioritized, the joint protection strategy process can be supported by identifying complementary action to address the causes of threats and of vulnerability to those threats, together with factors that are impairing people's capacity to withstand them. This action falls into the following categories:

- Responsive action: Assessing, preventing and responding to immediate harm and abuse. This may require complementary action, including direct protection and non-protection interventions, local conflict resolution or humanitarian diplomacy and advocacy.
- Remedial action: Restoring people's dignity and living conditions. This could involve specific sector assistance (food security, water, sanitation and hygiene, education, etc.) from both humanitarian and development actors.
- Environment building: Fostering an environment that creates the conditions for full respect of people's rights, including their agency. This may for instance require dedicated human rights engagement or specific efforts by organizations.

Not all these types of action will fall within the role or capacity of humanitarian or human rights actors.

MONITORING, EVALUATION AND LEARNING

G

- 3.4 Protection actors should take an iterative approach to the monitoring, evaluation and modification of the strategy. They should carry out regular analysis of changes in patterns of protection risk and the monitoring and evaluation of outcomes – or lack thereof – of ongoing or completed actions, with a view to evaluating progress towards the achievement of protection outcomes and ensuring accountability for the actions taken. Changes in patterns of protection risk and lessons learned should be incorporated into protection strategies periodically, as required.

MONITORING

Monitoring activities have been integrated more systematically in protection activities over recent years. However, it is still difficult to ensure that analysis and monitoring are designed to effectively measure protection outcomes – or the lack thereof. Monitoring of protection outcomes cannot rely solely on project or programme mechanisms that are designed to measure the outputs of activities. Monitoring should also include gathering observational and other qualitative information that can help identify changes in behaviour, patterns and the agency of populations.

Taking 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:

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

Information management and monitoring systems should include the choice of indicators, methods and procedures for collecting information, how the data will be used and by whom.

Every effort must be made to draw on information available to other actors, in order to avoid duplication and to triangulate information (see Chapter 7).

Protection information management systems should be designed to meet these protection analysis and monitoring needs, to ensure that protection strategies are treated not as linear processes but as iterative and adaptable processes that are sensitive and responsive to complex and dynamic realities (see Chapter 7).

Measuring the outcomes and results of protection strategies presents considerable challenges. The more precisely the protection analysis identifies protection risks, the more feasible it is to define and precisely describe the risk patterns faced. Protection risks should be identified with the affected population, to establish a baseline of risk factors that a protection strategy seeks to address and ultimately reduce in order to achieve a protective outcome. In addition, the causal logic that underpins the strategy serves as a basis for monitoring the critical milestones that lead to a reduction in protection risk.

Establishing a purely quantitative baseline against which to measure outcomes and impact is often very difficult. In any case, there are other reasons for not even attempting to do so. One of these is that collecting information related to protection risks may be sensitive or may risk re-traumatizing victims of violations. For instance, practical and/or ethical considerations may make it impossible to collect information on the frequency of sexual violence against women. 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 began.

Confidentiality permitting, multi-stakeholder joint-analysis processes should examine quantitative data to identify critical information and related proxy indicators so that one can interpret changes in the effects of the threats affecting the population, together with behaviour, policies and other critical patterns.

However, when a protection analysis is carried out to identify the factors contributing to violations, abuses and risk patterns, those factors can then be used to define key indicators to monitor the underlying threats, vulnerabilities and capacities. Tracking whether these variables – the risk drivers – are going up or down should make it possible to deepen and refine the protection analysis and use it as a basis for continually assessing whether the strategy is on track to achieve the desired results and, if it is not, to undertake course adjustments. This should also make it possible to detect new risk factors and any negative consequences of implementing the strategy. Monitoring is essential to ensure that programmes are developed and implemented in an iterative manner 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, etc.) of their safety or the degree to which they are increasing or reducing their movements in a given area. Such proxy indicators can reveal shifting trends affecting a protection problem. Indicators and data-collection methods should be selected in consultation with the people at risk wherever possible.

Different actors will approach this regular protection analysis in different ways, depending on their mandates and expertise and on how analysis influences the ultimate outcome they seek to achieve. For example, human rights monitoring is central to the work of human rights organizations, providing the basis for their analyses and activities and ultimately for improved and strengthened protection outcomes. Human rights analysis should be incorporated in humanitarian protection analysis as much as possible.

Once the causal logic underpinning the response strategy has been established, the milestones leading to reduced risk and underpinning programme design serve as the basis for programme monitoring. Monitoring programme implementation against these milestones, including key activities and progress, 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 reducing risk or whether the assumptions and strategy need to be revised.

One way to overcome the difficulty of measuring protective outcomes is to use “result monitoring” to track changes in the behaviour of perpetrators, the actions of the authorities responsible, the behaviour of other actors (e.g. regional/international actors who have an influence on the situation) and the actions of the people affected. 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 indicator can be devised, depending on the expected results specified in the SMART objectives.

Different types of indicator and information source should be used to triangulate analysis and, whenever possible, to assess the degree to which a change in the risk factors can be attributed to the action of specific actors. In addition to using indicators, assessing the effects of a protection action should also involve a more general analysis of changes in the political, social or economic contexts. 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 directly attributed.

When deciding on the most relevant indicators, organizations should be realistic regarding the resources they will need. A balance must be struck between the expected benefit of the information provided by the indicator and the resources needed to collect and analyse it. Protection actors must also avoid causing harm when conducting monitoring activities (see Standards 2.4 and 2.5, and Chapter 7).

The difficulty of establishing measurable results and attributing these results to specific actors should not deter humanitarian actors from innovating in this challenging area or tackling complex protection issues. In addition, some organizations are mandated to carry out certain protection activities, meaning that regardless of difficulties in measuring outcomes, they have an obligation to carry out protection activities and are accountable not only for the results they achieve but also for fulfilling their mandate.

EVALUATION AND LEARNING

Things change rapidly in a crisis. This necessitates regular protection analysis, including monitoring of the risks that humanitarian actors seek to address, to maintain a high degree of adaptability. Cultivating and encouraging adaptability in programming de-emphasizes simplistic success/failure judgements 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 work benefits from allowing time for protection actors to regularly reflect on the action taken to reduce risk, and to review and adapt their objectives and activities. While informed risk-taking should be encouraged, it is the implementing organization and its financing partners that must bear those risks, not the affected population.

Regular investment in learning – involving affected people, staff and others – enhances ownership of and responsibility for the methods, processes and results of protection strategies. Organizations engaged in protection should also encourage adaptability and 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.

Evaluation of the entire protection action may be conducted whenever necessary in order to capture and formulate lessons learned. 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.”²⁴

24 OECD, [Evaluating Development Co-operation, Summary of Key Norms and Standards](#).

Evaluations enhance understanding of the contributions that various actions and actors make to a protection outcome. Once the causal logic for the activity or response has been established, evaluations can seek evidence for the contributions of actors and actions to the milestones and results achieved and then assess it. Of particular interest is the adoption of policies, practices and behaviour by duty bearers that contribute to their enhanced compliance with their obligations under international law and to an environment more conducive to protection.

Thorough programme documentation, detailing the contributions of multiple actors if applicable, can help guide future programme or strategy design, including the selection of appropriate analysis, planning and coordination methods. Evaluations are also essential for determining what long-term and sustained impact a programme has had. Internalizing lessons learned from programmes and investing in protection evaluations also encourages informed risk-taking and promotes a learning culture within a community of actors involved in protection work.

Evaluating protection strategies is particularly difficult because of the variety of issues they may address, the volatility of the factors affecting the risks 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 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, and 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 can be evaluated, i.e. the “evaluability” of an activity or response.

Evaluability is enhanced when the desired outcome and expected results of a programme are clear. This determines what to evaluate and where to look for sources of data to establish evidence or results – positive and negative, intended and unintended.

Evaluation shares many challenges with monitoring as regards 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 guide the overall approach and methods to be used. In particular, they should pay close attention to Chapter 7 on managing data and information for protection outcomes with regard to such topics as personal data, confidentiality, the collection of information from affected people and the importance of securing those people’s informed consent.

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

REFERENCE MATERIAL FOR CHAPTER 3

Results-Based Protection (InterAction): *A Problem-Solving Approach to Enhance Protection and Reduce the Risk People Experience in Complex Humanitarian Crises*

IASC, [IASC Policy on Protection in Humanitarian Action](#), 14 October 2016

GPC, [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

OECD, [Evaluating Development Co-operation, Summary of Key Norms and Standards](#)

Beck, T., [Evaluating Humanitarian Action using the OECD-DAC criteria: An ALNAP guide for humanitarian agencies](#), Annex 1, ALNAP, 2006, pp. 71–76

Christoplos, I. and Dillon, N., with Bonino, F., [Evaluation of Protection in Humanitarian Action](#), ALNAP, 2018



4. BUILDING ON THE LEGAL BASE OF PROTECTION

Knowing the legal framework

- S** 4.1 Protection actors must be familiar with the legal frameworks that apply.

Referring to the law with consistency

- S** 4.2 Protection actors must be consistent when referring to, reporting on or urging respect for the letter or spirit of the law applicable to the parties to an armed conflict or other violence.

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 applicable legal frameworks.

Referring to domestic laws and other standards

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

Upholding international 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.

INTRODUCTION

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

KNOWING THE LEGAL FRAMEWORK

S

4.1 Protection actors must be familiar with the legal frameworks that apply.

There are many international norms and standards (treaties, customary law and soft law) that require states and other actors to protect people during armed conflict and other violence.

These may apply to:

- certain groups of people, such as refugees, children, women, people with disabilities, detainees, IDPs, migrant workers or people belonging to national, ethnic, religious or linguistic minorities
- 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
- specific violations of international norms, such as the 1948 Convention on the Prevention and Punishment of the Crime of Genocide
- specific types of weapon, such as the Anti-Personnel Mine Ban Convention and the various Protocols to the 1980 Convention on Certain Conventional Weapons.

International criminal law also contains obligations and prohibitions applicable to individuals. Protection actors should be familiar with this branch of the law, even if they choose not to promote its implementation.

While many protection actors do not need to know the details of all types of law, they do all need to know which legal frameworks apply to them and to the context in which they are working. All protection staff planning or implementing protection activities must therefore understand the essence of IHL, IHRL and IRL (see box below) and how they complement each other.

This may require such staff to undergo training (see Chapter 9 on professional capacities) regarding 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 contained in the branches of law outlined in the box below.

Essential features of IHL, IHRL and IRL

Three bodies of law set out the international legal norms requiring respect and protection for people, in particular protection against violence and abuse:

- International humanitarian law (IHL), also known (especially in military circles) as the law of armed conflict (LoAC)
- International human rights law (IHRL)
- 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

Designed specifically for armed conflict. It aims to ensure respect and protection for people 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 and protects the activities of the ICRC and other impartial humanitarian organizations. While the humanitarian principles of humanity and impartiality are found in IHL, neutrality and independence are operating principles 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 people 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 people against threats emanating from armed groups, private individuals or natural hazards. The obligation to *fulfil* means that states must take measures to facilitate the enjoyment of basic human rights. IHRL is applicable in all circumstances, including armed conflict. However, there are 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 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 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.²⁵ Regional human rights treaties often reaffirm the obligations in international treaties or even impose additional obligations. Local actors may see them as particularly authoritative.²⁶

²⁵ International Covenant on Civil and Political Rights (ICCPR) (1966); Convention on the Rights of the Child (CRC) (1989); Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT) (1984); Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) (1979); International Covenant on Economic, Social and Cultural Rights (ICESCR) (1966); International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) (1965); International Convention for the Protection of All People from Enforced Disappearance (CPED) (2006); Convention on the Rights of People with Disabilities (CRPD) (2006).

²⁶ For more details, see [IASC Protection Policy](#), 2016, Annex I (“Normative framework”).

Customary international law – rules followed in state practice with the understanding that they represent a legal obligation, prohibition or authorization – applies 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. Where the requirements for the formation of customary international law are met, the norms contained in international treaties may also reflect customary international law. The norms contained in the Geneva Conventions of 1949 have attained the status of customary law. Most of the norms in the Universal Declaration of Human Rights and some of those in Protocols I and II of 8 June 1977 additional to the Geneva Conventions (the 1977 Additional Protocols), have also attained the status of customary international law.

These treaties and customary law are complemented by numerous internationally recognized standards (“soft law”), some of them adopted by policy-making bodies such as the UN General Assembly. These instruments are not formally binding but they may reflect rules of customary international law or constitute an authoritative interpretation of treaty obligations when they are backed by international consensus. Even where this is not the case, invoking international soft-law standards may help persuade authorities to assume their responsibilities and may provide a basis for action. Protection staff must know the international laws that apply in their operational context. This knowledge comes through comprehensive examination of the international and regional instruments (treaties, conventions, etc.) that the state has ratified. When a protection issue is covered by an international or regional instrument that the state has not ratified, customary law becomes all the more important. It is essential that protection staff know how to determine whether a rule has reached the status of customary law.

A major distinction between IHL and IHRL is that IHRL provides the individual with rights that the state (and possibly to some extent non-state actors) must protect, respect and fulfil, whereas IHL imposes obligations on all parties to an armed conflict, be they states or armed non-state actors.

In an armed conflict, both bodies of law are applicable and each influences the 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 rules on the conduct of hostilities, with their more permissive rules on the use of lethal force.

IRL

Regulates protection due to people who, owing to a well-founded fear of persecution, find themselves outside the territory of their country of nationality and do not enjoy its protection. IRL 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, their rights and the legal obligations of states. While the Convention’s definition of “refugee” is restricted to people suffering or at risk of persecution on grounds of race, religion, nationality, political opinion or affiliation to a social group, other regional instruments and elements of customary law enlarge the definition to people fleeing armed conflict or other violence.²⁷

²⁷ 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

S

4.2 Protection actors must be consistent when referring to, reporting on or urging respect for the letter or spirit of the law applicable to the parties to an armed conflict or other violence.

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

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. When referring to or applying IHL, protection actors must refrain from taking account of considerations related to the reasons for the conflict or to the political, moral or other reasoning with which the parties are justifying their use of force.

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 regarding their obligations, while recognizing that there might be practical differences when it comes to the implementation capabilities of the various parties.

It is important to recognize when other legal frameworks impose obligations on the state that differ from those imposed on organized armed non-state actors involved in conflict or other violence. For instance, IHRL primarily imposes obligations on state authorities. However, *de facto* authorities and non-state armed groups that exercise government-like functions and control over territory are increasingly expected to comply with international human rights norms and standards when their conduct affects the human rights of people under their control.²⁸

This standard requires protection actors to take a comprehensive approach to analysing the effects on the population of the actions – or lack of action – of the various perpetrators or parties to the conflict, taking account of all their obligations. This analysis might prompt a protection actor to focus 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 within 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 parties committing violations or abuses.

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 applicable legal frameworks.

If a protection actor intends to attempt to persuade authorities to assume their responsibilities, it should understand the applicable legal frameworks and know the norms it should be quoting. This does not mean that a protection actor must always expressly base its action on legal frameworks. What it does mean is that if a protection actor refers to the law and to the obligations of the authorities it must ensure that its references are correct and it must invoke the most relevant applicable legal framework. Certain issues – such as the rights of children, racial discrimination, the right to adequate housing, obligations pertaining to occupied

²⁸ IASC, [Policy on Protection in Humanitarian Action](#), 2016.

territory, conditions of detention in prisons and access to justice – require more detailed reference to 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 measures and any sanctions regimes 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 often use different wording to describe the same concerns, because their primary normative frames of reference are different. Consistency and accuracy both reinforce credibility and help avoid creating confusion or even contradictions when addressing the authorities. When making reference to international law, be it treaty or customary law, protection actors should also enhance accuracy and consistency by consulting other protection actors working on the same issue. This helps avoid the risk of confusion and contradiction; if several protection actors speak inconsistently or incorrectly about what they consider to be the laws and standards that apply, this can have a damaging effect. Coherence among the different protection actors will mutually reinforce their actions and give greater emphasis to the obligations that the authorities must assume. Conversely, incoherence will undermine this goal and is likely to be seized upon by the authorities to discredit the authors.

Protection actors addressing the authorities on similar patterns of violations or abuse should therefore consult each other. 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 regarding IHL, OHCHR regarding IHRL or UNHCR regarding IRL.

REFERRING TO DOMESTIC LAW AND OTHER STANDARDS

G

4.4 When domestic law or other 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 either increase or decrease the likelihood of abuse in a given society. When addressing local authorities and communities, protection actors may draw parallels between these laws, standards and traditions on the one hand and IHL and IHRL on the other. This can emphasize the universal relevance of international legal frameworks and norms. When domestic laws or other standards are not in full conformity with international law, protection staff should be aware of the discrepancies and should try to promote improvements.

In some countries, the official legal framework of reference may be pluralistic, meaning that other sources of jurisprudence, such as Islamic Law, are recognized as legally binding. Where a protection actor has an understanding of the parallels between other sources of jurisprudence and IHL or IHRL, it can be helpful for the protection actor to draw on these parallels in engaging with stakeholders.²⁹

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

²⁹ See, for instance, ICRC, [Islamic Law and International Humanitarian Law](#).

However, understanding the local legal system, its interaction with international law and its degree of implementation and enforcement is far from easy. Protection actors should draw on the expertise of legal advisers who are knowledgeable about the local legal system and understand the domestic laws, their interpretation and how the authorities apply them.

Other standards or sources of law may also exist and can be referred to, if they are consistent with the norms of international law or with accepted international standards.

These include frameworks of professional ethics (for health-care or legal professionals, journalists, academic researchers, etc.). Those frameworks may protect certain people 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 ensure the confidentiality of communications between patients and medical personnel and protect health records.

Public declarations or commitments by parties to a conflict, underscoring 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 enhance protection.

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 Commitment. Political manifestos, codes of conduct³⁰ and orders issued by senior leaders and commanders may also contain protection commitments.

Additional types of commitment made by states include individual or open pledges signed in the framework of International Red Cross and Red Crescent Conferences³¹ and regional plans of action adopted by regional organizations in such areas as the implementation of IHL.³²

However, national laws and other normative frameworks should only be invoked alongside international law if 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 should identify those domestic normative frameworks and their implementation that they can use 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.

³⁰ See, for instance, Geneva Call, [Directory of Armed Non-state Actor Humanitarian Commitments](#).

³¹ See, for instance, [Search pledges and reports – Statutory Meetings](#).

³² See, for instance, ECOWAS IHL Plan of Action ([Implementing IHL in West Africa: Redux](#)); ICRC, [Eighth Periodic Report on the Implementation of International Humanitarian Law at the Level of Arab states 2015–2018](#).

Traditional, social, religious and cultural norms

The behaviour of affected people 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 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 entitlement to community resources for people who are displaced from their homes or who have lost their heads of household. 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 harmful coping mechanisms such as forced marriage, or an 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. It is important for protection actors to understand what is the law and what is the practice, norm or tradition, since norms and traditions can at times be perceived as legally binding, when in reality this is not the case. 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.

UPHOLDING INTERNATIONAL 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.

In their actions and in their relationships with parties to an armed conflict or with actors involved in other violence, protection actors must avoid creating the impression that universal international law and standards can be lowered in accordance with domestic or local laws, standards and traditions. The norms and standards embodied in international law cannot be adapted or adjusted to the domestic context. Domestic law cannot be invoked as justification for a breach of an international legal rule.

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 affected population.

Such an approach to convincing the authorities may involve helping them acquire the technical, financial and other means to fulfil their international obligations. In addition, it may be necessary to engage in public education or to raise awareness among local constituencies to secure 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 set up 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 people 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 further – do not give rise to enforceable rights by themselves; to do that, they have to be incorporated in domestic law. Protection actors must convince the authorities of the relevance of these standards, to help them better fulfil their duties to the people affected.

Counter-terrorism measures, sanctions regimes and protection work

The recent proliferation and widening scope of counter-terrorism measures and the increased use of sanctions may have far-reaching protection implications. Such restrictive measures may be those of the country where a particular protection actor operates or those of the country where the protection actor's headquarters are located, or they may be imposed by multilateral/regional bodies.

Sanctions and counter-terrorism measures may affect civilian populations not only directly (e.g. by expanding a state's detention powers) but also indirectly where they reduce the capacity of human rights and humanitarian actors to provide protection and assistance in complex emergencies, particularly in areas under the control of armed groups and especially when these groups are designated as "terrorist groups". Restrictive national and international measures to block financial or other material support to proscribed groups – groups that have been designated as "terrorist groups" or against whom sanctions have been imposed by the UN Security Council, regional organizations or individual countries – can be particularly problematic, as they may apply to the activities of impartial humanitarian organizations.

IHL protects the provision of humanitarian services without distinction between victims of war. However, counter-terrorism laws may effectively criminalize medical assistance to injured fighters or the provision of humanitarian assistance to civilian populations; they may even consider IHL training to be "material support to terrorism" in areas where proscribed groups may be operating. Protection actors may also be prosecuted for providing legal assistance to "terrorist" suspects and helping 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 counter-terrorism measures. Engaging with a proscribed group may also carry significant reputational and financial risks for protection actors.

The financial sector is subject to regulations intended to combat the financing of “terrorist” activities; these can have unintended consequences for aid actors reliant on banking services. To mitigate the risk of breaching counter-terrorism regulations or sanctions, 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* – provide protection for human-rights defenders. Furthermore, IHL clearly entitles impartial humanitarian organizations to offer their services to all parties to a conflict. Prohibiting humanitarian actors from delivering humanitarian activities in areas where designated entities or people are active or in 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.

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” because of their alleged affiliation to certain groups, undermines the principles of humanity and impartiality (for more details on humanitarian principles, see Chapter 2).

Protection actors should be vigilant and insist that organizations and states do not take counter-terrorism and sanctions measures that infringe human rights or impede humanitarian work. Whenever a new measure is envisaged, they should engage with policymakers and legislators on its potential impact on protection actors and affected populations. Restrictive measures should be based on precise definitions of prohibited conduct and must contain exemptions for principled humanitarian and human rights work that requires engagement with non-state armed actors for the purposes of protection and humanitarian assistance. More broadly, sustained dialogue with donors, financial institutions, government entities and the public is essential to countering narratives 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 challenge counter-terrorism measures and sanctions regimes that may undermine principled humanitarian action.

REFERENCE MATERIAL FOR CHAPTER 4

Geneva Call, [Directory of Armed Non-state Actor Humanitarian Commitments](#)

GPC, [Minimum Standards for Child Protection in Humanitarian Action](#), 2012

IASC, [Policy on Protection in Humanitarian Action](#), 14 October 2016

ICRC, [International Humanitarian Law and the Challenges of Contemporary Armed Conflicts](#), October 2015

ICRC, International Rescue Committee, Save the Children, UNICEF, UNHCR and World Vision, [Interagency Guiding Principles on Unaccompanied and Separated Children](#), 2004

ICRC, [Islamic Law and International Humanitarian Law](#), 4 September 2018

Norwegian Refugee Council, [Risk Management Toolkit in Relation to Counter-Terrorism Measures](#), Geneva, 2015. See also revised version: [Toolkit for Principled Humanitarian Action: Managing Counter-Terrorism Risks](#)

OCHA, [Guiding Principles on Internal Displacement](#), 2004

UN, [Madrid International Plan of Action on Ageing](#), Report of the Second World Assembly on Ageing, New York, 8–12 April 2002

UN, [Standard Minimum Rules for the Treatment of Prisoners](#), UN Economic and Social Council, Resolution 663 C (XXIV) of 31 July 1957 and 2076 (LXII) of 13 May 1977

UNICEF, [The Paris Principles and Guidelines on Children Associated with Armed Forces or Armed Groups](#), Paris, 2007

Bartles-Smith, A., [Religion and International Humanitarian Law](#), *International Review of the Red Cross*, No. 920–921, November 2022

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



5. PROMOTING COMPLEMENTARITY

Complementarity of action among protection actors

- S** 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

- S** 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

- G** 5.3 Protection actors should share their analyses, to enhance understanding of protection issues and their impact on populations at risk.

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.

Providing information on protection services and facilitating referral to services

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

Responding to harm and violations

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

INTRODUCTION

This chapter is concerned with managing interaction among the increasingly numerous and diverse humanitarian and human rights actors that undertake protection work during armed conflict and other 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. The chapter also touches upon complementarity between humanitarian, human rights and other actors in the development and peace sectors.

Enhanced synergies between the protection activities of various actors can help optimize the benefits for populations at risk. Such synergies reduce gaps, potential overlaps and duplication and help prevent the activities of one actor disrupting or undermining those of another. For example, the publicity generated by the advocacy efforts of human rights actors can enhance the impact of quiet persuasion and community organizing undertaken by humanitarian actors regarding the same issues.

However, enhancing synergies should never jeopardize the character of any of the protection actors involved. They must respect and maintain their distinctive characteristics, to preserve their identities and principles and to avoid blurring the individual responsibilities of protection actors for the safety of the populations and for the use they make of the information collected. As far as possible, protection strategies to reduce risk should incorporate the contributions of multiple actors to the desired protection outcome (see Chapter 3).

Given the diversity of protection actors, methods and approaches should be used in complementarity to achieve optimal protection outcomes. Humanitarian, development and peace actors may all be present in a context. Humanitarian actors should therefore identify the appropriate form of complementary action with other types of actor, and this will depend on their mandates and principles.

Complementary action can take several forms.

Forms of complementary action³³

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

Cooperation or collaboration

Joint work to achieve a common aim, involving multiple actors, may include joint analysis and action. This does not necessarily involve 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.

³³ Adapted from the IASC reference paper [Civil-Military Relationship in Complex Emergencies](#), Geneva, 2004.

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”³⁴ – they also have different identities, mandates, priorities, approaches and activities that necessitate dialogue and coordination. As described in Chapter 2, especially in difficult negotiation environments, establishing common bottom lines or joint key messages on certain issues can be crucial to upholding humanitarian principles collectively and to creating a more conducive environment for protection dialogue involving different humanitarian and human rights actors.

Organizations that subscribe to the principles of neutrality or independence as a means to gain access to all communities and actors during armed conflict and other 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 people following a crisis that has 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 may vary. These factors influence every protection actor’s willingness, interest and ability to coordinate with others. Disparities in capacity or resources or even the distance between locations can present additional obstacles to complementary action. In the case of local or national actors, scarcity of funding and therefore limited availability to participate in time-consuming coordination meetings can also present a significant obstacle.

Often, however, such differences are 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 be better placed to obtain results. They may also experience fewer access constraints and are often rooted in the communities they serve, which can give them a more granular knowledge and understanding of the context. International actors may be more effective in other circumstances, especially for activities that benefit from a perception that the protection actor is external to the context and free of linkages, or where a greater risk is involved, potentially necessitating the evacuation of staff.

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 closely. For instance, a confidential dialogue to persuade primary duty bearers to fulfil their protection responsibilities can sometimes be reinforced 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. Conversely, failure to coordinate the sequencing of activities can have a counterproductive effect.

Thematic collaboration among selected actors is frequent, such as inter-agency cooperation on disarmament, demobilization and reintegration or on 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 those on gender-based violence or child protection.

³⁴ See the IASC-endorsed definition of “protection” in the introduction to this document, p. 12.

The actual form of complementarity to adopt will depend on an assessment by the protection actor of the most effective response to a given context or protection issue, and on 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, to preserve its confidential dialogue with weapon bearers and authorities.

COMPLEMENTARITY OF ACTION AMONG PROTECTION ACTORS

S

- 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.³⁵

As outlined in Chapter 6 (on the protection architecture), all actors involved in protection activities, including human rights, peace and development actors, must explain their roles so that others can understand their intentions and their work. Liaison with others working in the same geographical areas or on the same issues will help ensure that protection risks 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 achieved through existing multilateral coordination mechanisms (e.g. the in-country protection cluster) or through bilateral contacts.

As noted in Chapter 6 (Standard 6.2), a protection actor must also ensure that its actions do not undermine the capacity of the authorities to fulfil their protection obligations, while nonetheless acting in accordance with its mandate or mission statement.

Being able to deliver on commitments 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 open and honest regarding their roles/activities and their estimated duration (see Chapter 9). 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

S

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

While humanity, impartiality and non-discrimination are central to all protection work, some protection actors also have the principles of neutrality and/or independence as core values that enable them to gain access and proximity to people at risk during armed conflict and other violence. Adherence to these principles is a working method that enables these organizations to undertake protection activities with all parties to a given conflict and with all sections of the affected population.

³⁵ See also Standard 8.10 in Chapter 8, on how protection actors can work in complementarity to address digital risks.

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

COMPLEMENTARITY OF ANALYSES

G

5.3 Protection actors should share their analyses, to enhance understanding of protection issues and their impact on 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 predict future risks (see Chapter 3).

The diversity of humanitarian and human rights actors doing protection work enhances this understanding and contributes to more comprehensive responses. Different actors focus on many different matters such as: specific geographical areas; issues such as gender-based violence, tracing, judicial reform, prison conditions, the role of security forces in emergencies and sub-groups within the affected population. The resulting diversity of perspectives and approaches enriches analysis. Sharing this diversity enhances overall understanding of a given context. Communities must also be involved in analysing protection risks.

Contextual analysis should examine the environment, pattern of violations and abuses, perpetrators, duty bearers and their capacity and willingness to protect, and the impact on affected people. It should also cover age, gender and other diversity factors that might increase people's exposure to threats. This information should be shared with appropriate amounts of detail, while respecting the principles of informed consent and confidentiality.³⁶ 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 common 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. Particularly when common purposes and approaches exist, inter-agency analysis and assessment should be given priority, to reduce duplication and to contribute to coherent messaging and advocacy. Additionally, the number of assessments must be kept to a minimum, given the potential impact on affected people's well-being. Drawing upon existing analyses and assessments is often useful, provided they are relevant and of good quality.

³⁶ See Chapter 7 for further guidance on sharing and transferring protection data and information.

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 (see Chapter 3). But in situations where the authorities are failing, humanitarian and human rights actors may have 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 both in terms of contributing to the development of legislative norms or policy and as regards operational responses. Encouraging action by others does not imply directing their response, but rather sharing information and analyses regarding important, unaddressed protection risks.

PROVIDING INFORMATION ON PROTECTION SERVICES AND FACILITATING REFERRAL TO SERVICES

G

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

Protection actors can help people make informed decisions about how to best meet their essential needs, by providing accurate information on critical services including health care, psychological support, secure shelter, livelihood, tracing missing family members, obtaining ID documents and legal support. These services may be provided by state authorities, civil society actors, community-based organizations and national and international humanitarian/human rights organizations.

ENSURING A SURVIVOR/VICTIM-CENTRED APPROACH WHEN ESTABLISHING A REFERRAL PATHWAY

The survivor-centred approach is guided by the principles of safety, confidentiality, non-discrimination and respect. It allows for agency, i.e. for survivors to choose and determine their needs and next steps. This can be accomplished by developing a holistic protection referral system or pathway, which summarizes all the essential services in an area (health care, psychosocial support, safe houses, legal aid, financial aid or access to livelihood and other services) in a list or flowchart.

Protection actors must:

- map the services
- provide such details as access times and costs
- assess the quality of the services against the survivor-centred principles and other quality measures in conformity with professional standards.

This can be accomplished through coordination with other clusters or sectors to obtain information about services and their quality.

If possible, direct visits to services should be carried out to verify that they can take on new cases and to establish referral procedures in advance. If a service is unsafe or abuses a community member it should be suspended from the pathway and the pathway should be updated.

Once completed, the list/flowchart should give information on where people can obtain each service and how, when and at what cost. It is important to ensure this information is accessible not only to humanitarian/human rights actors but also to the community. For example, if literacy levels are low, it may be essential to provide oral and visual information rather than written materials. Additional efforts should also be undertaken to ensure the same information is accessible to people with visual, auditory and other disabilities.

FACILITATING FACE-TO-FACE REFERRALS

In many humanitarian contexts, people face extensive physical, economic, administrative and/or security barriers that prevent them from safely accessing these services. Where this is the case, it will be necessary to facilitate referrals. The informed consent of the person being referred must always be obtained before initiating this process (see Chapter 6). Where this is not possible, owing to the age or legal incapacity of the person(s), consent to refer can be obtained from a parent/legal guardian. If that option is not available, protection actors must decide to refer based on the best interests of the person. A well-coordinated referral system should reduce the need for a person to disclose their history on multiple occasions, reduce the time and cost associated with getting service and overall prevent further harm.

In some cases, facilitating a referral may go beyond connecting the person to the service, requiring the protection actor to take additional steps to ensure the person can physically access the necessary services. This can include negotiating with authorities or other actors controlling the area to ensure fair and secure access, urging specialist service providers to increase their coverage or capacity or supporting them by facilitating visits by a mobile outreach team. In particularly urgent or vulnerable cases, facilitation might entail calling emergency services, transporting the person(s) in question and/or providing the financial means to access services. Whenever possible, a trusted person should accompany the person being referred. It is good practice to also cover the costs for that person, in full or in part.

The person referred must be informed of the limitations of the assistance the protection actor can provide and of the rules and regulations of the services to which they are being referred, particularly if referral could result in any unintended consequences or additional risks. For instance, they need to know the extent to which they will have to provide more detailed personal information and whether this information will be kept strictly confidential or if the service provider is required by law to pass it on to other authorities, etc. Adequate follow-up should also be undertaken with the individual and/or the service provider as necessary, according to the actor's competencies and capacities.

FACILITATING DIGITAL REFERRALS

Whenever protection actors establish digital platforms that can be accessed by people affected by crisis (e.g. websites for searching for missing family members, portals where information can be shared on unfolding protection concerns or events, etc.), these platforms should include information on safe services. Protection actors should use specialist service providers to ensure that their internet platforms are of good quality, accessible and user-friendly. They should comply with data protection standards, including the confidentiality requirements discussed in Chapter 6. When third parties set up such platforms, protection actors should ask them whether they would be willing to disseminate information on protection services.

RESPONDING TO HARM AND VIOLATIONS

G

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

Protection actors should take 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. When these violations are serious, protection actors have a duty to take action.

The type of action will depend on the circumstances and on 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.³⁷ 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 humanitarian and human rights actors typically engage the authorities directly and urge them to fulfil their obligations under IHL and IHRL – 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 (see also Chapter 3). If violations or abuses have occurred, action can be taken to prevent any recurrence, to reduce the consequences for affected populations and to ensure accountability. If violations 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 affected people, respecting the informed consent provided by sources of information and protecting the security of staff (see also Chapters 7 and 9). Some protection actors may not be able to provide detailed information for reasons of confidentiality.

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

³⁷ IASC, [Terms of Reference for the Humanitarian Coordinator](#), 2009.

REFERENCE MATERIAL FOR CHAPTER 5

IASC, [Civil-Military Relationship in Complex Emergencies](#), 2004

IASC, [Civil-Military Guidelines and Reference for Complex Emergencies](#), 2008

IASC, [Terms of Reference for the Humanitarian Coordinator](#), 2009

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

Giossi Caverzasio, Silvie (ed.), [Strengthening Protection in War: A Search for Professional Standards: Summary of Discussions among Human Rights and Humanitarian Organizations, Workshops at the ICRC, 1996–2000](#), ICRC, Geneva, 2001

Graves, Sue, Wheeler, Victoria, and Martin, Ellen, [Lost in Translation: Managing Coordination and Leadership Reform in the Humanitarian System](#), HPG Policy Brief 27, ODI, London, 2007



N. Markogiannis/UN Peacekeeping

6. THE PROTECTION ARCHITECTURE

Relating to the primary duty bearers

- S** 6.1 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** 6.2 Protection actors must avoid undermining the willingness and ability of primary duty bearers to fulfil their obligations.
- S** 6.3 Protection actors must not substitute for the role of the authorities when they are willing and able to assume their responsibilities.
- G** 6.4 Protection actors, UN peace operations and internationally mandated military forces and police deployments should support duty bearers in their prevention and preparedness efforts with advisory services, technical support and, where relevant, advocacy and mobilization of partners.
- G** 6.5 Protection actors should include communication with the authorities in their overall approach.
- G** 6.6 Protection actors should ensure that, whenever feasible, they establish a protection dialogue with armed non-state actors.
- S** 6.7 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** 6.8 Protection actors must understand the roles 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** 6.9 Protection actors should engage UN peace operations with a view to promoting positive protection outcomes for populations at risk.
- G** 6.10 Protection actors should interact 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, and to ensure more informed protection efforts.
- S** 6.11 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.

Communities, civil society and other actors

- S** 6.12 Protection actors must take into account the various protection roles of political, judicial and economic actors.
- G** 6.13 Protection actors should support civil society and other local actors' efforts to take preventive action to reinforce capacities, reduce risks and vulnerabilities or mitigate the impact of protection risks on affected people.
- S** 6.14 Protection actors must support communities' own protection dialogues with duty bearers and others and, where relevant and appropriate, ensure that their own interactions with those stakeholders support those of communities.

INTRODUCTION

This chapter outlines the “global protection architecture” and how humanitarian and human rights actors doing protection work should relate to it and each other.

This global protection architecture, comprising various actors at local, national and international level with protection roles and responsibilities, is based on rights and obligations set out in IHL, IHRL and IRL. These rights and obligations must be incorporated in domestic legislation, which frequently expands and enhances the rights agreed upon internationally and lays down responsibilities for enforcing them.

While the state bears primary responsibility for protecting 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 people under their control.³⁸

All parties to armed conflicts, including organized non-state armed groups that conduct military operations, are also bound by IHL, which imposes protection responsibilities on them for affected civilians and other people 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 protecting the population. If the capacity or will of authorities to protect people under their jurisdiction is limited – or worse still, when authorities themselves are perpetrating violations against the population – such protection mechanisms are likely to be ineffective or inadequate. A response by other actors is then required to protect those at greatest risk. As members of the United Nations and as parties to the Geneva Conventions, states bear protection duties towards people at risk, even if these people are outside their jurisdiction. A protection response can hence also be led by other states or multilateral bodies. 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.

States have conferred specific protection mandates on a number of international humanitarian and human rights organizations, including the International Committee of the Red Cross, the Office of the High Commissioner for Human Rights, the Office of the United Nations High Commissioner for Refugees and the United Nations Children’s Fund. 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 peace-keeping operations with protection of civilians mandates. Within the protection architecture, all these actors bear certain protection responsibilities.

State actors, of course, remain the primary duty bearers. However, reducing protection risks should be central to all humanitarian actors, extending beyond mandated organizations. Non-mandated organizations also play an important role in specialized protection work. It is therefore essential for humanitarian and human rights actors engaged in protection work to be familiar with the global protection architecture and to position themselves within this framework to ensure that their collaborative action is more effectively coordinated and has greater impact.

For the work of these actors to achieve the expected protection outcomes, affected communities must play a key role in identifying risks, vulnerabilities and coping mechanisms, and in defining the desired protection outcomes. When safely feasible, communities must play a central role in implementing preventive and/or preparedness measures to reduce the protection risks they face.

³⁸ IASC, [Policy on Protection in Humanitarian Action](#), 14 October 2016. See also Chapter 4 of this document.

The first section of this chapter emphasizes that the protection work of humanitarian and human rights actors must be positioned within the existing protection architecture and improve the way it functions – as opposed to replacing it – especially at local and national levels. It also emphasizes the importance of prevention and preparedness actions, carried out by duty bearers or at community level and supported by humanitarian and human rights actors where appropriate and possible.

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 the undermining of other actors' efforts 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.³⁹ The standards and guidelines capture some commonalities between the very diverse views protection actors can have on how to engage with military and police forces of which the mandate may include the protection of civilians. It also underlines the role that UN peacekeeping operations and other internationally mandated military and police forces can play in supporting duty bearers in their prevention and preparedness efforts.

RELATING TO THE PRIMARY DUTY BEARERS



6.1 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 each actor involved in protection work is responsible for its own actions, it does not work 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 people on their territory or under their jurisdiction.

Authorities include military, police and other state security forces, together with judicial institutions and ministries with specific responsibilities, such as 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 avoid or minimize harm to civilians and ensure that civilians have access to goods and services essential to their survival.

No effort should be spared to remind duty bearers of their responsibilities and urge them to fulfil their obligations entirely. 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 are raising awareness of duty bearers' obligations through persuasion, mobilization and denunciation; and substitution, where duty bearers are unable or unwilling to fulfil their obligations. These modes of action may be preferred with duty bearers who, by their acts of commission or of omission, i.e. by their action or inaction, are responsible for the violation of rights.

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

Persuasion efforts by humanitarian and human rights actors aim to convince stakeholders to take actions that fall within their areas of responsibility or competence, often through bilateral confidential dialogue.

Mobilization in this context involves protection actors mobilizing influential third parties (such as states, regional organizations, private companies, members of civil society or religious groups that have a good relationship with the authorities in question) in support of their protection dialogue with duty bearers.

Denunciation means publicly reproaching duty bearers for their failure to comply with legal frameworks and focuses on the imminent or established violation of a rule designed to protect people.

Different protection actors may adopt different approaches, depending on the issues to be addressed, their unique capacities and mandates and what they are capable of doing. Protection actors should therefore strive for complementarity in their collective efforts to improve protection outcomes.

S

6.2 Protection actors must avoid undermining the willingness and ability 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 violence must aim to encourage, assist and persuade the authorities to assume their obligations more fully. Protection outcomes may often involve supporting the establishment of national protection systems and/or strengthening existing systems.

Whatever their approach, protection actors must 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 champion well-functioning national protection agencies, such as ombudsmen and other national human rights institutions.

S

6.3 Protection actors must not substitute for the role of the authorities when they are willing and able 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 reduce the incentive for 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. Humanitarian actors should establish a clear timeframe for their actions.

Similarly, independent human rights monitoring and other protection work by human rights actors can support the efforts of a state but does not relieve that state of its responsibility to fulfil its obligations vis-à-vis populations affected, including obligations related to protection and accountability.

Activities based on direct substitution traditionally focus more on the populations at risk. They can include measures to reduce those populations' 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 of the formal system and continuing only until the authorities become willing and able to resume their roles.

Ideally, substitution activities should be accompanied by efforts to build or strengthen the capacity of the authorities and of 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 to fulfil their obligations but lack the capacity to do so. Total substitution should occur only in extreme circumstances. Even then, protection actors should constantly deploy persuasion and advocacy to encourage the authorities to better fulfil their obligations and responsibilities to protect people at risk.

G

6.4 Protection actors, UN peace operations and internationally mandated military forces and police deployments should support duty bearers in their prevention and preparedness efforts with advisory services, technical support and, where relevant, advocacy and mobilization of partners.

Preventing rights violations requires a conducive environment. Building this environment is the responsibility of primary duty bearers, and protection actors should support their efforts. Having robust systems in place to reduce protection risks takes time, effort and expertise. Where authorities are willing to implement international standards but dispose of limited means and capacity, protection actors can provide valuable support and must at the same time ensure coordination and complementarity with development actors (see Chapter 5 on complementarity).

This approach can reduce protection risks or their impact on affected people through the preventive application of mitigation measures. Engagement on legal frameworks prior to an outbreak of violence or conflict may also create more conducive conditions for commencing a protection dialogue later.

G

6.5 Protection actors should include communication with the authorities in their overall approach.

Protection actors should communicate (directly or indirectly) with authorities and duty bearers, with the aim of encouraging them to respect, protect and fulfil the rights of all.

Direct communication usually takes the form of evidence-based analysis and recommendations that mandated and other protection actors communicate to the authorities bilaterally or make public, calling for improved respect for, or changes to, behaviour, laws and policies. The aim is to obtain a direct response from the authorities. Humanitarian actors should consider relaying the authorities' response to the communities concerned.

Indirect communication can take many forms. It may for instance be conducted through leaflets presenting key messages about the activities of an organization in a given country. Relaying messages to duty bearers through local leaders is another indirect channel of communication.

Communication should focus on the need to improve the protection of people at risk and the responsibility of the primary duty bearer to provide this protection. When communicating with authorities, it is essential to be open and honest regarding the activities, mandate and/or mission statement of one's organization.

Maintaining dialogue with the authorities is even more essential when working in substitution for the formal authorities. The content of the dialogue will depend on the causes of the protection shortfalls on the part of the primary duty bearers, such as 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 is unlikely to create conditions conducive to the sustainability of an actor's presence and may pose additional risks for affected communities.

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, which it 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 their will, for individuals or communities that would be at greater risk if the authorities were to learn of this action.

At the community level, formal and informal or traditional leaders have varying levels of influence. Conflict and violence also affect community dynamics and may disrupt traditional hierarchies in practice even where the roles continue to exist. It is important to try to understand the social power dynamics at the community level to navigate communication with local leadership in a way that is conducive to protection outcomes. Similarly, engagement with local leadership should be accompanied by an analysis of the relationship between formal and informal authorities and non-state armed groups where applicable. Engagement with local leaders is essential and must be carefully managed.

G

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

To secure access to all areas, improve the security of operations and achieve protection outcomes for the population, it is often essential for protection actors to establish a dialogue in the field with all key stakeholders. These include armed non-state actors, such as militias, rebel or guerrilla movements and private security companies. If party to an armed conflict, they all have obligations under IHL and engaging with them does not affect the legal status of parties to the conflict. The actions and modus operandi of the actor 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 against the civilian population, and their consequences in humanitarian terms. Protection actors must also understand the motivations and incentives of armed non-state actors, their organization, their command structure and their strategies, in order to influence their behaviour. This can be particularly difficult in the case of actors that pursue both political and criminal objectives or groups that are primarily motivated by religious norms. The decision on who to engage with strategically, how to do so and who should undertake such engagement should be based on a solid understanding and analysis of the context dynamics, the role of local communities impacted by the conflict and the relevance/importance of the various armed non-state actors. To influence behaviour, an exclusive focus on the law is not as effective as a combination of the law and the values underpinning it.⁴⁰

Protection actors who engage in dialogue with armed non-state actors should remind these actors of their obligations and responsibilities. The measures they could take to reduce the impact of conflict and other violence on the civilian population should be presented to them and discussed. Confidence-building measures will be necessary to establish the conditions for such a dialogue. When dealing with certain actors operating transnationally, protection actors should ensure that their engagement is consistent between geographical regions.

⁴⁰ ICRC, [The Roots of Restraint in War](#), 2018.

Not all protection actors will choose to engage in such a dialogue; some may prefer to voice their concerns through public communication, through humanitarian organizations or through others who have the necessary contacts. Engaging in any form of dialogue with armed non-state actors can be difficult because of security considerations for their representatives and for the protection actors' personnel in the field, and because of implications for the organization's relationship with the state in which the armed non-state actor operates. Both domestic and international counter-terrorism measures, including sanctions, may pose additional challenges, as they seek to prevent engagement with listed groups. Furthermore, any such interaction must be conducted in a manner that does not put affected populations at greater risk and does not undermine the ability of humanitarian and human rights actors to operate and to be seen to operate, in accordance with the principles that underpin their work.

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 where remote management is being used) organizations must ensure that they provide adequate security, legal, financial and managerial support. This is particularly important when national staff are not protected by an organization's privileges/immunities and contact with the armed non-state actor is criminalised under national law. Organizations must also carefully evaluate the potential risk transfer and take protective and mitigation measures when relying on community leaders who engage with non-state actors on their behalf. Organizations working with local implementing partners must also evaluate risks jointly with the partner and provide support and financing to allow for risk mitigation and for sharing of the residual risks.

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



6.7 Protection actors must specify their roles, protection objectives, institutional priorities and means of action.

Cooperation between 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 clarity greatly facilitates interaction and complementarity and clarifies their relationship with the existing international protection architecture.

A mission statement expresses the mandate and objectives of a protection actor with a formal mandate in a coherent manner. It can outline the protection elements on which the actor is authorized and expected to act, and clarify any additional issues to which the actor intends to respond.

For actors that 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, communicating them to other protection actors, authorities, communities and other stakeholders. Institutional clarity on general objectives and the type of activities to be carried out is also necessary for effective communication with people at risk – for example, to enable them 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 operations⁴¹

UN peacekeeping operations 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).⁴²

Beyond these general obligations the 2000 *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”.⁴³

Furthermore, in 2015, the High-Level Independent Panel on Peace Operations⁴⁴ 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”.⁴⁵ 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”.⁴⁶

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”⁴⁷ and his Call to Action for Human Rights noted that “within the United Nations, human rights must be fully considered in all decision-making, operations and institutional commitments”. As part of the Call to Action, the UN’s Agenda for Protection outlines a common UN approach to strengthening protection through human rights.⁴⁸

⁴¹ The term “UN peace operations” encompasses both peacekeeping operations and special political missions. Peacekeeping operations are managed by the UN Department of Peace Operations (DPO). They include “traditional peacekeeping”, which is essentially military in character and aimed at preserving the peace where fighting has been halted, as well as multidimensional peacekeeping operations (i.e. also comprising police and substantive civilian personnel) that also engage in “peace building” to reduce the risk of lapsing or relapsing into conflict. Peacekeeping operations may exceptionally include “peace enforcement” with coercive measures when specifically authorized by the Security Council. (see: UNDPKO/DFS, [United Nations Peacekeeping Operations, Principles and Guidelines](#), 2008). Special Political Missions (SPMs) are managed by the Department of Political and Peacebuilding Affairs and engage in conflict prevention, peacemaking and post-conflict peacebuilding. These include a range of configurations, which may work on specific countries, regions or issues. They are civilian in nature. (see: <https://dppa.un.org/en/dppa-around-world>).

⁴² When deployed in situations of armed conflict, UN peacekeeping 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 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) when they are engaged as combatants. See Secretary-General’s *Bulletin on Observance by United Nations Forces of International Humanitarian Law*, ST/SGB/1999/13.

⁴³ UN, *Report of the Panel on United Nations Peace Operations (the Brahimi Report)*, [A/55/305–S/2000/809], 21 August 2000. The term “peace operations” used in this report referred to peacekeeping missions only and not special political missions, in line with the practice that existed at that time.

⁴⁴ 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.

⁴⁵ *Ibid.* p. 22.

⁴⁶ *Ibid.* p. 26.

⁴⁷ 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.

⁴⁸ UN, *The Highest Aspiration: A Call to Action for Human Rights*, 2020, p. 3.

The Security Council has explicitly mandated all multidimensional UN peacekeeping missions to protect civilians under threat of physical violence from state or non-state actors and has mandated most UN peace operations to promote and protect human rights. Security Council resolutions usually underline that UN peacekeeping missions engaged in hostilities have obligations under IHL and specifically call upon these missions to mitigate risk to civilians in the conduct of military and police operations.

A “protection of civilians” (PoC) mandate is generally phrased as follows:

The UN Security Council,

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

⁴⁹*(...) 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 mandates of individual missions may vary in language and include specific tasks and approaches to PoC that will guide implementation of the mandate and the strategic approach it takes.⁵⁰ The mandate may also include a focus on particular themes (e.g. protection of medical care) or on vulnerable categories of population.

In 2023, six UN peacekeeping missions, accounting for more than 95% 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.⁵¹

While UN special political missions do not have these PoC mandates (i.e. mandates to protect civilians against the threat of physical violence), given their lack of military forces, the Secretary-General has stated that all UN peace operations have an obligation to advocate for the protection of civilians. However, country-based special political missions may be mandated to support the protection of civilians in other ways, such as monitoring and reporting on the situation of civilians or supporting government efforts to protect them.⁵² The Security Council has also increasingly recognized unarmed approaches to protection within UN peace operations. 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.

⁴⁹ A Chapter VII mandate need not have a protection of civilians mandate, see e.g. UNIFIL.

⁵⁰ UNDPO, [Policy: The Protection of Civilians in United Nations Peacekeeping](#), 2023, p.5, para. 12.

⁵¹ Such as Security Council Resolution 2573 [on the protection of civilian infrastructure], 27 April 2021, S/RES/2573; Security Council Resolution 2475 [on the protection of people with disabilities], 20 June 2019, S/RES/2475; Security Council Resolution 2474 [on missing persons], 11 June 2019, S/RES/2474; Security Council Resolution 2417 [on conflict and hunger], 24 May 2018, S/RES/2417; Security Council Resolution 2286 [on the protection of health care], 3 May 2016, S/RES/2286; and Security Council Resolution 2222 [on the protection of journalists], 27 May 2015, S/RES/2222. 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, *Building a Culture of Protection: 20 Years of Security Council Engagement on the Protection of Civilians*, OCHA, 2019.

⁵² For example, some country-based UN Special Political Missions, such as UNAMA (Afghanistan), have been mandated to coordinate efforts to protect civilians and to monitor, report and advocate with regard to the situation for civilians. See Security Council Resolution 2210, 16 March 2015, S/RES/2210 and Security Council Resolution 2266, 17 March 2022, S/RES/2626. UNITAMS (Sudan) was mandated to support national and local authorities on civilian protection in conflict-affected areas and support the Sudanese government in implementing the National Plan for Civilian Protection. See Security Council Resolution 2579, 3 June 2021, S/RES/2579.

Several UN peace operations have mandates and tools that are relevant to protection. For example, a number of such 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 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. Reporting has included civilian casualty recording that has supported advocacy and engagement to protect civilians.⁵³

UN policy reaffirms that all mission personnel have a responsibility to ensure that human rights are promoted, respected and protected through and within their operations.⁵⁴

UN peace operations and humanitarian organizations may undertake complementary protection activities, such as protecting children and preventing and responding to conflict-related sexual violence. UN peace operations sometimes lead implementation of the Security Council-mandated Monitoring, Analysis and Reporting Arrangements (MARA) on conflict-related sexual violence and of the Monitoring and Reporting Mechanism on grave violations of children's rights in armed conflict.

Finally, the UN Human Rights Due Diligence Policy stipulates that the UN will not support national security forces when there are substantial grounds for believing that there is a risk of such forces committing grave violations of IHL, IHRL or IRL and where the authorities fail to take the necessary corrective or mitigatory measures.⁵⁵

UN peacekeeping and the implementation of PoC mandates

The UN Department of Peace Operations defines the protection of civilians mandate in UN peacekeeping as “without prejudice to the primary responsibility of the host state, integrated and coordinated activities by all civilian and uniformed mission components to prevent, deter or respond to threats of physical violence against civilians within the mission’s capabilities and areas of deployment through the use of all necessary means, up to and including deadly force”.⁵⁶

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: Establishing a protective environment

⁵³ The longest-standing UN casualty recording system was established by the United Nations Assistance Mission in Afghanistan (UNAMA) human rights service in 2007. Since then, casualty recording systems have been operated by OHCHR in Iraq, Libya, Somalia, Palestine, Ukraine and Yemen. See: OHCHR, *Guidance on Casualty Recording*, New York and Geneva, 2019.

⁵⁴ See for example the UN policies on: Human Rights in United Nations Peace Operations and Political Missions, OHCHR/DPKO/DFS/DPA, 2011; Policy on Child Protection in United Nations Peace Operations, DPKO/DFS/DPA, 2017; and Policy on Preventing and Responding to Conflict-Related Sexual Violence, UNDPO/DPPA/OHCHR/OSRSG-SVC, 2019.

⁵⁵ UN, Human Rights Due Diligence Policy on UN Support to non-UN Security Forces [A/67/775-S/2013/110], 5 March 2013.

⁵⁶ UNDPO, *Protection of Civilians in United Nations Peacekeeping*, 2023, p.5, para. 13. See also: UNDPO, *The Protection of Civilians in United Nations Peacekeeping Handbook*, 2020.

Implementing such mandates can 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)
- longer-term, more structural efforts, such as training, mentoring or supporting national military and security staff (tier 3).

The contribution of other mandated tasks in areas such as security sector reform or child protection may also fall into these tiers.

Missions are required to design a “mission-wide protection strategy”, generally structured on these three tiers, and to report on its implementation.

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 a presence in areas where populations are most at risk, as a preventive and early-warning strategy
- 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 for UN peace operations but also for other internationally mandated military forces and police services.⁵⁷

Over the past decade, UN Security Council mandates provided to some international forces operating outside the UN system have encouraged the protection of civilians through adherence to IHL and other legal obligations and sometimes even included an explicit mandate to protect against physical threats. Meanwhile, the stabilization approaches of individual states and a few multilateral organizations have evolved into a policy framework for some international military interventions in fragile and conflict-affected states. A number of regional organizations and states have clarified their PoC ambitions by adopting PoC policies or guidelines.

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



6.8 Protection actors must understand the roles 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 the physical protection of civilians by projecting or using force, to activities such as the monitoring, reporting and advocacy undertaken by all peace operations (i.e. both peacekeeping and political), which may overlap with the activities of other protection actors.

⁵⁷ 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.

The UN Department of Peace Operations and troop- and police-contributing countries have clarified the potential roles and responsibilities of the components of a peacekeeping mission regarding the protection of civilians against the threat of violence, i.e. the specific responsibilities of:

- the civilian leadership of the mission
- the military command of the force
- countries contributing police and/or military personnel.

Missions with explicit PoC mandates are now required to establish protection strategies, which should be developed in consultation with the populations at risk and 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, coordination mechanisms, documents and policies of UN peace operations and internationally mandated military forces and police services regarding PoC.

They need to be familiar with the above at two levels:

- General/policy level:
 - UN Human Rights Due Diligence Policy
 - UN Secretary-General’s bulletin on sexual exploitation and abuse⁵⁸
 - DPO PoC Policy
 - UN policies on human rights, child protection and conflict-related sexual violence.
- Country level:
 - structure of the mission
 - substantive civilian staff and roles
 - PoC or other strategies
 - for peacekeeping missions, rules of engagement and role of troop-contributing countries.

The depth of understanding required may vary, depending on the types of issue 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.

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

Many humanitarian and human rights actors have long expressed concern about the impact that 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 belligerents or segments of the population perceive them as being aligned with the political objectives of such missions. This becomes especially acute where UN peacekeepers and forces are conducting peace enforcement or engaging 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 difficult for humanitarian organizations that rely on their neutrality to gain access to the population and to all armed actors.

⁵⁸ UN, [Special Measures for Protection from Sexual Exploitation and Sexual Abuse](#), Secretary-General’s Bulletin, [ST/SGB/2003/13], UNSG, 9 October 2003.

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 help create a security environment conducive to civilian-led provision of humanitarian assistance. UN peace operations, supported by their human rights components, can support protection through their engagement with the authorities.

While many humanitarian and human rights organizations on the ground may value UN peace operations' contributions, 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 affected populations.

Dialogue and interaction between humanitarian organizations and UN peace operations are therefore essential in order to strengthen the roles and activities of each, enhance the overall protection response and prevent the blurring of their roles and responsibilities in the eyes of local authorities, communities and others.

The UN's Policy on Integrated Assessment and Planning of February 2023 recognizes the need for humanitarian action to remain distinct and separate from the political objectives of UN missions, while maintaining dialogue and engagement.

Integration arrangements should support joint analysis, coordination, complementarity and coherence among humanitarian, peace and security, development and human rights actors. While humanitarian action can help to sustain peace, its main purpose is to save life and alleviate suffering. Accordingly, most humanitarian action is likely to remain distinct from other United Nations activities so as not to challenge the ability of UN and other humanitarian actors to deliver according to humanitarian principles. However, the UN's integrated strategic approach may include humanitarian activities related to PoC, durable solutions to internal displacement and early recovery, on the basis of a joint analysis of context, risks, costs and benefits.⁵⁹

The integrated approach and integration arrangements should allow United Nations and other humanitarian actors to deliver according to humanitarian principles and should facilitate effective humanitarian coordination with all humanitarian actors.⁶⁰

Other internationally mandated deployments of military and police forces raise similar concerns, often in more acute form. These forces are usually involved in hostilities against one or more local forces. Interacting with them can therefore be very complex. However, it is also important to recognize their potential for contributing to PoC and to engage 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 or support their military operations, they must take all feasible steps to ensure that the parties, particularly those with which they are partnering, comply with their IHL obligations.⁶¹ Dialogue and interaction between humanitarian actors and these forces will therefore be needed, to ensure that those forces fulfil their obligations and that their local partners fulfil their obligations to respect and protect civilians during their military operations.

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

⁵⁹ UN, *Policy on Integrated Assessment and Planning*, 8 February 2023, para. 9.

⁶⁰ *Ibid.*, para 20.

⁶¹ 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.

During peacekeeping operations, UN human rights actors interact with UN military and police components as defined by policy. Continuous efforts to exchange information and coordinate work are also required, however. 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 the exchange of information.

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 affected populations or humanitarian workers to greater risks.

G

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

Protection actors should seek and promote a common contextual understanding of the roles and responsibilities of the various actors engaged in enhancing protection in the field.⁶²

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

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
- 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 sometimes constitute an indirect channel for advocacy efforts with senior local government personnel and officials of the armed forces.

It may be necessary to address some of the issues documented at higher levels, with the UN Secretariat in New York and Geneva, or with the military and political authorities of 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 OCHA, including its Civil-Military Coordination (CM-Coord) Officers and Focal Points⁶³ or national networks.

⁶² For further guidance, see, for instance, GPC, *Diagnostic Tool and Guidance on the Interaction between field Protection Clusters and UN Missions*, 2013.

⁶³ See UNOCHA, *Guidance Note on OCHA CMCoord Support to Protection Outcomes*, 2020.

G

6.10 Protection actors should interact 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, and to ensure 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 of and respect for IHRL (and IHL and IRL where applicable), together with other protection concerns and trends where appropriate. Internationally mandated military forces and police services working with domestic forces and services have an obligation to ensure that they respect their obligations under IHL.

Protection actors may therefore approach internationally mandated forces on various issues, such as:

- the precautionary measures they take when engaged in hostilities
- displacement
- arrest and detention
- proper procedures for the management of human remains, including their transfer and handover and the management of post-mortem data to prevent disappearances.

Information exchange may involve sharing non-confidential information on general trends and on risks facing civilian populations. It requires proper procedures and agreed communication channels and must be conducted in conformity with data management standards (see Chapter 7). 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 essential in order to achieve improved protection outcomes. This must be conducted 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 take care not to undermine the ability of humanitarian actors to operate according to their principles and to be perceived as doing so. Protection actors, collectively or individually, should develop a review mechanism to avoid these risks.

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.

S

6.11 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.⁶⁴

Large sectors of the population and some of the parties engaged in the fighting may not see these entities as neutral and impartial, whether or not they are engaged in the conduct of hostilities or the use of force, because of their very nature. 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, the greater the risks. All protection actors must therefore reassess and adapt their engagement regularly in the light of these risks and the changing environment.

⁶⁴ See also Standard 5.2.

COMMUNITIES, CIVIL SOCIETY AND OTHER ACTORS

S

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

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

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

Through their policies and programmes, economic actors such as those responsible for domestic development policy or international development assistance may help create an environment conducive to protection – or may do the opposite. They may also be able to influence primary duty bearers to enhance the protection of people at risk.

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

Assessing which of these actors is best positioned to have the desired impact also requires interaction and a will to identify and foster synergies. Communicating about humanitarian principles and activities to wider audiences may have a positive impact. When engaging with private-sector, political, judicial and economic actors, protection actors must maintain their adherence to humanitarian principles.

G

6.13 Protection actors should support civil society and other local actors' efforts to take preventive action to reinforce capacities, reduce risks and vulnerabilities or mitigate the impact of protection risks on affected people.

Engaging local/national actors (L/NAs) is critical to the success of humanitarian action. L/NAs are often the first responders and are at the heart of humanitarian prevention and response efforts. They provide an invaluable understanding of local challenges and potential solutions, can mobilize local networks and offer greater access to affected populations, hence contributing to more effective, efficient and sustainable humanitarian prevention and response action, with enhanced accountability to affected populations. They are also often adept at working across the humanitarian-development-peace nexus to support affected communities in their preparedness, response and recovery, and after the withdrawal of international actors.⁶⁵

⁶⁵ IASC, [IASC Guidance on Strengthening Participation, Representation and Leadership of Local and National Actors in IASC Humanitarian Coordination Mechanisms](#).



6.14 Protection actors must support communities' own protection dialogues with duty bearers and others and, where relevant and appropriate, ensure that their own interactions with those stakeholders support those of communities.

Protection actors must understand whether communities have any dialogue with perpetrators of violations and how protection actors could support communities' efforts. Protection actors must take great care to understand the potential risks involved and undertake regular discussion with communities to ensure that their approaches continue to be aligned.

Independent civil society can play an important role in mitigating the protection risks to which communities are exposed.

They may use their expertise to:

- raise awareness on topics including the applicable national and international legal frameworks
- inform people of their rights
- conduct advocacy and capacity-building
- monitor and report on issues of concern.

Civil society organizations are stakeholders whose positions, principles and capacities we should understand and support where appropriate and possible.

Since civil society organizations are often permanently present in communities, they can play an important role in preventing the violation of rights through the above-mentioned modes of action, by influencing policy- and law-making and by pushing for greater accountability on the part of duty bearers. Protection actors should support existing prevention efforts through measures such as capacity-building.

REFERENCE MATERIAL FOR CHAPTER 6

DPKO/DFS/DPPA, [Policy on Child Protection in United Nations Peace Operations](#), 2017

GPC, [Diagnostic Tool and Guidance on the Interaction between Field Protection Clusters and UN Missions](#), 2013

IASC, [Civil-Military Guidelines and Reference for Complex Emergencies](#), March 2008

IASC, [Growing the Sheltering Tree: Protecting Rights through Humanitarian Action – Programmes and Practices Gathered from the Field](#), 2002

IASC, [Policy on Protection in Humanitarian Action](#), 14 October 2016

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

OCHA, [Aide-Memoire for the Consideration of Issues Pertaining to the Protection of Civilians in Armed Conflict](#), 2014

OCHA, [Building a Culture of Protection: 20 Years of Security Council Engagement on the Protection of Civilians](#), 2019

OCHA, [Guidance Note on OCHA CMCoord Support to Protection Outcomes](#), 2020

OCHA, [Security Council Norms and Practice on the Protection of Civilians in Armed Conflict](#), 2014

OHCHR/DPKO/DFS/DPA, [Human Rights in United Nations Peace Operations and Political Missions](#), 2011

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

UN, [Guidance Note on Human Rights Due Diligence Policy on UN Support to Non-United Nations Security Forces](#), 2015

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

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, [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

UN, [United Nations Policy on Integrated Assessment and Planning](#), 2023

UN, [Uniting our Strengths for Peace – Politics, Partnership and People, Report of the High-Level Independent Panel on Peace Operations](#), June 2015

UNDPKO/DFS, [Guidelines on Use of Force by Military Components in Peacekeeping Operations](#), 2016

UNDPKO/DFS, [Protection of Civilians: Implementing Guidelines for Military Components of United Nations Peacekeeping Missions](#), 2015

UNDPKO/DFS, [The Role Of UNPOL In Protection Of Civilians](#), 2017

UNDPKO/DFS, [United Nations Peacekeeping Operations, Principles and Guidelines](#), 2008

UNDPO, [Protection of Civilians in United Nations Peacekeeping](#), 2023

UNDPO, [The Protection of Civilians in United Nations Peacekeeping Handbook](#), 2020



7. MANAGING DATA AND INFORMATION FOR PROTECTION OUTCOMES

GENERAL STANDARDS FOR THE MANAGEMENT OF PROTECTION DATA AND INFORMATION

Lawful, legitimate and fair management

- S** 7.1 Protection data and information must be managed in a fair and legitimate manner. Personal data must be processed only if there is a lawful basis for doing so.

Defined purpose, necessity and proportionality

- S** 7.2 Protection data and information and their management must serve clearly defined and specific purposes, be proportional and relevant to those purposes and aim at achieving protection outcomes. Where protection actors process personal data, such data must be adequate and relevant to the clearly defined, specific purposes and must not exceed such purposes.

Data quality

- S** 7.3 Protection data and information must be relevant, accurate, timely, complete, standardized, interoperable, well-documented, up to date and interpretable, in line with their intended use and the operational context. Protection actors must ensure that inaccurate personal data are corrected or deleted without undue delay.

Data retention

- S** 7.4 Protection actors must set clear schedules and methods for the retention and destruction of protection data. To ensure that sensitive protection data and personal data are not kept longer than necessary, they must set a retention period, at the end of which they must decide whether to extend the retention period, erase the data or archive them.

Data security

- S** 7.5 Guided by organizational and technical procedures and safeguards, protection data must be managed in a manner that ensures an appropriate degree of security for as long as the data are retained, in line with the sensitivity of the data and ensuring the risk of data breaches is minimized. Protection actors must have procedures in place to ensure correct identification, mitigation and rectification of personal data breaches.

Confidentiality

- S** 7.6 Protection data and information must be managed in a manner that ensures an appropriate degree of confidentiality for as long as data are retained.

Assessing risks and benefits

- S** 7.7 At each step of managing and processing protection data, protection actors must assess the risks and benefits and maximize the benefits while preventing, reducing or mitigating potential adverse consequences for affected people and communities. Special consideration must be given to the identification, assessment and mitigation of risk connected with the processing of personal data.

Avoiding bias and discrimination

- S** 7.8 Protection actors must manage 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 disaggregate for age, gender and other factors of diversity.

Transparency

- S** 7.9 People must receive timely, clear and concise information regarding the management of protection data and information and the processing of personal data. That information must include who processes personal data, for what purpose, on what basis and for how long, together with details regarding data sharing and data subject rights.

Coordination and collaboration

- S** 7.10 Protection actors must refrain from duplicating the collection of protection data and information, to avoid unnecessary burdens and risks for affected people and communities.

Data sharing and transfer

- S** 7.11 Protection data and information may only be transferred to or shared with those recipients who require access to fulfil the clearly defined, specific and legitimate purposes for which the data are managed and who can guarantee the required level of data security and, where required, data protection.

Accountability

- S** 7.12 Protection actors must be accountable for their management of protection data and information. They must be able to demonstrate that personal data are processed in line with data protection principles and that adequate and proportionate measures have been put in place.
- G** 7.13 Protection actors should be accountable for their management of protection data and, where possible, provide feedback and information to affected people and communities about actions taken and results achieved.

ADDITIONAL STANDARDS FOR THE PROCESSING OF PERSONAL DATA

Compliance with legal frameworks

- S** 7.14 Protection actors must process personal data in accordance with the rules and principles of international, regional and national laws on data protection and/or organizational policy and guidance, as applicable.

Main actors of personal data processing

- G** 7.15 Protection actors should take account of the rules, regulations, roles and responsibilities of the actors involved in processing personal data.

Data protection by design and default

- S** 7.16 Data protection must be integrated in the design and development of protection data and information management systems and tools from the outset, ensuring that privacy is a core property.

Data subject rights

- S** 7.17 Protection actors must take action to respect and promote the ability of people whose personal data are processed to exercise their rights as data subjects.

INTRODUCTION

This chapter presents the standards to apply when processing personal data and best practices for the responsible management of protection data, including sensitive non-personal data. The chapter supports protection actors in upholding the Core Humanitarian Standard, including Standard 4.3 – Ensure safe, ethical and effective management of data and information to minimise risks for people and communities in line with recognised good practice for data protection.⁶⁶ For more detailed information and guidance on the processing of personal data, please refer to the ICRC’s *Handbook on Data Protection in Humanitarian Action*.⁶⁷ For more detailed information and guidance on the responsible management of data in humanitarian contexts, please refer to the IASC’s *Operational Guidance on Data Responsibility in Humanitarian Action*.⁶⁸

The padlock icon  indicates obligations regarding personal data that emanate from internationally accepted data protection standards.

STRUCTURE OF THE CHAPTER

Section 1

General standards and guidelines applicable to the management of all protection data and information, including sensitive data (personal and non-personal), making the necessary distinctions when specific measures are required for the processing of personal data.

These standards and guidelines apply to all aspects of the data management process, including collection or receipt, storage, quality assurance, analysis, sharing, use, retention, transfer and destruction.⁶⁹

Section 2

Standards and guidelines that apply to the processing of personal data.

These likewise apply throughout the entire life-cycle of personal data processing. Failure to apply these standards and guidelines may harm the people whose personal data are processed and may have legal consequences for the protection actor.

Personal data protection is recognized in many national, regional and international legal regimes as a key component of ensuring respect for people’s rights and freedoms. These regimes include clear rules and obligations regarding personal data.

WHAT IS PROTECTION DATA AND INFORMATION MANAGEMENT AND WHY IS IT IMPORTANT?

Protection work must use timely evidence and respond as closely as possible to the priorities of affected people. Protection data and information management is essential to this purpose, as it enables informed action to achieve protection results and outcomes. Protection data and information management, including the lawful and legitimate processing of personal data, generates the evidence needed to understand a particular context and associated protection risks, and to develop protection strategies and protection responses, including resource mobilization, protection programming and advocacy on protection.⁷⁰

Given the potential sensitivity of protection data and information and the legal obligations governing the processing of personal data, it is essential to manage them responsibly at each step of the data management process and to comply with data protection standards. Safe, ethical and effective management of protection data, including sensitive protection data, and lawful and transparent processing of personal data, are essential aspects of protecting people’s lives, their physical and mental well-being, their rights and their dignity.

⁶⁶ Core Humanitarian Standard, 2024.

⁶⁷ ICRC, [Handbook on Data Protection in Humanitarian Action](#), 3rd edition, Cambridge University Press, 2024.

⁶⁸ IASC, [Operational Guidance on Data Responsibility in Humanitarian Action](#), 2023.

⁶⁹ The standards presented in the first section are based on the [IASC Operational Guidance on Data Responsibility in Humanitarian Action \(2023\)](#) and the [Protection Information Management \(PIM\) Principles](#).

⁷⁰ See Chapter 3, on managing protection strategies.

The term “management of protection data and information” refers to the processes of managing data – the collection or receipt, storage, quality assurance, analysis, sharing, use, retention and destruction of protection data – that are required to enable evidence-based action for protection results and outcomes. The management of data requires multiple systems, processes, methods and tools that serve different purposes and produce different outputs in terms of data and information. Protection data must be managed safely, ethically and effectively, on a legitimate basis and in accordance with any legal obligations. The standards in this chapter promote clarity and best practices, to ensure more responsible, systematic and collaborative approaches.⁷¹

When designing and implementing a data and information management process, it is important to distinguish between personal data and non-personal data, noting that both can be sensitive, and both can expose people to risks. Data protection is recognized in international, regional or national law as a key component of ensuring respect for people’s rights and freedoms. When processing personal data, humanitarian organizations must adhere to national and regional data protection laws or, if they enjoy privileges and immunities such that national and regional laws do not apply to them, to their own data protection policies.

Working with protection data – including personal data and sensitive data (be it personal or non-personal) – can generate real-life risks for people, often with greater impact on the most vulnerable.

These risks may stem from:

- data sharing with other organizations, private actors, donors or governments without the necessary assessments and safeguards
- interception, theft, leakage, mishandling or misuse (see more in Chapter 8 and in Annex 2 to this chapter).

Other risks may result from data disaggregation or aggregation, and decision-making based on biased analysis or unverified information.

This chapter seeks to ensure that protection actors manage data in a responsible manner – i.e. safely, ethically and effectively – and in line with legal obligations and international data protection standards.

PROTECTION INFORMATION MANAGEMENT

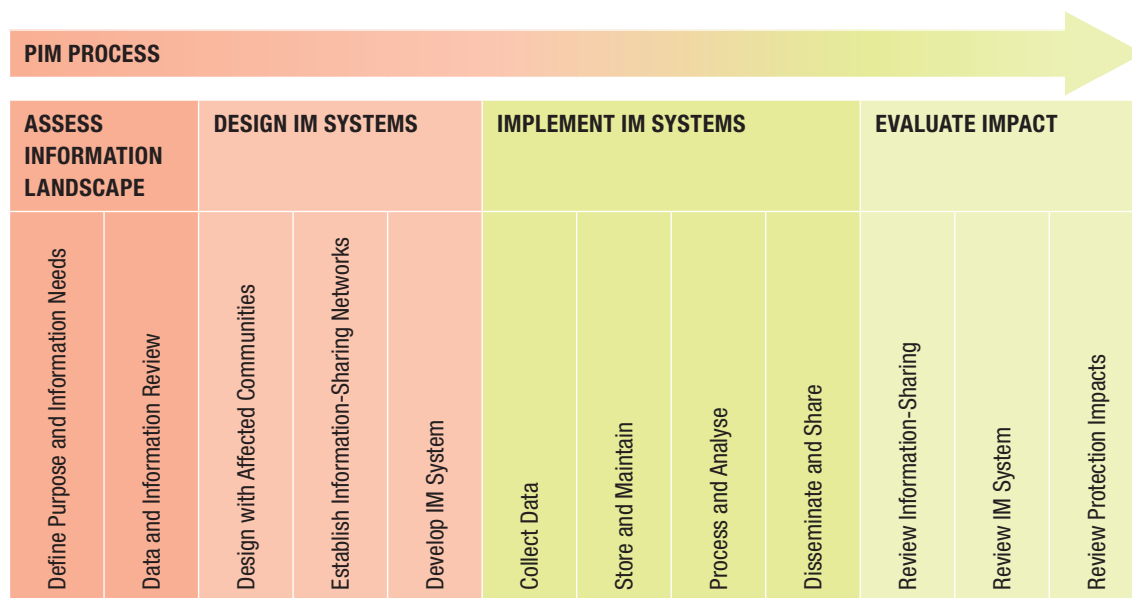
Making sense of the complexity of a humanitarian situation – understanding the protection risks, threats, vulnerabilities and capacities of affected people in order to plan and implement a coordinated response and monitor its impact, to effectively advocate and to mobilize resources – often means managing large quantities of data and information for decision-making, some of which will be sensitive.

The objective of protection information management (PIM) is to provide quality data and information on the protection of affected people in a given setting, to enable evidence-informed action for protection outcomes, and to do so in a safe and reliable manner.

Managing protection data and information often involves dealing with a number of sensitivities that are inherent to protection work, the contexts in which it is undertaken and the purposes it serves. For example, unauthorized disclosure of or access to personal data and/or sensitive protection data or information (such as violations of rights or threats of violations, patterns of violence, abuse, coercion and deprivation) may result in harm to the people whom protection actors aim to protect. The circumstances in which protection actors operate, in particular during armed conflict and other violence, create special challenges and require particular attention to the “do no harm” principle throughout the data and information management process.

⁷¹ See also the PIM Framework, comprising the definitions, principles, guidance, core competencies and other products of the [Protection Information Management Initiative](#).

Selecting the most relevant and appropriate systems, methods and tools for protection of data and information requires careful consideration of the operational context and the intended use of the data. Competent staff are needed to manage the data, to take account of possible bias⁷² and to assess the risks and benefits. Those staff should also be able to identify and assess the challenges associated with information and communication technologies (ICT),⁷³ including emerging technologies such as artificial intelligence and blockchain⁷⁴ that create opportunities for humanitarian and human rights action, as well as risks.



PIM - Protection Information Management Initiative (Danish Refugee Council and UNHCR)

These steps can be followed when designing and implementing any protection information management system, such as protection monitoring, protection needs assessments, case management or protection response monitoring.

The PIM process diagram highlights the importance of specifying from the outset the purposes for which data will be gathered. These purposes must also be communicated to those who will provide information.

While engagement with affected people must pervade the entire process, it is particularly important in the “Design IM Systems” step. Timely engagement enables protection actors to design systems that are appropriate and feasible in a given operational context, gathering the right protection data to design the response and meet protection priorities.

The diagram also highlights the importance of thinking about the sharing of protection data and information from the outset, before any data are gathered, in order to facilitate responsible sharing and to maximize use and re-use of the data, bearing in mind data protection requirements should personal data be in scope.

Lastly, the diagram highlights the need to not only implement data and information management but also evaluate its impact and ensure it remains fit for purpose. This includes determining whether data collection methods remain appropriate and safe in the context, whether the data analysis process is generating timely findings and recommendations that meet the defined purpose(s), whether data are being shared with other actors (and if so, whether the necessary safeguards are being implemented), whether the information is being effectively used to guide decisions, etc.

⁷² See Chapter 2, Standards 2.2 and 2.3.

⁷³ See Chapter 8 on digital risks.

⁷⁴ See more in Annex 1 to this chapter.

PROTECTION DATA AND INFORMATION: TYPES OF DATA, SENSITIVITY AND REQUIREMENTS

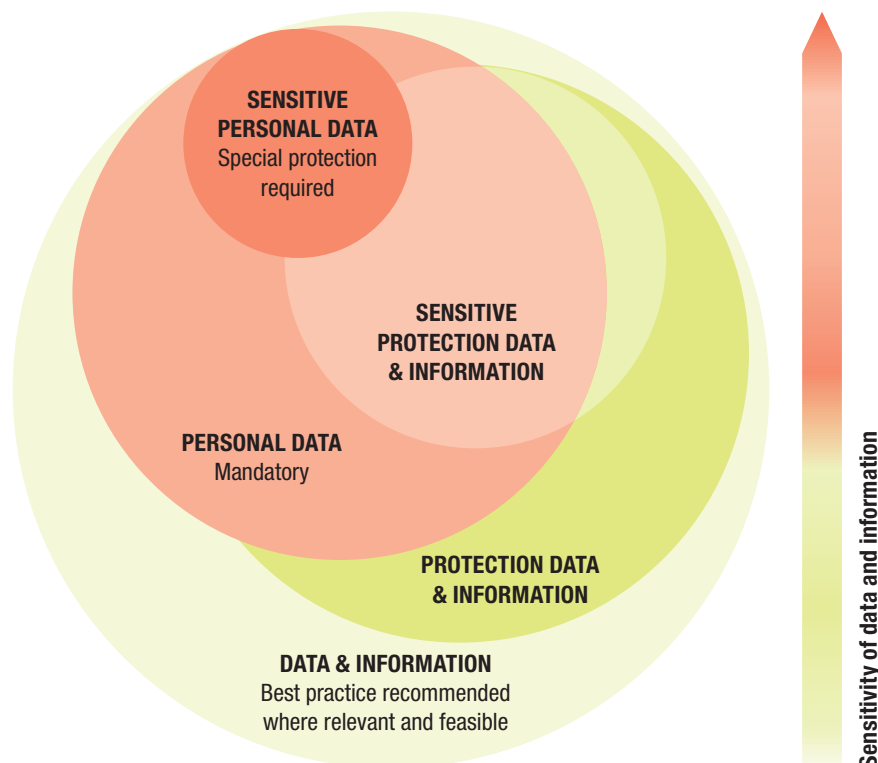
Data are raw, unorganized facts or figures that are collected and stored. They can exist as numbers, text, images or in other forms. On their own, they lack context and meaning. They are the most basic form of representation and need to be combined with other data and interpreted to become useful. “Information” is data in context. It is data that have been analysed, structured and given meaning in context. Information can be used to answer questions and make decisions. It is the result of data being combined and transformed so they can be used for a specific purpose.

Protection data are data that protection actors manage in order to carry out their operations for and with communities affected by crisis, conflict or other violence. Before collecting or receiving data or before designing a protection data and information management system, protection actors must determine what data and information they require and for which purposes, together with their level of sensitivity. Data and information managed for protection outcomes should be considered protection data, regardless of whether they were initially collected specifically as protection data.

Protection information is protection data that have been combined and analysed to make sense of them and provide insights. It includes information about the protection situation or context, the people affected by that situation, the protection risks, the response and its impact. Together, this information enables evidence-based design and implementation of protection strategies, programmes and other actions, together with monitoring and reporting. Protection information is used by protection and other actors to achieve evidence-based protection outcomes.

There are different types of protection data and information. Several broad categories are illustrated below. The diagram shows that as the sensitivity of the data and information increases, so too should the formality and stringency of the rules and standards that are applied to manage it. These categories sometimes overlap, in which case the higher level of safeguards should be applied.

APPLICATION OF STANDARDS AND PERSONAL DATA PROTECTION PRINCIPLES



Data and information types and sensitivity

Before gathering any data, protection actors must take the following action:

1. Define the categories of data they need for their purposes, consulting other actors as needed to ensure their efforts will meet the information needs of all involved in the response as far as possible.
2. Establish the sensitivity levels of the data in their context.
3. Establish the security measures required for each category and sensitivity level.

This will allow protection actors to define and classify their data in a consistent manner, maximizing the benefits and utility of the data and limiting the risk of harm.

Protection actors should adopt systems, methods, tools and approaches that enable responsible management of protection data and information. This includes both non-personal and personal data, noting that personal data are governed by legal frameworks, are most commonly recognized in applicable law and require compliance with requirements discussed in Sections 1 and 2 of this chapter. When processing personal data, protection actors must adhere to either data protection laws or their own organizational rules on data protection, if they enjoy privileges and immunities (see Section 2).

This chapter sets out standards and guidelines for protection data and information, which include both personal data and non-personal data.

When planning their approach, protection actors must establish internal policies and procedures that will take account of such factors as:

- organizational mandate
- operational context
- operational capacity
- potential harm⁷⁵ to individuals and communities
- financial, human and technological resources
- the nature of the protection data and their sensitivity level
- the timelines of the decisions the information is intended to guide.

Both personal and non-personal protection data can be sensitive. Data sensitivity is defined in relation to the response context; the same data may have different levels of sensitivity in different contexts and sensitivity may change over time. Due consideration must also be given to how data can be combined in ways that increase their sensitivity or conversely, how data can become more sensitive if extracted from a larger dataset and used in isolation. Many organizations have classification systems and tools⁷⁶ to assess data sensitivity, in order to facilitate responsible data management practices.

Protection data and information are sensitive if disclosing or accessing them without proper authorization is likely to cause:

- harm to the well-being of any person
- infringement of rights, including the rights of the source of the information and those of other identifiable people or groups
- damage to an organization's capacity to carry out its activities or to public perceptions of the organization.

The above definition emphasizes that non-personal protection data can also be sensitive.

⁷⁵ The principle of “do no harm”, for instance, requires protection actors to prevent and mitigate any negative impact of their actions on affected people. “Harm” can include violations or abuses of rights, including the right to protection from torture and cruel and inhumane or degrading treatment; to protection against arbitrary arrest, detention or exile; the right to marry and found a family and the right to a fair trial. International human rights law, humanitarian law and refugee law are the sources of internationally accepted human rights and should be considered when assessing potential harm.

⁷⁶ E.g. the [OCHA Data Responsibility Guidelines](#).

For example, a map of a protection of civilians site can be useful for coordinating response. However, it can also be used by armed groups to plan an attack, especially if the map shows the location of internally displaced populations, staff quarters, guard towers, etc.


Similarly, a public infographic that shows border crossings and displacement routes can be used by smugglers and traffickers, exacerbating protection risks when people are fleeing to safety.

Location data can also be sensitive, for example the GIS coordinates of alleged human rights violations such as a mass killing.

Even though sensitive non-personal data are not regulated by legal frameworks, technical, procedural and organizational safeguards must be applied to ensure they are accessed, shared and used responsibly.

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

This section presents the standards and guidelines for the responsible management of protection data and information, including the types of data and information that protection activities generate and use. It presents the general standards that apply to the management of all types of protection data.⁷⁷


The padlock icon  indicates obligations regarding personal data that emanate from internationally accepted data protection standards.

LAWFUL, LEGITIMATE AND FAIR MANAGEMENT



7.1 Protection data and information must be managed in a fair and legitimate manner. Personal data must be processed only if there is a lawful basis for doing so.

In some cases, the legitimate basis for managing protection data will be based on the best and/or vital interests of the affected person and the protection actor's mandate and expertise. Fairness and legitimacy in the management of protection data enable a more neutral and impartial response and foster respect for and the promotion of rights and freedoms.

-  Personal data must be processed fairly and lawfully. Processing is only lawful⁷⁸ if there is a lawful basis⁷⁹ for processing to take place, as described below. The other crucial component of fair processing is transparency, which is described in Standard 7.9.

⁷⁷ See also Chapter 3 on managing protection strategies.

⁷⁸ See ICRC, [Handbook on Data Protection in Humanitarian Action](#), 2024, Section 2.5.1.

⁷⁹ This concept may be referred to as the “legal basis” or the “lawful basis”; the terms are synonymous.

Internationally accepted lawful bases for personal data processing include:

1. Consent of the person concerned or their legal guardian. This must be freely given, informed, specific and unambiguous. Consent is discussed in further detail below.
2. Vital interest of the data subject or of another person. This applies where the processing of personal data is necessary to protect the life, physical or mental well-being, health, dignity or security of the data subject or other person.

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

3. Public interest, in particular in the implementation of protection activities, such as those grounded in the mandates of international organizations conferred 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.

4. Legitimate interest of a protection actor. Processing may also be carried out where a legitimate interest exists and the processing is necessary for the purpose of carrying out a specific activity contained in the protection actor's mission, provided that this interest is not overridden by the interests or fundamental rights and freedoms of the data subject.

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.

The most common way of determining whether legitimate interest is applicable is to conduct a legitimate interest assessment (LIA).⁸⁰

Other common lawful bases, such as processing for the performance of a contract or compliance with a legal obligation, are less likely to apply to protection work and are therefore not described in this section.

A lawful basis is tied to the purpose of processing personal data and legitimizes that purpose. More than one basis may apply, in which case all options should be identified and documented from the start. Every lawful basis allows for the processing of personal data and no lawful basis is “better” than another. The applicable basis or bases will depend on many factors, in particular the purpose of processing, the category of data, the category of person and the existence of a mandate or law.

When determining the correct lawful basis, consent should not be seen as the preferred or default option; the best lawful basis should be selected in the light of circumstances. This will ensure that consent is not used as a lawful basis where such consent cannot be freely given and informed.

⁸⁰ See the example LIA published by the UK Information Commissioner's Office: [How do we apply legitimate interests in practice?](#)

Furthermore, certain data protection laws may differentiate between “normal” personal data and “special categories of data”.⁸¹ These special categories include sensitive personal data that may require a separate or additional lawful basis for processing in order to ensure that such data are not processed excessively.

Consent

Consent as a legal concept for processing personal data is not the same as *informed consent* as a protection working modality. In both cases, consent means enabling people to have the final say over what happens to them or to their data. However, depending on circumstances, consent as a lawful basis for personal data processing might not be the best way to protect people’s rights and interests. Informed consent as an ethical working modality is meant to be the foundation of protection actors’ relationship with people, regardless of circumstances.

For protection actors, it is especially important to ensure that consent is obtained in ways that are culturally appropriate and relevant. Collection of protection data and information should not take place until staff have been trained, to ensure that they understand and respect the notion of consent. Protection actors should provide timely, clear and concise information to people who have difficulty understanding the information they need in order to give informed consent. This may involve using such means as visuals, audio or easy-to-read text.

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

In the situations in which protection actors usually operate, and during sudden onset or large-scale emergencies, it can be difficult to ensure that consent is freely given and informed, especially if consenting to the processing of personal data is a precondition for receiving protection. In these situations, the protection actor will require another lawful basis to process personal data, such as vital interest, public interest or legitimate interest.

Finally, obtaining consent does not relieve a protection actor of its responsibility to assess and mitigate the risks to an individual or group arising from the management of protection data or information. If the protection actor determines that the risks are excessive and are not warranted by the intended protection outcome, the personal data or information should not be processed, even if the consenting individuals are informed of these risks.

Consent is voluntary, informed, and freely given on the basis of a clear appreciation and understanding of the facts, and of the risks, implications and future consequences of an action. Staff must therefore record and specify which information can be used or disclosed and how, including the identity of the person and whether the information may be used on condition that their identity be kept confidential.

⁸¹ Examples of such classification can be found in Art. 9 of the European Union’s [General Data Protection Regulation \(GDPR\)](#), which lists the following special categories of data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person’s sex life or sexual orientation. Under the GDPR, processing this data is prohibited unless both a lawful basis and a separate condition exist. Legitimate interest is not a lawful basis in the case of special categories of data unless the protection actor can also show that a separate Article 9 condition also exists.

At a minimum, the information below must be communicated to the source of information or the data subject in order for consent to be regarded as “informed”:

- the identity of the organization collecting the data and a brief explanation of its mandate
- the purpose of the data collection exercise, its scope and method and the intended use of the data (to present cases, to provide assistance, for statistical purposes, etc.)
- the potential risks and benefits of participation in the data collection exercise
- contact information, so the person can contact the organization collecting the data
- the duration for which the data will be used or stored and how and where they will be kept
- to whom the data will or are likely to be communicated (especially if they may be passed on to authorities, such as law-enforcement authorities, non-state armed groups, *de facto* authorities, etc.) and whether the data will be transmitted across an international border
- a reminder that the person has the right to:
 - stop participating at any time
 - object to the processing of their personal data
 - demand access to their personal data
 - demand corrections to personal data they have provided
 - demand that their personal data be destroyed.

When major changes occur, such as the emergence of new or significant risks, consent may no longer be valid and should therefore be obtained anew.

When processing personal data, the consent of the person concerned – or in certain cases that of their legal guardian – is an important lawful basis. However, the high threshold for consent, the potential vulnerability of affected people and the nature of protection work mean that some protection actors will not be able to rely on consent for most of their personal data processing. Regardless of the lawful basis, data subject rights ensure the agency and involvement of people with regard to how their personal data are processed (see more in Standard 7.17).

For consent to be valid as a lawful basis, it must be freely given, specific, informed and unambiguous.

Freely given implies that a person has real choice and control. Where there is no real choice or the person feels compelled to provide it, consent is not freely given. The same is true if the person will experience negative consequences if they do not provide consent, or if they are unable to withdraw their consent without detriment.

Consent may also not be freely given where there is a strong and evident imbalance of power between the controller⁸² and the individual. Such an imbalance can result from the controller’s strong position, lack of alternatives to processing by this controller or the situation of the person, for example if their vulnerability forces them to provide consent.

⁸² See Standard 7.15.

Informed and specific together imply that the data subject must be enabled to fully understand the purpose of consent, appreciate the risks and benefits of providing it and understand the processing of the personal data or protection information. Consent acquired without doing this may not be considered valid. The person must receive explanations in simple, jargon-free language. Consent may also not be informed when data processing involves complex data flows using computer systems, when multiple stakeholders are involved or when the susceptibility of data or information to interception and misuse is unclear or dependent on technical considerations, thus preventing the individual from making a fully informed assessment of the risks involved.

Unambiguous implies that consent must be obtained through clear action or declaration, so as to leave no doubt as to whether the person provided their consent. It must be obvious to the person that they have consented, as consent should be an obvious and clear indication of their wish to have their personal data processed. This does not mean that consent can only be provided in writing, but it does mean that there should be a clear and affirmative action on the part of the person.

DEFINED AND SPECIFIC PURPOSE, NECESSITY AND PROPORTIONALITY

S

7.2 Protection data and information and their management must serve clearly defined and specific purposes, be proportional and relevant to those purposes and aim at achieving protection outcomes. Where protection actors process personal data, such data must be adequate and relevant to the clearly defined, specific purposes and must not exceed such purposes.

When working with protection data or setting up a data and information management system, protection actors must define the purposes for which data will be used and ensure this use will meet protection actors' information needs. Protection actors should be clear and open when communicating with stakeholders about the purposes of data management. This includes providing timely and accurate information to affected populations, in a format and style that takes advantage of their preferred communication channels. Protection actors should also ensure that the purposes do not evolve over time without a deliberate decision (function creep⁸³), as this may undermine the legitimacy of data management and potentially expose affected people to new or greater harm.

A data management activity can have multiple purposes, each of which should be specified so as to ensure consensus and clarity regarding the uses and users of the data. For example, a specific purpose such as "Prioritize locations and population profiles in province A for the delivery of non-food items in the second quarter", rather than the general "Provide humanitarian assistance" creates clarity and promotes more effective approaches. It also reduces the risk of unnecessary data gathering that may expose both staff and affected populations to harm.

🔒 Personal data must also be processed in accordance with the principles of data minimization and purpose limitation.⁸⁴

Data minimization seeks to ensure that only the minimum amount of data is processed to achieve the objective and purposes for which the data were collected. Data minimization is essential for the management of protection data. Protection actors must determine the scope, level of precision and depth of detail of the data collection exercise, in accordance with the use they intend to make of the data. This principle is particularly important in the context of inter-agency coordination and of multi-sectoral needs assessments conducted by humanitarian organizations, where protection actors may gather excessive amounts of data if they do not

⁸³ Bert-Jaap Koops, [The Concept Of Function Creep](#), Law, Innovation and Technology, 2021.

⁸⁴ See ICRC, [Handbook on Data Protection in Humanitarian Action](#), 2024, Sections 2.5.2 and 2.5.4.

coordinate and prioritize their information needs, defining those needs in accordance what they need to know to achieve their defined purposes rather than what is interesting.

When processing personal data and non-personal sensitive data, determining whether minimization requirements are being respected involves answering the following questions:

- Is the scope of data adequate?
- Is the scope of data relevant?
- Is the scope of data limited?

Purpose limitation means defining and stating the specific purposes for which data are to be managed or processed. Those purposes must be explicit and legitimate. Purpose limitation is related to the concept of further processing, which allows protection actors to process data, including personal data, for purposes other than those specified at the time of collection, but only where further processing is compatible with the initial purpose, including where necessary for historical, statistical or scientific purposes. To assess the compatibility of the purposes, protection actors need to take account of the following factors in particular:

- the link between the initial purpose and the intended further purpose, and the consequences of the further purpose
- the circumstances of data collection
- the nature of the data
- the existence of appropriate safeguards
- the person's expectations regarding further processing.

DATA QUALITY



7.3 Protection data and information must be relevant, accurate, timely, complete, standardized, interoperable, well-documented, up to date and interpretable, in line with their intended use and the operational context. Protection actors must ensure that inaccurate personal data are corrected or deleted without undue delay.

Data quality must be such that data management activities and their resulting products can be trusted, and can achieve their purposes and their intended protection outcomes.

Data quality is adequate if data are:

- relevant
- accurate
- timely
- complete
- standardized
- interoperable
- well-documented
- up to date
- interpretable

in the light of the intended use of the data and the operational context.

Where feasible and appropriate, protection actors should collect and analyse data by age, gender and other factors of diversity.

In accordance with Standard 7.9, ensuring data quality also includes providing information about the data and the related data management activity, such as intended uses of the data and any limitations. Protection actors should periodically review their data and information to assess their reliability, accuracy and currency.

Misinformation and disinformation spread rapidly in humanitarian and crisis settings, so protection actors must verify data and information using multiple trusted sources and tools to corroborate (triangulate) them and ensure their quality as far as possible.

- Ⓐ Every reasonable step must be taken to ensure that inaccurate personal data are deleted or corrected without undue delay, taking into account the purposes for which they are processed. It may be necessary to verify that data are reliable, accurate and up to date. In considering the frequency of review, account should be taken of, in particular:
 - logistical and security constraints in the operational context
 - the purposes of processing
 - the potential consequences of personal data being inaccurate.⁸⁵

DATA RETENTION

S

7.4 Protection actors must set clear schedules and methods for the retention and destruction of protection data. To ensure that sensitive protection data and personal data are not kept longer than necessary, they must set a retention period, at the end of which they must decide whether to extend the retention period, erase the data or archive them.

Protection actors must establish a data retention and destruction schedule that indicates how long data will be retained and when and how they will be irretrievably destroyed. Sensitive data must only be retained for as long as they are necessary for the specified purposes for which they are managed or as required by laws or audit regulations. When retaining sensitive data, organizations must ensure their safe and secure storage to prevent misuse or exposure. Procedures that set out schedules for data destruction must include guidance and/or tools on how to do so in a way that renders data retrieval impossible. Protection data must be retained in line with laws, regulations and policies and provided that access rights are established and the sensitivity of the data is reassessed on a regular basis.

- Ⓐ Where personal data are processed, a review must be carried out at the end of the specified retention period to determine whether to extend the retention period, erase the data or archive them. In certain exceptional cases, when a protection actor processes personal data for a further compatible purpose, they must also identify the correct retention period for this further purpose (described further in Standard 7.14).⁸⁶

DATA SECURITY

S

7.5 Guided by organizational and technical procedures and safeguards, protection data must be managed in a manner that ensures an appropriate degree of security for as long as the data are retained, in line with the sensitivity of the data and ensuring the risk of data breaches is minimized. Protection actors must have procedures in place to ensure correct identification, mitigation and rectification of personal data breaches.

Data security is a crucial component of managing protection data in a safe, effective and ethical manner. Protection actors must implement appropriate organizational and technical safeguards, procedures and systems to prevent, mitigate, report and respond to material external breaches, unauthorized or inappropriate internal access or manipulation, accidental disclosure, damage, alteration, loss and other security risks related to data management. Data security measures must be based on the sensitivity of the data, updated as data security standards and best practices evolve and be in place prior to any collection of data or information. The protection actor must ensure the integrity and confidentiality of the data and their availability for authorized users at all times.

⁸⁵ See ICRC, [Handbook on Data Protection in Humanitarian Action](#), 2024, Section 2.5.5.

⁸⁶ For more on the concept of further processing, see ICRC, [Handbook on Data Protection in Humanitarian Action](#), 2024, Section 2.5.2.1.

Which measures are required depends on, *inter alia*:

- the sensitivity of the data, based on the potential harm its unauthorized access or use would cause and the likelihood of this risk materializing
- the possible consequences to the people concerned
- the type of protection activity
- the obligations imposed by national and regional legislation or organizational policies
- the context in which the data are being managed, e.g. security, access and logistical conditions plus political dynamics with local and national authorities (including the estimated surveillance and interception capabilities of the parties to a conflict or other violence).

Appropriate measures must be applied at each step of the data and information management process. If an appropriate level of data security cannot be guaranteed throughout, notably at the collection, storage and sharing stages, the protection actor should consider different approaches.

It is recommended to refer to internal policies, guidelines and best practices to ensure compliance with data security obligations, which often vary between data types depending on confidentiality and sensitivity classifications.

Data security measures should be routinely reviewed and upgraded as needed to ensure a level of data security that is appropriate to the sensitivity and confidentiality of the protection data. If security problems arise, perhaps because of a change in the operational environment, it may be necessary to destroy the data if it is not possible to mitigate the risks to data security.

Response to personal data breaches

Protection actors must pay special attention to the security of personal data, as a data incident involving such data can have serious consequences for affected people and legal consequences under data protection law. Any such incident must be reviewed to see whether it constitutes a data breach.

A *personal data breach* is the unauthorized modification, copying, unlawful destruction, accidental loss, improper disclosure or undue transfer of or tampering with personal data. There are three commonly recognized types of data breach:

- *Confidentiality breach* – unauthorized or accidental disclosure of or access to personal data.
- *Integrity breach* – unauthorized or accidental alteration of personal data.
- *Availability breach* – unauthorized or accidental loss of access to or destruction of personal data.

Given the increasing role of personal data, its significance, its value and the scope for misuse, it is more a matter of “when” a personal data breach will occur, rather than “if”.

The most common reasons for data breaches include:

- weak data security measures
- loss or theft of devices containing personal data
- human error
- phishing, malware
- ransomware attacks
- lack of training
- physical breaches.

Protection actors must know how to respond to a breach and must establish a procedure for doing so. The steps below focus on ensuring compliance with data protection requirements. Security, political or reputational issues may require additional consideration.

1. **Identify and contain the breach:** Report breaches immediately to relevant departments and take swift containment measures, such as disabling access, changing passwords or isolating affected servers. Staff in all roles and at all levels must report any breaches of which they become aware.
2. **Investigate the breach:** Collaborate with relevant departments to investigate the nature, scope and timeline of the breach. Gather evidence, identify affected people and pinpoint the vulnerabilities that led to the breach.
3. **Assess the risk and impact:** Evaluate the severity of the breach in terms of the sensitivity of the data concerned, the people affected and the potential consequences. Assess risks to people (such as violation of their human rights, identity theft or retribution) and consider possible damage to the reputation of the organization.
4. **Notify the relevant parties:** Notification obligations will depend on such factors as the applicable law. Some laws or regulations may require notification of a supervisory authority and/or the people affected. However, even where no such requirements exist, one should still consider notifying the people affected of any breach that poses a significant risk. Communicate the details of the breach and actions taken clearly and promptly, to maintain the trust and confidence of affected people and, where applicable, of national authorities and governments, donors, partners and the public.
5. **Implement mitigation measures and preventive action:** Propose technical and organizational solutions to prevent future breaches. Offer additional training or limit data access if human error contributed to the breach.
6. **Monitor, evaluate and learn:** Establish a monitoring mechanism to track the effectiveness of the measures implemented and to address any issues promptly as they arise. Update standard operating procedures for breach management and registry of data breaches, together with other similar internal processes, to reflect lessons learned.

CONFIDENTIALITY



7.6 Protection data and information must be managed in a manner that ensures an appropriate degree of confidentiality for as long as data are retained.

Protection actors must ensure the confidentiality of protection data by implementing organizational safeguards and procedures to keep data confidential for as long as they are retained, even after completion of the activity for which they were managed and for as long as disclosure of the data may cause harm. Confidentiality safeguards must be in line with organizational policies and legal requirements, taking into account the sensitivity level of the data and information in the response context.

- 6 The confidentiality of personal data must be maintained for as long as data are retained, even if the person concerned is no longer receiving services or assistance from the protection actor.

ASSESSING RISKS AND BENEFITS



7.7 At each step of managing and processing protection data, protection actors must assess the risks and benefits and maximize the benefits while preventing, reducing or mitigating potential adverse consequences for affected people and communities. Special consideration must be given to the identification, assessment and mitigation of risk connected with the processing of personal data.

Protection actors must take all feasible measures to reduce the risk⁸⁷ of harm to people from whom or about whom data are collected.

⁸⁷ Risks specific to the use of digital technologies and non-data-specific digital risks are addressed in Chapter 8.

This includes making every effort to prevent or mitigate harm to those people resulting from data security incidents such as unauthorized access to data, interception, misuse or mishandling of data (see Standard 7.5 in this chapter and Standard 8.3 in Chapter 8). At every step of the data and information management process, protection actors must regularly review the risks and benefits associated with their data management activities, with due consideration for the sensitivity level of the data and whether they are personal or non-personal. Any residual risk associated with the management of data should be proportionate to the purposes and to the intended protection outcome. Preserving the safety and dignity of the people involved (families, communities, etc.) must be a priority, in line with the principle of “do no harm”.

A data impact assessment (DIA) can be conducted to determine the expected impact of a data management activity and recommend action to mitigate any potential negative impacts,⁸⁸ while a data protection impact assessment (DPIA) must be used to assess personal data protection risks (see Section 2). A DIA must be conducted in the early stages of the process to guide the design of the data management activity, which must be redesigned, suspended or cancelled if its foreseeable risks outweigh its intended benefits despite prevention and mitigation measures, or if the expected risks materialize into harm that cannot be sufficiently mitigated. A protection actor using personal data or sensitive protection data from other sources, including open-source information, is accountable for the consequences of managing those data.

For example, the fact that first-hand accounts from survivors of sexual violence have appeared in a report provided to selected protection actors to support programming and advocacy for better services does not mean the report can be made available outside this group, e.g. to government entities or donors. Before making the report or any of its data available, protection actors must identify the risks and benefits, along with mitigation measures. The decision may be made, for example, to present a redacted version of the full report, to create a new public version or to further restrict circulation, bearing in mind the purpose and legitimate basis, and implementing technical or procedural safeguards to limit access if necessary.

The mere fact of having been in contact with a protection actor can sometimes be a source of risk. Before starting to collect data, protection actors must therefore identify the risks associated with the data collection methodologies and tools that will be used (such as face-to-face interviews, focus group discussions, interviews via phone or other remote technology), both for those providing data and information and for those collecting them. Such risks should always be compared with the expected benefits of having and using the data.

When analysing these risks and benefits, one must decide what constitutes “sensitive” data in a given context and how that sensitivity can materialize into risks at different steps of the data and information management process. For example, a key informant may be at risk if the interview is conducted in a public space (data collection step), while certain villages may be at risk if the data are disaggregated in a certain way in the report (dissemination and use step). Other threats may include interception, leakage and seizure of the data or the devices on which they have been collected

Understanding the risks and benefits for affected individuals, communities and staff at each stage of the data and information management process requires timely dialogue, especially with affected people. Data collection methods and tools should be piloted or otherwise tested prior to launch, to ensure all risks in the given operational context have been identified and the approach has been adjusted accordingly.

88 “Data impact assessment” is a generic term for various types of assessments and tools that aim to determine the potential positive and negative impacts of a data management activity. For details, see IASC, [Operational Guidance on Data Responsibility in Humanitarian Action](#), 2023.

Examples of measures that can or must be taken:

- conduct interviews in a safe and private place, shielded from public curiosity and where other people cannot exert pressure or intimidation of any kind
- use a data collection method that creates less exposure for people and staff
- tell people clearly why the data are being collected and how they will be used
- remove questions from the data collection tool or reformulate questions in a way that is more appropriate for the context and local sensitivities
- anonymize the data before disclosing them to other entities or using them
- take the data security measures that the sensitivity of the data requires, bearing in mind that even anonymous and non-personal data may be sensitive
- prepare internal and external versions of reports, with different data disaggregation and granularity
- contact informants, if agreed, to check that they have not suffered reprisals or been exposed to additional risks.

If a data collection method will jeopardize the safety and dignity of the people concerned and the risks cannot be mitigated to an acceptable level, protection actors should select more responsible methods and tools. They may also use proxy data and indicators to meet their information needs.

6 Data protection impact assessments

When personal data are being processed, a protection actor may need to conduct a DPIA,⁸⁹ which is a systematic evaluation process aimed at identifying, assessing and mitigating the risks associated with processing personal data. A DPIA is an essential tool for ensuring compliance with many data protection regulations. More importantly, it helps mitigate any risks to people's interests, rights and freedoms. As a general rule, a DPIA consists of four elements:

1. **Preliminary assessment:** Decide whether a process or project should go through a DPIA, by determining the likelihood of risk using a predefined set of criteria. The criteria should be adapted to the needs and specificity of each organization. The number of DPIAs will depend on such factors as the applicable law, the organization's profile and its risk appetite. A single assessment may address a set of similar processing operations, although this may depend on their complexity or other circumstances.
2. **Risk identification:** Identify potential risks and vulnerabilities associated with the processing of data by mapping data flows and analysing potential threats. At this stage, protection actors should try to answer the question "what can go wrong?". Depending on the protection actor's internal processes, a DPIA may be used to identify not only risks connected with the processing of personal data but also other risks that may exist.
3. **Risk assessment:** Evaluate the likelihood of each risk occurring and the severity of its consequences for people and for the organization, scoring and prioritizing these risks to determine which ones require immediate attention. The question to consider at the assessment stage is "how likely is the risk to occur, and how severe would its consequences be?". A simple three-level (low, medium, high) likelihood/severity matrix may help determine the level of risk.
4. **Risk mitigation:** Take technical, organizational and legal measures to reduce, control or eliminate the risks to an acceptable level. The mitigation stage requires protection actors to try to answer the question "how can we ensure the risk does not occur or that its impact is as limited as possible?".

Given the nature of personal data processing and other circumstances, it may not always be possible to mitigate risks to acceptable levels. Where this is the case, the protection actor will have to decide whether to accept the risks or not. It is also possible that modifying the process and implementing mitigating measures will create additional data protection risks.

⁸⁹ For details, see also ICRC, [Handbook on Data Protection in Humanitarian Action](#), Section 5.

Finally, the DPIA must be properly documented to ensure that its findings are applied and then continuously reviewed and regularly reassessed to capture developments and changes to the tool or process, plus any new data protection risks. Technology advances rapidly, bringing new ways of collecting, storing, analysing and processing data. This can create new risks, but it can also create new means of mitigating existing risks. Re-evaluating DPIAs enables organizations to identify and address potential gaps or vulnerabilities and ensure the relevance of data protection measures against a background of technological, political, legal and organizational change.

AVOIDING BIAS AND DISCRIMINATION

S

7.8 Protection actors must manage 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 disaggregate for age, gender and other factors of diversity.

Given the challenges inherent to humanitarian contexts, protection data may be incomplete, inaccurate, biased,⁹⁰ insufficiently disaggregated or otherwise low in quality. This may lead to incorrect analysis, which can lead to incorrect findings and recommendations, which in turn can lead to discrimination in the response, e.g. against under-represented individuals or groups.

Protection actors must be aware of the possible under- or over-representation of some categories of affected population in data management activities, owing to language barriers, political affiliation, power dynamics, educational level, access to means of communication and other factors.

Bias in data management may stem from respondents, intermediaries, or the protection actors themselves.

For example, in the design of their data collection activities, protection actors may select methods that over-emphasize information or knowledge provided by men, if women are less visible in public life and more difficult to access. Choosing data collection methods that are less accessible for women results in not engaging sufficiently with women or with a sufficient number of women, and risks biasing both the analysis and the recommendations.

Certain segments of the population may be under-represented because protection actors cannot access certain locations or types of area.

Bias may result from communication barriers between the protection actor and the informant, such as female interviewees being reluctant to give certain information to male interviewers, or prejudice and assumptions on the part of the interviewer.

Protection actors must take all reasonable measures to avoid replicating the dynamics of social exclusion that already exist in a context and to prevent and mitigate possible biases that may result in unintentional discrimination. Even when bias does not amount to discrimination, it impedes accurate understanding of the situation and distorts the decisions taken, including the protection response.

The principle of non-discrimination⁹¹ requires protection actors to identify discrimination in any situation they are trying to address. To do this, they must collect data that can be disaggregated by such characteristics as age, gender, sexual orientation, rural/urban, ethnicity, nationality, affiliation, country of origin and socio-economic status, plus other factors such as time and location. The appropriate characteristics for disaggregation will depend on the purposes for which the data are to be used, the operational context, the sensitivity of the data, etc.

⁹⁰ “Bias” may be defined as any systematic distortion of information, whether intentional or not. Understanding the potential for bias in data management is the starting point for avoiding it and minimizing or mitigating its effects. For more information on bias, see Standards 2.2 and 2.3. See also ACAPS, [Technical Brief on Cognitive Bias](#), 2016.

⁹¹ See Standard 2.2.

TRANSPARENCY

S

7.9 People must receive timely, clear and concise information regarding the management of protection data and information and the processing of personal data. That information must include who processes personal data, for what purpose, on what basis and for how long, together with details regarding data sharing and data subject rights.

Organizations must manage data in ways that offer meaningful transparency towards protection actors and stakeholders, particularly affected populations. This includes providing timely and accurate information about the data management activity such as its purpose(s), the intended use(s) of the data and how they will be shared, plus any associated limitations and risks.

Before starting to gather protection data and information, protection actors must determine the level of reliability and accuracy that will be required to meet their defined purposes, and how often the data and information would need to be updated.

Any report – internal or external – should be clear about the reliability and accuracy of its data and information. A report can include incidents that have not yet been verified or confirmed, as long as it indicates the status of the incidents (e.g. alleged versus verified) and the limitations that should be considered when using the report to guide decisions. This does not necessarily mean providing details about individual experiences or situations; protection actors should always respect confidentiality and avoid publishing sensitive data that may do harm. However, they must provide information about data and information collection methods, as appropriate given the nature of the report and its intended audience and use, and must record full details in internal documents.

Protection data and information must be:

- as detailed (i.e. granular and disaggregated) as required for the defined purposes
- updated at a frequency appropriate to those purposes
- corroborated (triangulated) using multiple (primary and secondary) sources as appropriate.⁹²

See Standard 7.2 regarding the concept of clearly defined, specific purposes.

A classification system may be created to identify and tag different levels of data and information reliability. For instance, a secondary source report that has not yet been cross-checked, 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 information on the ground can be costly, take time, create risks for everyone involved or be impossible (for example owing to access constraints). Using open-source information (OSI) and other means or technologies in a responsible and intentional way to remotely collect and compile data can be useful where physical presence is impossible or restricted. When an organization is present on the ground or has a network of trusted and reliable sources, OSI can help corroborate data collected by other means. In most cases, the information needs of protection actors are met by combining primary and secondary data.

When gaps in the quality of the data and information affect the protection response (e.g. owing to limited reliability, accuracy, completeness or timeliness), protection actors should take the necessary remedial action.

⁹² It is essential that the protection actor not commit a data breach by disclosing personal data when corroborating data.

This may include

- undertaking a more extensive desk review to identify usable secondary data
- redesigning collection methods and/or tools
- combining multiple methods/tools
- establishing categories to systematize the data
- clarifying terms in glossaries
- providing coaching and training on fact-finding, interviewing and information collection (see the PIM process above, which emphasizes the importance of deliberately designing and later evaluating the data collection system and methods, the risks involved and the protection impact).

- 🔒 Fair and transparent processing of personal data is based on the principle of transparency,⁹³ which requires that at least a minimum amount of information concerning the processing of a person's data be provided to them at the moment of 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. See the box above regarding consent for guidance on the information to be provided.

COORDINATION AND COLLABORATION

S

7.10 Protection actors must refrain from duplicating the collection of protection data and information, to avoid unnecessary burdens and risks for affected people and communities.

Protection actors must minimize duplicative data collection that creates or exacerbates burdens and risks for affected people.

They must:

- assess whether the data and information they require for their defined purposes are already available (e.g. by conducting a desk review)
- coordinate their data collection and analysis with actors inside and outside the humanitarian sector (e.g. through forums such as the protection cluster or more informal groups)
- consider harmonizing and coordinating their data collection with other actors (e.g. through joint multi-sectoral needs assessments).

Data collection must be complementary, enhancing the scale and quality of the evidence base available to actors involved in the response.

Protection actors must be aware of which data can be disclosed, for which purposes, to whom and how.⁹⁴

Coordinating and collaborating can help avoid repeatedly asking people the same questions. This is particularly important when they are survivors of violations or abuse. Repetitive questioning may traumatize or re-traumatize respondents. The protection actor must be sensitive to such risks and must ensure that the person receives psychological or psychosocial support both during and after the interview (see also Chapter 5, Guideline 5.5, which provides further information on referral pathways).

⁹³ See ICRC, [Handbook on Data Protection in Humanitarian Action](#), 2024, Section 16.3.2.3.

⁹⁴ See Standard 7.11 on sharing data.

Protection actors must comply with the “do no harm” principle⁹⁵ when balancing the need for information (to develop, adjust or report on the response) and the need to minimize the burden on and risks to the people providing that information. Protection actors must maximize the benefits and minimize the risks of data management in humanitarian action. Working effectively with affected populations, other protection actors and peace and development actors will help to achieve this.

DATA SHARING AND TRANSFER

S

7.11 Protection data and information may only be transferred to or shared with those recipients who require access to fulfil the clearly defined, specific and legitimate purposes for which the data are managed and who can guarantee the required level of data security and, where required, data protection.

Protection actors increasingly work in partnership and seek to ensure complementarity with other sectors, while avoiding duplication (see Chapter 5 on complementarity). Protection data and information should be shared according to its classification, nature and level of sensitivity. The benefits of sharing data and information must be balanced against the need to protect people’s privacy, well-being and security, and the “do no harm” principle. Protection actors may transfer or share protection data and information only if doing so serves a protection purpose and there is a legitimate basis for doing so.⁹⁶ The protection data and information must be shared and transferred in a safe, ethical and effective manner. Protection actors should take appropriate security measures including encryption, access restrictions and physical measures to protect against interception and unauthorized access and use (See Standard 7.5).

Protection actors should contribute to information sharing protocols (ISPs) at the response level and take ISPs into account when sharing protection data. When sharing highly sensitive or strictly confidential data or information, protection actors should establish data sharing agreements (DSAs) that set out the terms and conditions governing the sharing of specific data and information between two or more parties. These agreements are essential to upholding legal, policy and/or normative requirements related to the sharing of sensitive non-personal protection data. DSAs are a necessary safeguard for sharing personal data.

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

- Prioritize protection outcomes and the safety and well-being of the people or populations concerned.
- Be open about the data management activity, and the accuracy and reliability of the data and/or information provided, to minimize the risk of presenting an incorrect or incomplete assessment of the issues they intend to address (see Standard 7.9).
- Consider the sensitivity of the data and information in the context and the potential risks they may create for individuals and/or communities. This is usually achieved at the response level through the data and information sensitivity classification included in ISPs.⁹⁷ When sharing aggregate or statistical data, consider whether there is any risk that individuals and communities will be re-identified from the sample, alone or in combination with other data and information (the “mosaic effect”) and be adversely affected as a consequence.
- Undertake a DIA to determine the expected impact of sharing data, and make recommendations for mitigating any potential negative impact.
- Undertake a DPIA before sharing any personal data – see Standard 7.11.

Sharing data in line with ISPs where available, and establishing DSAs where needed, helps ensure that the purpose of sharing is well defined, sensitive data have been classified and the necessary safeguards have been set up to ensure that the transfer, reception and storage of the data are secure.

⁹⁵ Standards 2.4. and 2.5.

⁹⁶ See Standards 7.1, 7.14 and 7.17.

⁹⁷ For guidance on sensitivity classifications and ISPs, see IASC, [Operational Guidance on Data Responsibility in Humanitarian Action](#), 2023.

- 6 The sharing and transfer⁹⁸ of personal data among protection actors and with other third parties (including across borders), are routine operational requirements in protection and are essential to the provision of effective, timely and collaborative protection. Most national data protection laws restrict the sharing of personal data with third parties, in particular across national borders. Some national legislation even restricts the transfer 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.⁹⁹

Protection actors must take the following steps when transferring personal data internationally:¹⁰⁰

- Comply with data protection rules and privacy requirements (including local legal requirements regarding data protection and privacy¹⁰¹) prior to the transfer.
- Conduct a risk assessment such as a DPIA (see Standard 7.7) prior to the transfer, to confirm that it does not present unacceptable risks for the person or people concerned. Document the circumstances of the transfer, the laws in the country of destination and the additional safeguards put in place to protect the personal data.¹⁰²
- Strictly limit the quantity and types of personal data transferred and ensure that processing by the recipient is restricted to the specific purposes as far as possible.
- As the protection actor initiating the transfer, be able to demonstrate that adequate measures have been taken to ensure compliance by the recipient entity with the principles of data protection (as outlined in these Standards).
- Ensure that the transfer is not incompatible with the data subject's reasonable expectations.
- Inform the data subject as to the intended recipient(s) of the transfer and give them the opportunity to either consent or object to the transfer.
- Confirm or verify that there is a lawful basis for the transfer. The most common lawful bases are:
 - the vital interests of data subjects or other people
 - important grounds of public interest, based on the controller's mandate
 - the legitimate interest of the controller
 - consent of the data subject.

Sharing personal data is a form of data processing and therefore requires compliance with all the standards listed in this chapter.

As there is a very high risk of harm if personal data are mismanaged, protection actors must ensure that data are transferred or disclosed only to those entities that offer the required level of data security and protection. They must also ensure that the actual transfer uses the safest means possible, applying security measures such as encryption where needed.

Protection actors must also ensure that the sharing of personal data does not compromise the identity or character – humanitarian or human rights – 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 people they are protecting and assisting.

⁹⁸ 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 digital or electronic means.

⁹⁹ For further guidance on the conditions for international data sharing, see ICRC, [Handbook on Data Protection in Humanitarian Action](#), 2024, Chapter 4.

¹⁰⁰ For examples, see ICRC, [ICRC Rules on Personal Data Protection](#), 2020, Chapter 4.

¹⁰¹ Many countries have enacted data protection laws that regulate the international transfer of personal data. Staff should consult their legal and/or data protection department to find out whether any national and/or regional laws apply to the transfer.

¹⁰² This assessment is often referred to as a “transfer impact assessment”. It is described in more detail in [EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data](#).

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


ACCOUNTABILITY



7.12 Protection actors must be accountable for their management of protection data and information. They must be able to demonstrate that personal data are processed in line with data protection principles and that adequate and proportionate measures have been put in place.

This accountability can be implemented in a variety of ways, including formal policies, guidance or procedures with clear roles and responsibilities, and monitoring and supervisory mechanisms. Accountability is also enabled by ensuring that sufficient and appropriate resources are available, including financial, human and technological. Protection actors must ensure that staff are capable of understanding and implementing their accountabilities, especially when they interact with affected people and communities.

Protection actors will not only collect data but also re-use data from existing sources, including open sources. They must assess the reliability of the source (notably the organization's or individual's areas of expertise and known biases) and the quality of the data, as these will determine whether the data can be responsibly re-used for the intended purpose. Protection actors are accountable for how they re-use data, and for any errors or biases that may be introduced into the analysis and the associated findings and recommendations. Affected people should be involved throughout the data management process, including the management of open-source data.

-  Where protection actors process personal data, the principle of accountability¹⁰³ is premised on the responsibility of protection actors to comply with data protection law and the standards set out in this section. A protection actor must be able to demonstrate that their organization has taken adequate and proportionate measures to prevent the harm that may result from non-compliant processing or from security incidents.

These measures may include:

- internal policies
- guidelines and instructions
- standard operating procedures
- supervisory structures
- training
- monitoring mechanisms including data protection controls and metrics and carrying out and documenting DPIAs.

Accountability mechanisms may also include internal data protection policies, codes of conduct, certification schemes, records of processing activities and disciplinary measures.

A protection actor is also accountable when it delegates processing of personal data to service providers, partners, private companies, research institutions or the communities themselves. The protection actor is responsible for ensuring that subcontractors apply the required standards at every step of personal data processing.

¹⁰³ See ICRC, [Handbook on Data Protection in Humanitarian Action](#), 2024, Section 2.9.

G

7.13 Protection actors should be accountable for their management of protection data and, where possible, provide feedback and information to affected people and communities about actions taken and results achieved.

People who have provided information on abuses and violations (including personal data) usually expect the protection actor gathering the information to take action on their behalf. This may include taking steps to ensure respect for the rights of the people whose data are processed.

Engaging with affected people and communities, communicating with them and providing them with feedback¹⁰⁴ enables them to participate and to be included, represented and empowered to exercise agency. It demonstrates respect for those who have provided information or will be included in the response, and builds trust.

Protection actors should have mechanisms through which they can see whether engagement with people (generally or in relation to data collection) is causing harm, e.g. in the form of repercussions and reprisals. Whenever such adverse consequences are reported, the protection actor should do its utmost to take corrective action in the specific case and identify preventive actions for the future. The protection actor should also incorporate the incidents into risk analyses and evaluate the need to revise preventive measures and procedures for managing data and information. Return visits, even if agreed with the respondent, may create risks because they draw further attention to the respondent's contact with a humanitarian or human rights actor.

SECTION 2 – ADDITIONAL STANDARDS FOR THE PROCESSING OF PERSONAL DATA

Personal data are the only category of data that is widely recognized and protected in international, regional or national law as a key component of ensuring respect for people's rights and freedoms. These regimes include clear rules and obligations regarding the processing of personal data. Although protection actors have obligations towards all protection data, they must give special consideration to personal data, i.e. data that allow individuals to be identified.

COMPLIANCE WITH LEGAL FRAMEWORKS

S

7.14 Protection actors must process personal data in accordance with the rules and principles of international, regional and national laws on data protection and/or organizational policy and guidance, as applicable.

- Ⓐ Personal data are the main legally recognized type of data. Understanding data protection requirements involves navigating a complex legal landscape influenced by the factors below.

Applicable law

Data protection laws safeguard personal data and regulate their use by organizations within a country's jurisdiction. These laws establish guidelines, frameworks and legal obligations for the processing of personal data throughout the data life-cycle (for example collection, storage and sharing). They ensure that people have control over their personal data, promote transparency in how personal data are processed and protect against unauthorized access or misuse.

¹⁰⁴ Accountability to affected people (AAP) is a collective approach that ensures the needs and interests of people are at the centre of humanitarian action. It is based on a commitment to take account of, give account to and be held to account by the people humanitarians seek to assist. For more detailed information, see OCHA, [Data Responsibility and Accountability to Affected People in Humanitarian Action](#), 2023.

The main data protection obligations stem from data protection law, but other legislation may influence protection activities and generate potential burdens or risks. There are various examples around the world of legislation to facilitate access by national investigators to electronic information held by service providers¹⁰⁵ or to prevent money laundering, financing of terrorism, fraud and other illegal activities.¹⁰⁶ When selecting service providers, protection actors should consider the likelihood of any such access to personal data and the severity of the consequences.

Organization policies and standards

An organization's policies and standards complement (or replace, if an organization enjoys privileges and immunities) external legal requirements and ensure robust data protection, security and responsible processing of protection data. Examples include data protection and privacy policies, retention policies, breach handling policies, bring-your-own-device policies, etc. These policies and standards may cover other types of protection data, in addition to personal data.

The applicable external and internal rules and regulations should be considered from the earliest stages of any process or project, limiting legal burdens and risks further down the line.

Just as protection work can cross borders, so too can data protection law and such laws may apply even though the humanitarian effort takes place somewhere the other side of the world, where seemingly no data protection law exists. This would be the case where the headquarters of a humanitarian actor are located in a country of which the laws apply regardless of the actual place of data processing.¹⁰⁷

Certain international organizations enjoy privileges and immunities, so they can perform the mandate attributed to them by the international community under international law in full independence and are not subject to the jurisdiction of the countries in which they work. Such organizations can process personal data according to their own policies and rules, subject to internal monitoring and relevant oversight and compliance systems.

MAIN ACTORS OF PERSONAL DATA PROCESSING

G

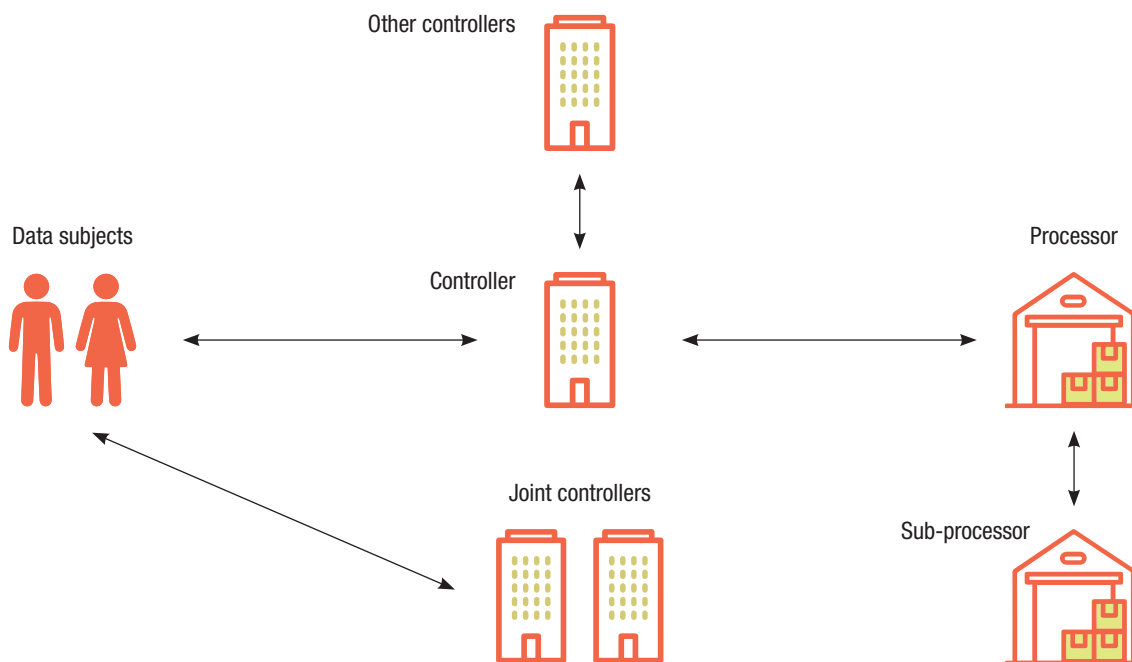
7.15 Protection actors should take account of the rules, regulations, roles and responsibilities of the actors involved in processing personal data.

- Ⓐ Processing personal data entails the existence of certain actors, with different roles and responsibilities.

¹⁰⁵ Examples include the US Cloud Act, the UK [Crime \(Overseas Production Orders\) Act](#), 2019 and the Australian [Telecommunications \(Interception and Access\) Act](#).

¹⁰⁶ Know Your Customer or KYC laws are designed to protect against fraud, corruption, money laundering and financing of terrorism, in an increasingly global economy. KYC processes require processing of personal data in order to: identify individuals, verify their identity, assess financial risks connected with particular individuals and enable monitoring, reporting, regulatory compliance and audit.

¹⁰⁷ Examples of such extra-territorial applicability include Article 3 of the GDPR, which states that "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."



Data subjects are the people whose personal data are processed by the controller. Data subjects can be categorized in accordance with various attributes or the purpose of processing, e.g. internal/external staff, partners or third parties and new/existing clients. In protection work, categories of data subject include:

- affected populations
- missing people
- forcibly displaced people (including refugees and internally displaced people)
- IDP or refugee returnees
- stateless people
- unaccompanied minors
- victims and survivors of sexual or gender-based violence.

These categorizations are not mutually exclusive and they depend on the purpose for which personal data are being processed. Given the sensitivities associated with protection work, respect for data protection is essential when processing the personal data of any of these categories of data subject, to avoid causing additional harm.

A controller is the natural or legal person or the entity that determines the purposes and means of processing personal data. As the main actor responsible for setting up the processing of personal data, the controller must comply with a number of requirements described in more detail in the next sections of this chapter. Should two or more controllers jointly decide on the purpose and means of processing personal data, they are called joint controllers. Usually, this cooperation requires a joint controllership agreement that explains the roles and responsibilities of each controller, to avoid impinging on people's rights and freedoms.

Depending on various factors such as the purpose and legal basis for processing, personal data often flow between various controllers ("other controllers"). In this case, however, these other controllers have full independence in deciding on the purpose and means of processing personal data, unlike in the case of joint controllership. Disclosing personal data to any other controller should be governed by a DSA that covers in particular the purpose, scope of data and lawful basis for such disclosure.

If a controller arranges for another entity to process personal data on their behalf, that entity is termed a processor. Depending on the nature of the processing, multiple processors may assist a single controller. They will have little or no power of decision regarding the key aspects of how personal data are processed. The parties should draw up a data processing agreement (DPA) to clarify the processor's role and the purpose of the processing.

DATA PROTECTION BY DESIGN AND DEFAULT

S

7.16 Data protection must be integrated in the design and development of protection data and information management systems and tools from the outset, ensuring that privacy is a core property.

- Ⓐ A risk-based approach requires continuous estimation of the risks associated with the processing of personal data throughout the data life-cycle or PIM process (see Standard 7.7).

One such risk-based approach, data protection by design (often referred to as “privacy by design”), ensures that privacy and data protection principles are considered from the start of the design phase of any system, service, product or process. It requires technical and organizational measures and the integration of safeguards in processing, to ensure the protection of rights and compliance with legal requirements and/or internal policies and guidance. These measures and safeguards must be capable of achieving the intended purpose, which is to ensure compliance with data protection principles.

Data protection by design continues to undergo development, building upon the basic principles. Several organizations have created detailed resources in the area of data protection by design and by default. Guidelines on privacy-enhancing technologies for researchers and universities have also provided new ideas on how to approach privacy by design (see the list of reference material in Annex 3 to this chapter).

One approach involves technically enforced purpose limitation, where instead of concentrating on data minimization, the design ensures that only the identified purpose can be achieved through processing and nothing more. This methodology consists of the following steps, starting at the inception stage and continuing throughout the design phase:

1. Clearly identify and determine the purpose of processing.
2. Avoid broad purposes and do not design solutions for multiple purposes.
3. Add technical measures that limit any purpose creep, such as ensuring that the personal data collected can only be used for the specified purpose.
4. Assess and mitigate the risks of the initial design.
5. Use custom-built solutions that allow for the incorporation of privacy-enhancing technologies.

With this approach, data minimization should emerge naturally. However, before implementing data protection by design, protection actors must identify what privacy actually means for their data subjects. In certain cases, for instance, privacy is interchangeable with confidentiality. In such cases, protection actors should concentrate on minimizing the disclosure of personal data and enhancing data security. In other cases, privacy can mean user agency and users having control over their data. Protection actors that integrate accountability, transparency and user participation in their processing enable data subjects to more fully exercise their rights and enhance trust between protection actors and communities.

DATA SUBJECT RIGHTS

S

- Ⓐ **7.17** Protection actors must take action to respect and promote the ability of people whose personal data are processed to exercise their rights as data subjects.

Personal data should not be processed in silos, without informing or involving the people whose data are being processed. Data protection legislation aims to ensure this involvement through data subject rights. These rights empower people to exercise their rights and agency over how their personal data are processed and ensure fair, open and honest processing. For a description of the right to information, please see the section on “transparent” processing in Standard 7.9.

Staff responding to data subject requests should ask the following questions:

- Does the request concern the requester's personal data?
- Does the request relate to the requester (or the person on whose behalf the authorized person makes the request)?
- Has the person's identity been verified?
- What right is the requester trying to exercise?

Data subject rights

Individuals must be able to exercise these rights using the internal procedures of the organization, such as by lodging an enquiry or complaint with the relevant staff or office. Any request from data subjects should be handled without delay, although applicable laws may specify the timeframe required. As described in the *Handbook on Data Protection in Humanitarian Action*,¹⁰⁸ these rights include:

Right of access: People have a right to access any of their personal data that an organization holds, and to obtain information about how it is processed. A copy of a person's personal data must be made available to them on request.

To what data or categories of data is the requester seeking access?

Understanding the scope of the request makes it easier to locate and retrieve the relevant data efficiently. People can submit a request without specifying the scope of data or else can request access to a specific scope of information. In complex cases where a protection actor processes vast amounts of personal data, often for multiple purposes, it is possible to ask the requester to further specify the information or processing activities their request relates to before responding to the request.

Does the request involve information about other people?

Protection actors should evaluate whether they can fulfil the request without revealing details that identify another person. If this is not achievable, there is no obligation to fulfil the request unless the other person agrees to disclosure or it is legitimate to do so without their consent (see Standard 7.1 and text box on consent).

Right to object: People have the right to object to the processing of their personal data when the processing is based on legitimate interest or public interest.

To what processing activities is the person objecting?

Understanding the objection helps in assessing its validity and determining the necessary action. As this right is closely tied to the lawful basis of processing, it might not apply where the lawful basis is consent. However, if the LIA (see Standard 7.1) has determined that legitimate interest is the appropriate lawful basis for processing, people must be able to submit an objection.

Do the person's rights and freedoms override the legitimate reasons for processing?

When a person exercises their right to object, a protection actor will need to balance the interests of both parties. The LIA should be revisited.

¹⁰⁸ For further information, please see ICRC, [Handbook on Data Protection in Humanitarian Action](#), 2024, Section 2.11.

Right to correct: People have a right to rectify any inaccurate or incomplete personal data held by an organization. Whenever possible, organizations must ensure that personal data are accurate and up to date, as described in the data quality principle (see Standard 7.3).

Should proof of inaccuracy be requested?

Depending on the nature of the correction request, it may be necessary to request proof of inaccuracy, especially if the request relates to the humanitarian organization's findings or records or other sensitive information which, if corrected, may affect the affected person's situation.

Right to have data deleted, also known as the "right to be forgotten". A person can request the deletion or removal of their personal data if one or more of the following apply:

- they are no longer necessary
- the person withdraws consent or objects to the processing and there is no lawful basis to continue processing
- the processing does not comply with the applicable data protection and privacy laws.

Does the right to erasure always apply?

As described above, a deletion request will only apply in certain situations. If the criteria are not met, the personal data will not be deleted.

Are there any circumstances supporting a limitation or restriction to this right?

In view of the consequences of deletion, the protection actor can limit or restrict the right of deletion until they have obtained clarification, e.g. if they are concerned that the person is requesting deletion because of external pressure and that deleting personal data would harm that person's interests and/or those of another person.

ANNEXES TO CHAPTER 7

ANNEX 1: THE DATA-RELATED RISKS AND BENEFITS OF VARIOUS PROCESSES AND TECHNOLOGIES

Internet and mobile phones

In their daily work, protection actors rely on multiple communication channels, including formal and informal, official and unofficial and direct and indirect means of exchanging information.

They use these communication channels for such activities as:

- collecting information via surveys and questionnaires
- communicating with staff and affected people
- issuing notifications regarding dangerous areas
- disseminating information on humanitarian corridors and how to access them
- passing messages between detainees and their families.

The use of internet or mobile phone networks is often essential for the protection activity, both to receive and share information.

Nevertheless, humanitarian workers need to consider the individual and collective risks inherent to the various channels. Such an assessment can enable them to choose the means of communication most appropriate and feasible for their purposes and in their context:

- SMS messages can be intercepted, manipulated and replayed by malicious actors.
- SMS messages are rarely encrypted and if they are, inexpensive equipment can crack the encryption.
- SIM cards are uniquely identifiable by the network provider.
- Malicious entities can impersonate legitimate networks (pre-5G).
- Modern messaging channels rarely encrypt the metadata, i.e. the data related to the message (sender, receiver, time of delivery, etc.). This data can reveal a lot of information about the communication with little effort.
- Internet service providers and network operators often keep past traffic and metadata in the form of logs, etc. Authorities may (legally or otherwise) request access to information on protection actors or beneficiaries.

Messaging apps

Messaging apps have become an integral part of communication in protection work, providing protection actors with real-time communication and efficient and immediate means of exchanging information with the affected population and other protection actors. The features of messaging include person-to-person communication, group chats, video conferencing, live streaming and image/file sharing. However, like any communication method, messaging apps come with their own set of risks.

These include:

- Limited encryption: Messaging apps, especially SMS, may lack robust encryption, making them vulnerable to unauthorized access or manipulation.
- Metadata exposure: Even where a messaging app provides end-to-end encryption of messages and calls, such encryption will not usually extend to metadata, and those metadata will reveal details such as sender, receiver and delivery time. Enough metadata can tell interested parties as much as the encrypted message itself or more, with minimal effort.
- Storage of data: While some apps store data on the user's device, others use cloud storage. Without encryption, the information will be available to anyone accessing that storage.
- App access rights: Different apps require different access rights to operate. Messaging apps will often ask not only for access to contacts, but also to SMS/MMS, the phone's storage or even its camera or microphone. This may lead to unwanted disclosure of information stored on the phone or of words spoken nearby.
- Phishing attacks: Users are vulnerable to phishing attacks in the form of malicious links or messages that appear to be from trusted contacts. These can also compromise the information stored on the device.

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.

Benefits of such technology include:

- Enhanced understanding: Provides insights about the situation on the ground, facilitating evidence-informed decision-making.
- Verification and evidence: Offers photographic proof that can corroborate survivor or witness statements regarding incidents or violations, promoting accountability.
- Protection assessment: Aids in assessing the scope of protection needs, identifying trends in forcible displacement and estimating damage to civilian infrastructure and housing.
- Identification and documentation: Can corroborate alleged mass graves, detention centres, etc. and contribute to transparency and accountability.
- Chronological insight: Sequenced, time-stamped imagery can help create an event timeline, which is invaluable for establishing a chronological record of incidents and identifying the actors involved.

- **Reliability:** Satellite imagery is an objective representation of ground realities and is less likely to be affected by misinformation/disinformation, manipulation, etc. as long as the necessary security measures and other safeguards are applied.
- **Access:** Satellite imagery can be gathered remotely, helping protection actors overcome barriers to access in operational contexts.

However, protection actors should be aware of data protection risks:

- **Targeting:** During violence or armed conflict, misuse of this imagery can lead to the targeting of populations and/or locations, putting them at risk.
- **Privacy concerns:** The collection and sharing of such imagery may intrude on individual privacy, particularly if individuals are identifiable in the images or through other factors that allow for identification (e.g. detailed land markers, vehicle or ship markings).

Although the nature and severity of the risks may greatly depend on the purpose and the technology used, a DPIA is recommended, to ensure that the rights and freedoms of individuals are safeguarded.

Photographs and other visual data

Visual data include photographs, video footage and other recognizable visual representations of individuals (e.g. courtroom sketches). When they collect visual data, protection actors are responsible for assessing and managing the risks to the individuals and communities portrayed in or identifiable from them and must process them in line with the standards presented here.

Visual data are particularly compelling and may have several advantages for protection work:

- enhanced storytelling, which can in turn enhance advocacy and resource mobilization
- increased engagement
- improved decision-making and response efforts
- enhanced transparency and accountability
- empowerment of affected communities

However, visual data that include people will most likely entail processing of personal data and may pose certain data protection risks:

- **Lawful basis:** It can often be difficult to ensure that the consent people give in an emergency situation is informed and freely given, and other lawful bases might not apply in such cases.
- **Further processing:** Visual data can be stored indefinitely and be re-used for purposes other than the original purpose without the appropriate lawful basis and without the person's knowledge.
- **Metadata:** If metadata are not disabled, the metadata of images may reveal the exact coordinates of the location at which they were acquired.
- **Misuse and exploitation:** Visual data can be exploited for various purposes, including propaganda, misinformation and commercial gain, jeopardizing the safety and well-being of those depicted.
- **Security threats:** The use of visual data may inadvertently expose individuals to security risks, particularly in areas with political unrest or conflict.

Stock images used for protection purposes should be treated with the same due diligence, and the same safeguards must be applied. Furthermore, protection actors should develop internal communication and media guidelines on ethical and safety standards and should foster a culture of responsible data use among humanitarian and human rights actors.

Open-source information analysis

OSI analysis is the process of collecting and analysing data gathered from open sources in order to produce actionable information.¹⁰⁹ Open-source information, as the name implies, is information that is publicly available. OSI can include articles, news sites or blog posts, published in print or digitally and intended and made available for everyone to access.

Anything a user publishes via social networking, including images, may be considered open-source. It is not always obvious whether information on social media is open-source, but it is generally considered publicly available when it is accessible not only to the user's personal contacts, but also to people or organizations who are not logged in to the particular social media platform or are logged in but are not one of the user's contacts.

Although this may vary, depending on applicable law, data protection rules apply to information gathered as part of OSI activities. This is sometimes referred to as a "privacy paradox" – the fact that data are publicly available does not mean they are not protected.¹¹⁰

The benefits of using OSI include the following:

- Quantity and availability: OSI allows protection actors to gather information from a wide range of open sources.
- Access: OSI can be gathered remotely, helping protection actors overcome barriers to access in operational contexts.
- Timeliness: OSI can provide real-time information, allowing protection actors to respond quickly to changing situations.
- Cost-effective: OSI may be more cost-effective than other methods of data collection.
- Multi-source verification: OSI allows for data triangulation by cross-referencing information from multiple sources. This verification process can enhance the reliability and accuracy of the information collected.
- Increased situational awareness: OSI can give protection actors better situational awareness, together with insights into the needs, challenges and potential risks of a given population in a specific area, allowing them to tailor their response accordingly.

However, OSI may involve data protection risks:

- Lawfulness of processing: Organizations conducting OSI must identify the correct lawful basis for such activities. As described in Section 1 of this chapter, consent will often not be the best option owing to the high threshold of it being *freely given* and *informed*. Instead, depending on the purpose of OSI activities, humanitarian actors may decide to rely on vital interest, public interest or legitimate interest. An LIA may be required if legitimate interest is claimed.
- Transparency: By the very nature of OSI, people may be unaware of such processing and may hence be unable to exercise their rights.
- Data quality: Open sources can contain unreliable data, misinformation, rumours or deliberately false reports.
- Data storage and preservation: The use of OSI can lead to the aggregation of a vast amount of information that may be difficult to store securely and preserve effectively.
- Data minimization: OSI activities may result in the collection of vast amounts of information concerning individuals, exceeding the scope necessary for the intended purposes. Such information can often include highly sensitive data.

¹⁰⁹ Outside the humanitarian sector, the terms open-source intelligence ("OSINT") and social media intelligence ("SOCMINT") are often used instead of OSI.

¹¹⁰ Leonore Ten Hulsen, [Open Sourcing from the Internet – The Protection of Privacy in Civilian Criminal Investigations Using OSINT \(Open-Source Intelligence\)](#), Amsterdam Law Forum, Vol. 12, 2020.

- Information overload: OSI activities can expose protection actors to a vast amount of information, potentially leading to information overload. Filtering these data for relevance and utility and then analysing them can be time-consuming. Moreover, exposure to large amounts of graphic content may harm staff health and well-being.
- Bias: There is a risk of unintentional bias creeping into the analysis process, which may affect decision-making. Bias in OSINT can be:
 - algorithmic – certain information may be over-represented in open sources
 - cognitive – the bias of the researcher may affect the analysis process.
- Data subject rights: Even though the information has been obtained from publicly available sources, individuals have data subject rights and may wish to exercise them, which may pose a challenge for the collecting organization.
- Mosaicking: By combining datasets, outside actors can de-anonymize information or reveal new – and potentially harmful – information through *mosaicking*.¹¹¹
- Data protection of the protection worker: Protection workers are exposed to risks concerning their personal data on social media and other platforms. There is the risk of doxing,¹¹² together with other risks that arise if an official account interacts with a public user or profile.

Organizations should carry out a DPIA beforehand to identify and mitigate the risks to the rights and freedoms of people connected with OSI activities.

Machine learning and AI

While there is no single, universally accepted definition of the term, machine learning (ML) can be understood as algorithms that learn from data. It is a subset of AI¹¹³ and aims to allow technology developers “to entrust a machine with complex tasks previously delegated to a human”.¹¹⁴ Feeding large amounts of data to the machine trains the algorithm to understand underlying relationships in the data and identify trends that would otherwise require a highly specialized human. Currently, most tasks given to AI systems consist of classifying data, predicting new data or generating data (as in the case of large language models and generative AIs).

At the time of this revision (2024), protection actors were still examining where and how machine learning and AI could be used responsibly in humanitarian contexts. Tasks that AI could perform to enhance the efficiency of protection and general humanitarian work include the following:

- Reconstruct a full body or facial image of a person based on their remains.
- Improve understanding and prediction of forced displacement.¹¹⁵
- Estimate population densities using satellite images.
- Predict natural disasters and the areas that will be most affected.
- Classify geographic locations as safe or affected by conflict/violence.
- Assist with medical diagnosis.
- Transcribe handwritten letters and video/audio files.
- Support decision-making (not automated decision-making) that requires the summarization of large quantities of data, with the necessary human autonomy and oversight.

¹¹¹ Jill Capotosto, [The mosaic effect: the revelation risks of combining humanitarian and social protection data](#), ICRC Humanitarian Law & Policy blog, 2021.

¹¹² An online practice of exposing personal information about others that had previously been kept private. Definition derived from Daniel Chandler and Rod Munday, [A Dictionary of Social Media](#), 2016.

¹¹³ Artificial intelligence is a system that can imitate cognitive functions such as problem-solving, inference, or insight. Additionally, machine learning studies patterns in data that data scientists later use to improve AI.

¹¹⁴ Council of Europe, [Artificial Intelligence Glossary](#).

¹¹⁵ The [UNHCR Jetson Project](#) is an example of such an initiative.

However, using AI to process personal data also involves risks:

- Processing on a large scale: Machine learning requires large amounts of data, which creates data protection and data security risks. As most AI and machine learning methodologies are centralized (although some can be federated or decentralized), cybercriminals may exploit vulnerabilities to gain access to large amounts of sensitive or personal data.
- Confidentiality of the model: Although models are tested under laboratory conditions, a trained model can leak sensitive, personal information. Querying the model may also reveal that a person was part of the dataset used to train and hence reveal that they had been in contact with protection actors.
- Lack of transparency and accountability: Currently, it is extremely difficult to understand the decision-making process of AI. This lack of understanding raises problems regarding the lawful basis for processing data. One can only use consent as the basis for processing if it is informed. Given the complexity of any AI tool, there is the risk that a person's consent cannot be deemed informed and hence that any activity relying on this technology may require a separate basis to comply with the principle of lawfulness.
- Bias: The model's outputs are only as good as the data with which it was provided. If that data is biased or incomplete, so too will be the outputs. For example, AI-based facial recognition may fail to recognize people of certain ethnicities or be more likely to mis-identify them, which could lead to discrimination.¹¹⁶
- Unsuitability for humanitarian work in general and protection work in particular: Protection data include many outliers (crisis environments, marginal populations, unique tracing requests, etc.) and most statistical algorithms try to eliminate outliers and find the most "normal" data items owing to the way they function. This means that responsibly applying ML and AI to humanitarian work may be difficult and that off-the-shelf solutions may never be fit for purpose.¹¹⁷

As AI and ML are increasingly used by the public sector, new risks may surface in the coming years. When using these technologies to process personal data, protection actors should therefore:

- minimize, aggregate and anonymize personal data as far as possible
- carry out a DPIA both before and during system and programme implementation, to identify high risks and take mitigating measures.

Processing of biometric data

Biometric data are personal data resulting from technical processing of the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. By their very nature, biometric data are sensitive personal data.¹¹⁸

Humanitarian organizations increasingly use biometric technology as part of their identity management systems because it can identify individuals and hence enable more effective assistance delivery and prevent fraud and misuse of humanitarian aid. Because they are generated and stored in digital form, biometric data are more difficult to counterfeit. They facilitate the effective management of humanitarian aid and are legitimately used for data analytics and other types of advanced data processing operations. In addition, by focusing on a person's unique features, biometrics can enable people to prove their identity who would otherwise be unable to do so (as may be the case for forcibly displaced people). This is a means of placing individual rights, dignity and agency at the heart of humanitarian action.¹¹⁹

Biometric processing is constantly changing, and new identifiers are emerging. Currently (2024), the technologies most often used in humanitarian work are automatic fingerprint recognition and iris scans. Fingerprints are the most frequently collected type of biometric data. Other forms of biometric data processing include palm vein recognition, voice recognition, facial recognition and behavioural characteristics.

¹¹⁶ OHCHR, [The Right to Privacy in the Digital Age](#), 2021.

¹¹⁷ See ICRC, [Handbook on Data Protection in Humanitarian Action](#), 2024.

¹¹⁸ *Ibid.*

¹¹⁹ *Ibid.*

Benefits include:

- reduced human error in identification
- combating of fraud and corruption
- identity authentication when other mechanisms are unavailable (e.g. some biometric traits continue to function post-mortem)
- enhanced speed and effectiveness of programming.

However, biometric data processing is not without serious risk:

- Data accuracy: The probabilistic nature of the biometric matching algorithm means that there is always a possibility of false matches and false acceptances.
- Inference of medical data: Biometric data can reveal medical data and are over-purposed by nature.¹²⁰
- Malicious use by others: Biometric data can be used to impersonate or track individuals.
- Unique link to the individual: A person's biometrics are unique and cannot be changed. This means that if they are lost or stolen they can never be used again owing to the risk of impersonation.
- Ethical issues: Cultural sensitivities, beneficiaries' perceptions and concerns about surveillance must be taken into account when deciding whether to collect biometrics and, if so, for which purposes and with which technology.¹²¹
- Function creep: A biometric system can be used for purposes other than those for which it was originally intended, including non-humanitarian purposes.
- Data disclosure: National or regional authorities may exert pressure to disclose biometric data.

Protection actors must therefore carefully assess the benefits of biometric data and the need to use them. They must explain clearly and openly how they intend to use these data in conformity with data protection requirements, ideally through public policies on the use of biometric data.

The *Policy on the Processing of Biometric Data by the ICRC*,¹²² adopted in 2019, is one such policy. It sets out the lawful basis for processing biometric data and contains a closed list of approved humanitarian purposes for which biometric data can legitimately be processed.

Given the highly sensitive nature of biometric data and the risks connected with processing them, humanitarian organizations should:

- apply data protection by design and default at the inception and design stage of the system, in particular to determine whether there are less intrusive ways of achieving the purpose and whether the collection of biometric data is proportionate to the intended use and purpose
- carry out a DPIA both before and during system and programme implementation, to identify high risks and take mitigation and prevention measures.

Digital ID

Every human being has an identity. The right to identity is undisputed and is recognized in international declarations and conventions.¹²³ However, since not everyone has an effective means of proving their identity, there is a growing need in humanitarian action for tools that provide a digital identity management system. While there is no single generally accepted definition of the term, Digital ID can be defined as “a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions”.¹²⁴

¹²⁰ Vincent Graf Narbel and Justinas Sukaitis, [Biometrics In Humanitarian Action: a Delicate Balance](#), ICRC Humanitarian Law & Policy blog, 2021.

¹²¹ Ben Hayes and Massimo Marelli, [Facilitating Innovation, Ensuring Protection: the ICRC Biometrics Policy](#), ICRC Humanitarian Law & Policy blog, 2019.

¹²² ICRC, [Policy on the Processing of Biometric Data by the ICRC](#), 2019. Other examples include Oxfam, [Oxfam Biometric & Foundational Identity Policy](#), 2021.

¹²³ See for example: *Universal Declaration of Human Rights*, Art. 6; *UN Convention on the Rights of the Child*, Art. 7.

¹²⁴ World Bank Group, [Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation](#), 2016, p. 11.

Digital ID offers several benefits, including:

- **Access to services:** Digital ID allows beneficiaries to easily access services, assistance or other protection activities without having to prove their legal identity. This eliminates the need to carry physical identification documents and allows for quick and convenient authentication.
- **Personalization of aid:** Digital ID systems that link digital identities to physical individuals enable organizations to provide targeted aid to individuals, such as health services. This helps ensure that aid is tailored to needs and improves the effectiveness of humanitarian programmes.
- **Interoperability:** Digital IDs can facilitate the exchange of information between different organizations, ensuring better coordination and collaboration in the humanitarian sector.
- **Use of innovative technologies:** Digital ID systems can use innovative technologies such as biometrics, blockchain and data analytics. These technologies can enhance the reliability and security of identity verification, promoting accuracy and efficiency.
- **Accountability and transparency:** Digital ID systems can provide a digital trail of identity verification and service provision, enhancing accountability and transparency. This can help prevent fraud, improve monitoring and evaluation and ensure efficient delivery of services.

Digital ID also poses data protection and other risks:

- **Function creep:** The use of identity systems for multiple humanitarian purposes could lead to the misuse of beneficiaries' data for purposes that were not originally intended.
- **Unauthorized access and surveillance:** Governments and non-state armed groups that do not respect human rights could access identification and other systems to identify enemies or opponents, potentially leading to discrimination, harm and human rights violations and abuses.
- **Exclusion:** Misuse of identification and profiling information may result in certain individuals or groups being excluded from essential services and aid. Digital ID systems may exclude individuals who lack the necessary digital literacy skills or access to technology.
- **Technological dependency:** Digital ID systems rely heavily on technology, including internet connectivity and reliable systems. Any disruptions or technical failures can hinder individuals' ability to access services or benefits.
- **Data breaches:** Despite encryption and secure storage, digital IDs are still vulnerable to cyber attacks and data breaches, putting personal data at risk.

In the light of the large-scale processing that digital identity systems involve and of other potential risks to data subjects arising from their use, humanitarian organizations should determine:

- what information is needed to implement a programme, including whether identification or authentication is needed
- the type of identity necessary.¹²⁵

This determination should be carried out in accordance with the principle of data protection by design and default. A DPIA should be carried out both before and during system and programme implementation, to correctly identify high risks and take mitigation and prevention measures. This is particularly important given that Digital ID may use technologies that pose their own data protection risks, e.g. the processing of biometric data, blockchain technology, data analytics and profiling, or wide data sharing.

¹²⁵ Examples may include: 1. Functional identity: enables a specific service (function) to authenticate participants; 2. Foundational identity: provides a legal identity issued by a trusted source to a broad population as a public good without specifying a specific service; 3. Conceptual identity: defines an individual's identity in relation to others within a given societal structure.

ANNEX 2: GLOSSARY

| TERM | DEFINITION |
|---|--|
| bias | Any systematic distortion of information, whether intentional or not. |
| biometric data | Personal data relating to the physical, physiological or behavioural characteristics of a natural person that result from technical processing, such as facial images or dactyloscopic data, and which allow or confirm the unique identification of that natural person. |
| data | Raw, unorganized facts or figures that are collected and stored. They can be in the form of numbers, text, images or other formats. On their own, data lack context and meaning. They are the most basic form of representation and need to be combined with other data and interpreted to become useful. |
| data and information management | The collection or receipt, storage, quality assurance, analysis, sharing, use, retention and destruction of data and information by humanitarian actors for operational response. |
| 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 data transmitted, stored or otherwise managed. |
| 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. |
| data impact assessment | Any of a variety of tools used to determine the potential positive and negative impacts of a data management activity. |
| data processor | The natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller. |
| data protection | <p>The process of protecting individuals' personal data that are collected, used, stored and shared or otherwise processed, including by humanitarian and human rights organizations.</p> <p>Protecting the personal data of individuals is an essential part of protecting their lives, physical and mental well-being and dignity.</p> |
| data protection impact assessment (DPIA) | A tool used prior to data processing, to identify and address all data protection risks, including by implementing risk mitigation measures. DPIAs are a requirement in many jurisdictions and in organizational policies and guidance. They are sometimes referred to as "privacy impact assessments". |
| data responsibility | The safe, ethical and effective management of personal and non-personal data for operational response, in accordance with established frameworks for personal data protection. ¹²⁶ |
| data security | A set of physical, technological and procedural measures that safeguard the confidentiality, integrity and availability of data and prevent their accidental or intentional, unlawful or otherwise unauthorized loss, destruction, alteration, acquisition or disclosure. |
| data subject | A person who can be identified, directly or indirectly, in particular by reference to personal data. |
| information | Data that have been given meaning as a result of being organized and analysed, and through relational connections. |
| lawful basis | <p>The legal justification for processing personal data.</p> <p>Personal data may be processed (collected, used, stored and transferred) only if there is a lawful basis for doing so (including consent, legitimate interest, vital interest, etc.; see under Standard 7.1.). Lawful bases may be specified in international, regional or domestic legal frameworks for data protection or in the organizational policies and guidance of humanitarian organizations.</p> |

¹²⁶ IASC, [Operational Guidance on Data Responsibility in Humanitarian Action](#), 2023.

| TERM | DEFINITION |
|--|--|
| metadata | <p>Data about data, or data that define or describe other data.</p> <p>Metadata provide additional information or documentation about the dataset that makes it easier for others to understand them and put them into context.¹²⁷</p> |
| personal data | <p>Any data relating to an identified or identifiable natural person.</p> <p>This may include an identifier such as a name, audio visual materials, an identification number, location data or an online identifier. Personal data may also be data linked specifically to the physical, physiological, genetic, mental, economic, cultural or social identity of a data subject.</p> <p>Depending on the applicable law or policies, the term may also include data identifying human remains or capable of doing so.</p> |
| processing of data (data processing) | <p>Any operation performed on personal data, such as collecting, analysing, using, sharing, storing, archiving or deleting them.</p> |
| protection data | <p>Data that protection actors manage in order to carry out their operations for and with communities affected by crisis, conflict or other violence. Before collecting or receiving data or before designing a protection data and information management system, protection actors must determine what data and information they require and for which purposes, together with their level of sensitivity. Data and information managed for protection outcomes should be considered protection data, regardless of whether they were initially collected specifically as protection data.</p> |
| protection information | <p>Information produced by making sense of protection data, analysing them and interpreting them in relation to the protection risks faced by people affected by crisis, conflict or other violence and affected people's capacities.</p> <p>It encompasses contextual elements and information crucial for the design and implementation of protection strategies and actions. Protection information serves as a foundation for evidence-based decision-making and for programmes to achieve evidence-based protection outcomes.</p> |
| sensitive personal data | <p>Personal data that might cause very serious harm to data subjects or other individuals if mishandled or disclosed (e.g. discrimination or repression).</p> <p>What constitutes sensitive personal data may be specified in international, regional or domestic legal frameworks for data protection or in organizational policies and guidance of humanitarian organizations. Examples of such sensitive personal data may include data that reveal racial or ethnic origin, political opinions, religious/philosophical beliefs, armed group affiliation, a data subject's sex life or their sexual orientation.</p> |
| sensitive protection data and information | <p>Protection data or information, the unauthorized access or disclosure of which is likely to cause harm (such as discrimination) to people such as the source of the information or other identifiable people or groups, or adversely affect an organization's capacity to carry out its activities or public perceptions of its character or activities.</p> <p>Certain data and information may be considered sensitive in one context but not in another. Both personal data and non-personal data can be sensitive.</p> |

¹²⁷ OCHA, [Centre for Humanitarian Data Glossary](#).

ANNEX 3: REFERENCE MATERIAL FOR CHAPTER 7

- AU, [African Union Convention on Cyber Security and Personal Data Protection](#), 2014
- COE, [Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data](#), 1981
- EDPB, [Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data](#), June 2021
- ENISA, [Data Protection Engineering](#), January 2022
- ENISA, [Promoting Data Protection by Design: Exploring Techniques](#), January 2022
- EU, [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 \(EU General Data Protection Regulation\)](#), OJ L119/1, 2016
- IASC, [Operational Guidance on Data Responsibility in Humanitarian Action](#), 2023
- ICRC, Engine Room and Block Party, [Humanitarian Futures for Messaging Apps](#), 2020
- ICRC, [Handbook on Data Protection in Humanitarian Action](#), 3rd edition, 2024
- ICRC, [Policy on the Processing of Biometric Data by the ICRC](#), 2019
- ICRC, [The ICRC and Data Protection](#)
- ICRC/Privacy International, [The Humanitarian Metadata Problem: “Doing No Harm” In The Digital Era](#), October 2018
- International Conference of Data Protection and Privacy Commissioners, [International Standards on the Protection of Personal Data and Privacy](#) (the “Madrid Resolution”), 2009
- NISO, [Understanding Metadata: What is Metadata and What is it For?: A Primer](#), 2017
- OCHA Centre for Humanitarian Data, [Guidance Note on Data Responsibility and Accountability to Affected People in Humanitarian Action](#), August 2023
- OECD, [Guidelines on the Protection of Privacy and Transborder Flows of Personal Data](#), 2013
- OHCHR, [The Right to Privacy in the Digital Age, Report of the UN High Commissioner for Human Rights](#), September 2021
- Oxfam, [Oxfam Biometric & Foundational Identity Policy](#), 2021
- Oxfam, [Responsible Data Management Training Pack](#), March 2017
- Oxfam, [Responsible Program Data Policy](#), August 2015
- PIM, [Framework for Data Sharing in Practice](#), May 2018
- PIM, [Principles, Matrix and Process – Quick Reference Flyer](#), March 2017

PIM, [Protection Information Management Common Terminology](#), April 2018

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

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

UN, [International Covenant on Civil and Political Rights](#), 1966

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, [Universal Declaration of Human Rights](#), 1948

UNHCR, [General Policy on Personal Data Protection and Privacy](#), 2022

UNHCR, [Policy on the Protection of Personal Data of Persons of Concern to UNHCR](#), 2015

UNHCR, [Using Social Media in Community-Based Protection: A Guide](#), 2021

WFP, [WFP Guide to Personal Data Protection and Privacy](#), 2016



8. A PROTECTION APPROACH TO DIGITAL RISK AND DIGITAL TECHNOLOGIES

Digital risks as protection risks

- S** 8.1 Protection actors must take all feasible measures to minimize risks that are enabled by digital technologies and might have consequences for the rights, safety and dignity of affected populations.

Respecting the principles of humanity, impartiality, and non-discrimination

- S** 8.2 Protection actors must ensure the principled delivery of protection action through digital tools and solutions.

Digital “do no harm”

- S** 8.3 Protection actors must avoid and mitigate the harm that could arise from the use of digital tools and solutions in their activities.

People-centric and inclusive digital technologies

- S** 8.4 The development and deployment of digital tools and solutions designed for protection action must be people-centric and inclusive.

Further ethical and operational implications

- G** 8.5 Protection actors should mitigate any negative impacts or ethical and operational implications of their choice, use of or dependency on digital technologies or providers.

Integrating digital risks in protection strategies

- G** 8.6 Protection actors should integrate digital risks and their harmful effects in their protection documentation and assessments. They should include and implement adequate responses and mitigating measures in their protection strategies.

Referring to and developing protective frameworks

- S** 8.7 Protection actors must be familiar with, uphold and respect the relevant principles and legal frameworks to ensure adequate protection for affected populations against digital risks. Where necessary and feasible, they should help develop a common understanding and guidelines to advocate for the protective application of these frameworks in contexts affected by armed conflict and violence.

Engaging in protection dialogue on digital risks

- S** 8.8 Protection actors must engage with relevant actors and establish protection dialogue on digital risks, related protection concerns and rights violations.

Strengthening affected people’s self-protection capacity and their resilience to digital risks

- G** 8.9 Protection actors should consistently build upon, support, promote and strengthen affected people’s capacity for self-protection and their resilience to digital risks.

Ensuring complementarity of protection action in the digital age

- G** 8.10 Where relevant, protection actors should cooperate with diverse expert stakeholders to complement their own actions to address digital risks.

Building preparedness of protection actors

- G** 8.11 Protection actors should ensure an adequate level of preparedness relating to digital risks, build and maintain awareness of these and provide sufficient capacity and expertise for response.

INTRODUCTION

DIGITAL REALITIES

Digital technologies are pivotal in how emergencies, armed conflict and other situations of violence (OSV) unfold and how protection actors respond to them. Protection organizations are increasingly leveraging the opportunities provided by digital technology to strengthen the effectiveness, efficiency, accountability and transparency of their protection work. However, these opportunities are accompanied by digital risks arising from the broader operating environment and digitalization.¹²⁸

States and private entities are seeking strategic advantages in digital technologies and their underlying components, such as machine learning software and electronic chips. States and other actors are attempting to use and control digital spaces and technologies, often under the remit of national security, border control or counter-terrorism, or in pursuit of economic and business interests.

The use of digital technologies in armed conflict and other crises foster digital-enabled protection risks – referred to as “digital risks” in this chapter. These risks can materialize into harm and impact the rights, safety and dignity of vulnerable or affected individuals. Digital technologies can be misused, diverted from their original purpose or fail, turning against the interests of crisis-affected populations or protection actors.

The emergence and prevalence of digital risks are tied to several trends that characterize the operating environment in crisis and humanitarian settings.

The digitalization of armed conflict and other situations of violence

Actors in armed conflict and other situations of violence use digital technologies as means and methods of warfare or for security purposes, causing, worsening or enabling significant harm. For instance, they increasingly resort to:

- cyber operations to disrupt critical infrastructure or protection actors
- information operations to influence conflict dynamics and gain information advantage in ways that amplify harmful or hateful narratives or affect people’s safety and well-being.
- denials of connectivity to limit flow of information, documentation and situational awareness
- data-intensive and (semi- or fully) automated systems to enable, support and direct the conduct of hostilities and law enforcement operations in ways that cause concerns with regards to their reliability, accuracy and transparency and discriminative potential.

The role and influence of tech companies in armed conflict and other situations of violence is also evolving: these actors may politically and technically support warring parties, their digital operations, defence and intelligence. They also hold a degree of ownership or influence over (digital) infrastructure and multilateral negotiations in ways that can influence armed conflict dynamics and their resolution. It is not clear how they can contribute to an environment conducive to better protection of civilians.

The connectedness of affected populations

During and after crises and armed conflict, affected populations increasingly use digital technologies, such as smartphones, social media and dedicated apps, to communicate, inform, self-protect and organize. However, their digital footprints on social media and elsewhere can be used to identify and target them. The same digital tools and solutions are also exacerbating armed conflict-related risks and facilitating civilian involvement in conflict and their exposure to harm, a trend that risks blurring the distinction between civilians and combatants. For instance, digital technologies allow civilians to partake – willingly or unwillingly; knowingly or unknowingly – in cyber operations against other civilian targets or to amplify misinformation, disinformation and hate speech on social media.

¹²⁸ For an overview of digital technologies in humanitarian settings, see OCHA, [From Digital Promise to Frontline Practice: New and Emerging Technologies in Humanitarian Action](#).

Connectivity is not only central to affected people's access to protection and assistance, but is also an enabler and sometimes a *de facto* requirement for full enjoyment of fundamental rights. However, despite advances in internet and telecommunication connectivity across the world, there are still underlying, structural inequalities in terms of access to, quality of and ability to fully enjoy the opportunities provided by connectivity – the digital divides. In certain contexts, these divides might be tied to lack of investment in telecommunication networks or to other structural circumstances, such as ID requirements, know-your-customer checks, insecure networks or data plans and energy affordability. Unequal access to connectivity, digital technology or (digital and media) literacy can exacerbate risks or intensify inequalities, discrimination and biases related to social, gender, ethnic, age and other factors of diversity.

The digital transformation of protection action

Protection actors are aiming to make the most of digital technologies; recent decades have seen the rapid digitalization and datafication of their operations and services.

Examples include:

- the use of AI-driven data analysis to improve projections and decision-making
- the use of mobile applications, chatbots, messaging apps and social media to complement face-to-face interactions with crisis-affected populations or improve access to information
- the use of digital tools to support the documentation of violations, including in the open-source environment.

The drivers behind this digital transformation include the need to:

- expand the reach to and access to affected populations
- optimize operational processes
- support cost-reduction¹²⁹ and traceability of resources deployed
- enable greater accountability and transparency (including with communities and donors).

These developments often involve a growing reliance on and partnerships with other actors, notably the private sector, to support the development, testing and use of these digital technologies.

However, depending on their context, design and implementation, digital-enabled protection activities may also harm or further marginalize affected populations. For instance, the deployment of artificial intelligence can lead to bias or discrimination, e.g. when it is based on unrepresentative, biased or incomplete training datasets.¹³⁰ Digital tools and solutions for protection activities can also malfunction, fail and sow mistrust.

A FRAMEWORK FOR PROTECTION IN THE DIGITAL SPACE

This chapter focuses on how protection actors should understand, conceptualize and address the protection risks that stem from these digital realities. A framework for protection in the digital space must address two core dimensions:

1. The use of digital technologies and the military use of civilian digital infrastructure by states and non-state actors can lead to harmful effects for people affected by armed conflict and violence. Digital technologies may bring affected people into closer proximity with conflict-related operations or result in targeting or persecution. This may also contribute to blurring the lines around applicable legal frameworks, potentially undermining the protection of civilians.

Protection workers must therefore further understand and integrate the resulting protection risks across their activities and strategies (see the first and second sections of this chapter, and Annex 2). Protection actors may also address the capacity of duty bearers to meet their obligations while achieving more effective, transversal, and impactful protection outcomes.

¹²⁹ There is little data or analysis available regarding the cost reductions that digitalization brings to humanitarian action.

¹³⁰ For more details, see Chapter 7, Standard 7.8 and Annex 1 on AI.

2. The development, integration and use of digital technologies by protection actors themselves, while providing opportunities to enhance the quality and effectiveness of their work, can also exacerbate risks and vulnerabilities and become vectors of harm.

Protection workers must therefore ensure a principled protection approach to digital technologies (see second and third sections of this chapter). They must ensure not only that they do not violate the rights of affected people when using digital technologies, or cause them harm, but also that they take effective prevention measures to ensure that they mitigate foreseeable negative impacts by third parties that their work could inadvertently facilitate. They must understand, manage and mitigate the risks, but also use strengthened and updated protection assessments to account for other digital risks. They must look beyond traditional protection frameworks and adopt ethical and rights-promoting approaches to digital technologies, including human control, transparency and accountability.

AIM, SCOPE AND STRUCTURE OF THE CHAPTER

This chapter's purpose is to outline some emerging standards and guidelines for protection work in the digital age and to scope out key issues for protection actors to examine further.

It:

- is complementary to Chapter 7 on the management of protection data and information and data-related risks
- addresses protection risks stemming from digital technologies, which can require responses that go beyond data-related measures taken by protection actors
- focuses on the harm that affected populations are subjected to by the behaviour of those participating in armed conflict or violence, their use of digital means and methods, and the use of digital tools and solutions in protection responses.

This chapter is divided into three sections.

- The risks associated with the use of digital technologies during armed conflict and other situations of violence.
- The fundamental principles underpinning protection work in digital contexts and the need to abide by ethical frameworks when using digital technologies.
- Guidance on achieving effective protection outcomes in the digital age.

PROTECTION WORK IN THE DIGITAL AGE

This section examines and illustrates various types of protection risk and harmful effects that can emerge from the use of digital technologies and related behaviour. It is complemented by Annex 2, which sets out specific digital risks, by which we mean protection risks enabled by the use of digital technology.

DIGITAL RISKS AS PROTECTION RISKS



- 8.1 Protection actors must take all feasible measures to minimize risks that are enabled by digital technologies and might have consequences for the rights, safety and dignity of affected populations.

Digital risks are of particular concern during armed conflict and other situations of violence owing to three interlinked factors:

- people are often at their most vulnerable
- protective frameworks and mechanisms are often challenged
- digital technologies are not necessarily adapted or designed to integrate or respond to people's vulnerabilities in these contexts.

Warring parties and others also use these technologies to harm people and infringe on their rights.

Examples of protection risks enabled by the use of digital technology (see more details in Annex 2)

- The disruption of critical infrastructure, such as water, health care or energy through cyber operations may lead to physical harm or economic hardship.
- The rapid spread of hate speech online and on social media platforms, including calls for violence against certain communities, may contribute to persecution, violence and killing.
- Cyber and other operations targeting infrastructure and resulting in the denial of connectivity and telecommunication services may reduce affected people's autonomy and resilience and hamper access to vital information and emergency services, increase the risk of family separation, endanger forcibly displaced people and make it harder for them to identify and verify safe zones.
- The use of facial recognition and other remote surveillance or automated technologies at borders may cause discrimination and restrict affected populations' right to seek and obtain asylum.
- The use of digital intrusion and interception tools to monitor the digital communications of affected populations (e.g. text messages, email, social media, etc.) to access sensitive and personal information may lead to targeting resulting in arbitrary arrest, torture or killing.

Some of the protection risks that emerge from the use of digital tools are not new, but they can all cause or amplify risks and harm that increase the vulnerability or suffering of affected people. The harmful consequences of the use of digital technologies and related behaviour can impact an affected person's life, safety, security, physical or psychological well-being, dignity and livelihood. These consequences include infringement of the fundamental rights of affected populations, as enshrined in international humanitarian law (IHL), human rights law (HRL), international refugee law (IRL) and other bodies of international law.

The likelihood of digital risks and their resulting impact depend on context and population profile and are influenced by intersectional factors (e.g. gender, ethnicity and socio-economic background) and the design, quality, accessibility, management and governance of digital infrastructure and tools. The digital and media literacy of affected populations – and protection actors – is also an important factor that can increase their resilience and ability to avoid or mitigate digital threats.

As a result, protection work in the digital age must entail:

Improved respect for and protection of the rights of people when they are restricted or affected by or via the digital space because of armed conflict and other relevant actors' behaviours and their use of digital means and methods.

Protection work extends to situations where people's rights, safety and dignity are affected as a result of digital means. In other words, protection work in the digital age aims to ensure that affected populations can fully access and exercise their rights, including online, and that they are protected from risks that are triggered by the use of digital technologies, enabling them to avoid or mitigate harm or to support their self-protection.

Protection work in the digital age should consider, as a priority, factors and vectors of harm mediated or exacerbated by digital technologies. These factors and vectors include physical (e.g. digital infrastructure and devices), intangible (e.g. data and software) and social or human (e.g. information and digital literacy). Protection work should also consider the effects of and interactions between humans, between humans and machines, and between machines.

Protection actors must adapt or develop protection activities and strategies that address protection risks related to the use of digital technologies. While capacity and expertise constraints may limit and delay their ability to address these risks, they should move towards being able to address digital risks and their resulting human rights and humanitarian impacts in accordance with their mandates and the severity and nature of the impacts. This includes operationalizing digital risk considerations across the cycle of protection work, including protection risk analysis, assessments and documentation processes (See Guideline 8.6).

A PRINCIPLED PROTECTION APPROACH TO DIGITAL TECHNOLOGIES

Digital technologies used by protection actors are not inherently protective or neutral and may trigger issues related to safety, perception or instrumentalization. When designing, deploying, and using these tools and solutions, protection actors must consider the digital risks in order to ensure respect for the protection principles laid out in Chapter 2. This section highlights the issues of which protection actors must be aware in order to uphold these principles when using digital tools and operating in digital contexts.

RESPECTING THE PRINCIPLES OF HUMANITY, IMPARTIALITY AND NON-DISCRIMINATION



8.2 Protection actors must ensure the principled delivery of protection action through digital tools and solutions.

Protection actors operating in digital(ized) environments and using digital technologies must apply and uphold the principles of humanity, impartiality, and non-discrimination. These principles must guide the choice, development, deployment and maintenance of digital technologies, together with protection strategies, activities and outcomes. Other guidance, tools and standards, such as those on data protection, due diligence, accountability to affected people or people-centric design can contribute to and uphold these principles.¹³¹

Humanity

Protection actors must ensure that affected populations are treated with humanity and that their dignity is respected in all circumstances, including when protection work is enabled or mediated by digital technologies (see Standard 2.1).¹³²

Digital tools (e.g. social media, digital apps, chatbots or other AI-enabled tools) have been praised as increasing the reach, scale and depth of engagement with affected populations. However, protection actors must ensure that their use of digital tools does not prevent them from engaging with affected populations with the necessary human empathy and compassion, which cannot be replaced, replicated or automated via digital means. Protection actors must also consider that the use of digital interfaces may limit crisis-affected populations' trust and negatively impact an individuals' ability to share personal stories or express sensitive feelings and needs.¹³³ Similarly, protection actors must ensure that the use of such interfaces does not foster detachment, remoteness or a loss of human touch with affected people. Digital solutions should enhance or complement – and not replace – face-to-face human interactions and services and avoid jeopardizing protection actors' ability to maintain physical presence and proximity.

¹³¹ These include, for instance, ethical principles relating to the use of artificial intelligence such as the [Principles for the Ethical Use of Artificial Intelligence in the United Nations System](#), or [UNESCO's Recommendation on the Ethics of Artificial Intelligence](#). See more in Annexes 1 and 2 to this chapter.

¹³² As also recognized in other ethical and legal frameworks, including the [Sphere Humanitarian Charter](#).

¹³³ Conversely, digital interfaces can be conducive to the sharing of personal and painful experiences, which underlines the importance of respecting individuals' preferences.

Impartiality and non-discrimination

Protection actors must ensure that affected populations and their needs are addressed impartially and that people do not suffer discrimination when protection work is enabled or mediated by digital technologies (see Standards 2.2 and 2.3).

Artificial intelligence and data analytics systems can help guide, optimize and support protection activities. When using these digital technologies in support of protection activities, protection actors must ensure the accuracy, quality, availability, reliability, accessibility and understandability of the data used. They must take proactive measures to prevent and mitigate the negative consequences that may arise as a consequence of biases in the datasets or the design of algorithms used to deliver response (see Standard 7.8 and Annex 1 to Chapter 7).

The implementation of digital-enabled programmes, and any associated technical and technological failures, may also lead to discriminatory effects. Protection actors must consider inclusive and appropriate access requirements (e.g. in terms of technologies, energy and connectivity), accessibility requirements (e.g. language and design)¹³⁴ and ensure these do not deny protection to certain populations or increase the digital divide that are due to pre-existing patterns of discrimination. Protection actors must have analogue and face-to-face alternatives in place to guard against such failures and adverse impacts.

Protection actors must ensure the highest possible levels of transparency in the use of digital technologies, strive to rely on digital solutions that are explainable to and comprehensible by affected populations and maintain the highest possible degree of human oversight and control over their functioning and outputs. Moreover, to ensure accountability to affected populations, the design and implementation processes of programmes using digital technologies should be documented and transparent.¹³⁵

DIGITAL “DO NO HARM”



8.3 Protection actors must avoid and mitigate the harm that could arise from the use of digital tools and solutions in their activities.

Protection actors must identify and address potential digital risks and harmful effects when their activities are being designed, analysed, implemented or monitored via or with digital technologies (see Standard 2.4).¹³⁶ If significant harm, particularly to affected people’s rights, cannot be prevented or mitigated, protection actors must not use the digital technology. Where relevant and possible, protection actors should also make remedy processes and measures available to affected people.

To effectively uphold the “do no harm” principle and avoid harmful adverse effects, protection actors¹³⁷:

- Must implement robust data and information management, cybersecurity and relevant protection frameworks to mitigate the misuse of or illicit access to protection data (e.g. errors, biases or attacks).¹³⁸
- Must ensure that their use of digital technologies and allocation of resources is driven by a genuine understanding of and a commitment to addressing clear and defined protection risks to affected populations. This requires a cautious approach that focuses on using technology when it is an appropriate and effective response to clearly identified protection risks.

¹³⁴ See, for instance, [W3C accessibility standards](#).

¹³⁵ See also Standard 7.9 on transparency and Guideline 7.13 on accountability with regard to protection data and information.

¹³⁶ See, for instance, Kristin Bergtora Sandvik, Katja Lindskov Jacobsen and Sean Martin McDonald, [Do no harm: a taxonomy of the challenges of humanitarian experimentation](#), *International Review of the Red Cross*, 2017; Pierrick Devidal, Lost in digital translation? “The fundamental principles in the digital age”, *International Review of the Red Cross*, 2024; Bergtora Kristin Sandvik, [Humanitarian Extractivism: The Digital Transformation of Aid](#). Manchester University Press, 2023.

¹³⁷ This is a non-exhaustive list.

¹³⁸ See Chapter 7.

- Must ensure that they and their partners never experiment, trial or deploy untested digital tools or solutions on affected populations. Prior to the deployment (at scale) of digital technologies, affected populations must be consulted and there must be credible evidence that the technologies are – and are considered to be – safe and effective, and do not pose undue risks to specific rights. Throughout the process, protection actors and their partners must abide by internationally accepted ethical standards and protective frameworks.
- Must account for human rights and other due diligence processes¹³⁹ when procuring digital technologies from third parties. This includes impact assessments that assess the risks posed by both the technology and the supplier. Protection actors must follow these processes throughout the life-cycle of the system and technology, to evaluate current and emerging risks and enable auditing.
- Should require that they and/or third parties operating on their behalf have the capacity and resources to use and maintain digital technologies or enable programmes in the manner designed for the entirety of their programme cycle.
- Should prepare for and mitigate against the risk of disruptions, whether of connectivity/communications or of their digital solutions (e.g. owing to technical malfunction) that could affect the planning, coordination and implementation of protection work. Standard operating procedures to manage such disruptions should be prepared, devised and tested.
- Should be mindful of the inherent power dynamics of digitalized and less-digitalized contexts and avoid reinforcing or exacerbating existing inequalities therein.
- Should ensure that digitalization and connectivity are only promoted to affected populations and local partners with the necessary support, such as digital literacy and risk awareness programmes. Whenever feasible, preference should be given to local, people-centric and community-led approaches.
- Should be conscious that external partners might not necessarily abide by rights-based approaches or principles and that there can be a risk of digital exploitation. In addition, policies and principles may not be implemented in practice and it is therefore important to adjust preventive and mitigating measures as necessary.

PEOPLE-CENTRIC AND INCLUSIVE DIGITAL TECHNOLOGIES



8.4 The development and deployment of digital tools and solutions designed for protection action must be people-centric and inclusive.

Digital tools must be used to respond to clearly identified protection needs and gaps, including the making of free and informed choices and to assert individuals' rights.

Protection actors must ensure that affected populations are equally included and engaged throughout the design, development and deployment phases of their digital tools and solutions – people-centric design (as outlined in Standard 2.6 and 2.7).¹⁴⁰ This includes understanding and addressing any barriers to participation faced by affected people (including digital literacy) and building on local capacities and adopting locally used tools where feasible and appropriate. This is essential, to minimize risks, to develop and maintain trust and to ensure that digital solutions are accessible, relevant, culturally appropriate, functional and sustainable. Insufficient engagement, inclusivity and communication with communities may result in misunderstandings, heightened anxiety and disengagement.

Protection actors must respect the concerns and objections of local stakeholders with regard to the use of digital technologies and consider refraining from their deployment in such cases. Receiving protection or humanitarian assistance should not be strictly conditional upon providing personal data or using certain digital tools or means. Affected populations should always have access to alternative solutions and be able to make informed and meaningful choices. They should be regularly updated about the decision-making process related to such technologies.

¹³⁹ See, for instance, *UN Secretary General's Guidance on Human Rights Due Diligence and Digital Technologies*, UN, 2024 (forthcoming).

¹⁴⁰ As described in other frameworks and standards, including Sphere Core Standard Commitment 4 or [The Signal Code](#) Obligations 3 and 5.

To ensure that engagement and consultation with affected populations is inclusive, protection actors must establish the necessary engagement, feedback and response mechanisms, which must continue after a technology system has been implemented (as outlined in Standard 2.7). Feedback mechanisms must ensure meaningful consultation with affected people and communities about the challenges they may face with the digital technology and immediate steps to address concerns and, if necessary, to suspend its use. Where protection action is digitized or automated, it must take into account challenges related to quality, speed, remoteness and the ability to capture certain human nuances such as language, tone and accent. Feedback mechanisms should always have human oversight.

FURTHER ETHICAL AND OPERATIONAL IMPLICATIONS

G

8.5 Protection actors should mitigate any negative impacts or ethical and operational implications of their choice, use of or dependency on digital technologies or providers.

Certain protection actors subscribe to the principles of independence and neutrality. While these principles are not fundamental to all protection actors, it is essential that those whose actions rely on them consider the ethical, operational and perception implications related to the choice and use of digital technologies or to operating in digital(ized) contexts. The related implications can also be relevant for all protection actors.

Neutrality

The design and choice of digital technologies and systems are not inherently neutral. They can impact how protection actors are perceived and trusted, which can in turn affect their access to affected populations. Technologies embody, encode and entrench the values and biases of their owners, designers, developers and promoters. The companies that develop, sell or maintain digital technologies for protection actors can also act in a non-neutral manner. Protection actors should therefore consider the risk that the digital solutions they choose and use could cause them and their partners to be perceived to be spying, supporting military operations or aligning themselves politically – to the potential detriment of affected populations.

Protection actors should avoid using or relying on digital technologies and providers that:

- directly contribute to armed conflict or OSV
- are closely associated with parties to armed conflict
- favour particular political interests
- promote activities or values that are contradictory to their mandate, fundamental principles or ethical values.

This can be achieved by developing or adapting procurement and due diligence mechanisms and applying relevant ethical frameworks relating to digital technologies.

Protection actors should also consider the potential operational impact of their technological choices and plan to mitigate them. For instance, the use of certain technologies originating from or used by one warring party might be limited for technical or political reasons,¹⁴¹ which might create acceptability, interoperability or risk challenges. To remain credible and neutral, protection actors may explore alternatives such as open-source software, when these offer adequate and safe solutions.

Independence

Although large-scale service providers offer advantages such as cost and security, reliance on them may increase the risk of being locked into commercial relationships with powerful suppliers that also engage in political or armed-conflict-related controversies – thus raising potential perception and ethical issues. These relationships may limit actual control over protection data and systems or lead to additional unforeseen, long-term financial consequences. Identifying and managing these digital dependencies can help protection actors ensure their operational continuity, agency and autonomy. It may also help them to manage perception risks related to reliance on specific digital technologies or providers.

¹⁴¹ Such as by sanctions or other restrictive measures.

As protection actors further partner with external actors to develop or procure digital tools and solutions, they need to be conscious of the fact that these partners and digital suppliers may have different interests, relationships with states and governments, incentive structures or legal and ethical frameworks and approaches. Protection actors should specifically address and manage the risk of instrumentalization¹⁴² by these stakeholders. Corporate agendas may reduce protection actors' operational autonomy while promoting the interests of commercial entities, including testing their tools, improving their reputation and creating distractions from misbehaviour and concerning practices (e.g. exploitative labour practices or lack of respect for the right to privacy).

ENHANCING PROTECTION OUTCOMES IN THE DIGITAL AGE

Protection actors must responsibly harness the opportunities offered by digital transformation to deliver positive outcomes for communities affected by armed conflict, other situations of violence and disaster. This section provides some guidance and considerations protection actors should take to operationalize their work and enhance protection outcomes in the digital age.

INTEGRATING DIGITAL RISKS IN PROTECTION STRATEGIES

G

8.6 Protection actors should integrate digital risks and their harmful effects in their protection documentation and assessments. They should include and implement adequate responses and mitigating measures in their protection strategies.

Protection actors should integrate digital dimensions in their documentation and protection analysis to guide their protection strategies.¹⁴³ The former should include engaging with communities whose lives are impacted by digital technologies, taking into account their diversity and their ability to understand the secondary effects that the use of technologies may have on their lives, safety or fundamental rights. It could also include developing a common taxonomy of digital-related harm or needs. It can be complemented by hybrid documentation and incident monitoring techniques, such as open-source investigation or social media analysis.

As per the latter, existing protection assessments may be limited in their ability to capture the different elements underpinning digital risks and the vulnerabilities of affected populations vis-à-vis digital technologies. Protection actors should therefore consider integrating digital risk elements in their protection assessments. These assessments should be context-based, engage with affected populations and account for various ecosystems (e.g. society, communities and individuals) that are dependent on or affected by the use of digital technologies. For instance, they should capture risks and needs beyond those that relate to data, encompassing the information environment (including social media), connectivity (telecommunications and internet), taxonomy of digital-related risks (differentiated by actor) and digital inclusion.

REFERRING TO AND DEVELOPING PROTECTIVE FRAMEWORKS

S

8.7 Protection actors must be familiar with, uphold and respect the relevant principles and legal frameworks to ensure adequate protection for affected populations against digital risks. Where necessary and feasible, they should help develop a common understanding and guidelines to advocate for the protective application of these frameworks in contexts affected by armed conflict and violence.

¹⁴² See, for instance, Aaron Martin, [Aidwashing Surveillance: Critiquing the Corporate Exploitation of Humanitarian Crises](#), Surveillance and Society, 2023.

¹⁴³ See Chapter 3 on managing protection strategies and Standard 3.1.

As outlined in Standard 4.1, protection actors must be familiar with the various applicable principles and legal frameworks that protect individuals and communities during armed conflict and other situations of violence. By extension, to ensure that the rights of individuals are protected against digital-enabled risks, staff working on protection issues relating to such risks must be competent in the application of the legal frameworks to digital risks, such as IHL or IHRL, together with other developing regulatory frameworks for specific digital technologies, such as artificial intelligence.¹⁴⁴

Protection actors with the necessary expertise and capacity should reaffirm, raise awareness of and advocate for the specific rules related to behaviour and operations that can foster digital risks during armed conflict and other situations of violence. This extends to engaging with private-sector actors, which may be duty bearers (individuals, groups and companies). It also includes supporting the development, interpretation and clarification of existing international and national legal and other frameworks, policies and procedures in digital contexts, to reduce ambiguity and ensure adequate protection of people, infrastructure, data and other objects. If protection actors engage in the development of new legal rules and norms, they should ensure they build upon and strengthen – not undermine – the protection of affected populations in existing international legal frameworks.

The rights established in various legal frameworks (see Chapter 4)

It is today also recognized that IHL applies to the use of cyber and information operations during armed conflict. For instance, cyber operations conducted in situations of armed conflict must comply with the principle of distinction, which prohibits cyber operations directed against civilian objects, and the principle of proportionality, which prohibits cyber operations that can be expected to cause excessive incidental harm to civilians and civilian infrastructure. IHL provides specific protection for medical and humanitarian operations. IHL rules also apply to other new technologies of warfare, such as AI, outer space operations, autonomous weapons systems and information operations. Note that states continue to debate the interpretation of IHL in these different fields.

The application of human rights to digital technologies has been recognized internationally, including in resolutions of the United Nations Human Rights Council and the General Assembly.¹⁴⁵

These include, but are not limited to:

- freedom of expression
- privacy
- access to information
- freedom of assembly and association
- the right to equality
- non-discrimination.

There has also been considerable discussion on specific practices, such as internet shutdowns, and how they might affect these rights.

The application of the elements of the right to privacy online has been extensively considered, encompassing the protection of individuals from unlawful interference with their private and family lives, homes or communications, and the right to data protection. This includes the systematic application of a set of principles regarding the processing of personal data, aiming to protect the privacy of individuals and uphold their rights as data subjects, such as the right to be informed, to access, to rectify, to object or to delete personal data (see Chapter 7).

¹⁴⁴ See Annex 2 to this chapter.

¹⁴⁵ UNGA, [Promotion and Protection of Human rights in the Context of Digital Technologies](#) [A/RES/78/213 22/12/2023].

ENGAGING IN PROTECTION DIALOGUE ON DIGITAL RISKS

S

8.8 Protection actors must engage with relevant actors and establish protection dialogue on digital risks, related protection concerns and rights violations.

Protection actors that have a relevant mandate and the necessary capacity must consider engaging in protection dialogue on digital risks, related protection concerns and rights violations. This could involve specialized governmental bodies such as law enforcement or the judiciary, and military entities (e.g. cyber commands, psychological operation units or cybersecurity agencies). Protection actors may also undertake such dialogue with non-state actors¹⁴⁶ such as hacker groups,¹⁴⁷ or private-sector entities such as internet service providers or social media companies. Protection dialogue should also be inclusive of relevant civil society and community-based actors working in this space.

The decision as to which actors to engage with should be based on a detailed examination of their actions (including harmful acts, threats and violations, together with capacities and positive protection actions in the digital space), affiliation, *modus operandi* and ability to influence or reduce harm to affected populations.

The aims and types of dialogue or interaction may vary. Dialogue could aim to persuade or recall a duty bearer to fulfil their legal obligations and protection responsibilities, achieve a specific protection outcome or improve the security of humanitarian operations or human rights missions. For instance, a cybercommand could be reminded not to indiscriminately target civilian or digital humanitarian infrastructure with disruptive cyber operations. A protection dialogue could also seek to raise awareness of the impact and harm resulting from certain behaviour or use of technology, such as internet or telecommunication shutdowns or the spread of harmful information on social media or via messaging applications. Similarly, a protection dialogue could aim at building trust, establishing points of contact, improving understanding of the context, enhancing the actor's capabilities or furthering the development and operationalization of protective legal frameworks.

The format and content of these dialogues should be tailored to the underlying motivations, incentive structures and strategic commitments of these actors. In some instances, this might require considering or referring to the relevant legal and other frameworks. For instance, in the case of a private (tech) company, this could include referring to the UN Guiding Principles on Business and Human Rights which it may be committed to or other relevant international, regional, or national legal obligations. Concurrently, protection actors should consider, identify and mitigate the risks that can arise from such engagement, including those relating to confidentiality.¹⁴⁸

STRENGTHENING AFFECTED PEOPLE'S SELF-PROTECTION CAPACITY AND THEIR RESILIENCE TO DIGITAL RISKS

G

8.9 Protection actors should consistently build upon, support, promote and strengthen affected people's capacity for self-protection and their resilience to digital risks.

Protection actors should acknowledge, understand and reinforce the self-protection capacities and resilience of affected individuals and communities in relation to digital risks.

¹⁴⁶ For armed non-state actors specifically, see also Standard 4.3 and Guideline 6.6.

¹⁴⁷ Dialogue elements can include, for instance, Tilman Rodenhäuser and Mauro Vignati, [8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them](#), ICRC Humanitarian Law & Policy Blog, 4 October 2023.

¹⁴⁸ See further guidance, such as ICRC, [Tip Sheet On Maintaining Confidential Digital Dialogue During Humanitarian Emergencies](#).

Such activities can include:

- working with affected populations to identify and respond to digital risks
- reinforcing digital risk awareness
- providing tools or guidance for self-protection in digital spaces
- providing psychological support to manage the impact of online harmful content, including hate speech.

In certain contexts, they can also include providing either information or connectivity-as-aid.¹⁴⁹

Digital risk awareness-raising must respond to the diverse risks individuals may be exposed to, based on the assessments outlined under Guideline 8.6, which should incorporate community perceptions. Mitigation strategies must also build on individuals' experience of navigating risks online, with information, tools and guidance made accessible to diverse groups.

In line with a people-centric protection approach (see Standard 8.4¹⁵⁰), protection actors should recognize, build on, support and avoid undermining local capacity and the agency of affected populations, including as regards how they decide to use digital technologies. Protection actors should strive to recognize, adopt and integrate innovative and rights-respecting solutions developed by local populations utilizing digital technologies. This also entails working with affected populations to assess and address any digital risks stemming from innovative solutions they have devised.

ENSURING COMPLEMENTARITY OF PROTECTION ACTION IN THE DIGITAL AGE

G

8.10 Where relevant, protection actors should cooperate with expert stakeholders to complement their own actions to address digital risks.

In line with Standard 5.1,¹⁵¹ protection actors should cooperate and coordinate their responses to digital risks and threats and leverage digital technologies to promote protection. Coordinated and complementary protection action that aims to leverage all protection actors' knowledge and capacity is essential to reducing any gaps in understanding digital risks and their adverse effects. It can also enable better preparedness, including in the management of protection data (see Standard 7.10). It also helps avoid inconsistent, redundant, concurrent or non-inclusive responses.

Complementarity might involve building on existing internal or external frameworks, relationships and expertise or creating new ones. For instance, protection actors should consider and encourage shared assessments of digital needs and of vulnerability, and shared mechanisms for coordinating specific digital programmes or technologies. In doing so, protection actors should also closely consider their respective comparative advantages, capacity, operational footprint and mandates. Coordination and cooperation should extend beyond protection actors to include diverse types of knowledge and operational partners – e.g. the technical and digital humanities – in academia and the private and public sectors. Such cooperation must abide by legal frameworks, ethical reviews and research protection, including duty of care.

¹⁴⁹ For connectivity-as-aid see, for instance, [NetHope](#), [the Emergency Telecommunications Cluster](#), [UNHCR's Connectivity for Refugees](#), [CISCO Tactical Operations](#), or the [GSM Association](#).

¹⁵⁰ Plus other standards and frameworks, such as [Sphere](#) Protection Principle 1 or [The Signal Code](#) Obligation 7.

¹⁵¹ Plus other standards and frameworks, such as [Sphere](#) Core Humanitarian Standard Commitment 6 or [The Signal Code](#) Obligation 8.

BUILDING PREPAREDNESS OF PROTECTION ACTORS

G

8.11 Protection actors should ensure an adequate level of preparedness relating to digital risks, build and maintain awareness of these and provide sufficient capacity and expertise for response.

Protection activities that involve the use of digital technologies and addressing digital risks require protection actors to develop and maintain a broad and complex range of competencies and capabilities. These include competencies related to digital and technological literacy, such as cybersecurity hygiene, data management and protection, social media literacy and open-source investigation techniques. To anticipate, detect, assess and respond to digital risks, protection actors must also ensure an adequate level of preparedness, in terms both of required skills and capacity and of processes, operational guidance and contingency planning.

As outlined in Chapter 9,¹⁵² protection actors should ensure that their staff and partners have not only demonstrated the relevant professional competency required for their duties and for the development, deployment and use of digital tools but that they are able to continuously learn, maintain and further develop these capabilities. This can entail digital upskilling,¹⁵³ tailored training on organizational policies, professional courses with external partners or experience-sharing mechanisms. These are key to identify, anticipate, prevent and mitigate potential harm from digital risks. It will often be effective to form a multifunctional team, including experts across relevant disciplines within an organization, to assess digital risks and the best protection responses.

ANNEXES TO CHAPTER 8

ANNEX 1: REFERENCE MATERIAL FOR CHAPTER 8

European Commission DG ECHO, [Policy framework for humanitarian digitalization](#), EU, 2023

ICRC, Engine Room and Block Party, [Humanitarian Futures for Messaging Apps: Understanding the Opportunities and Risks for Humanitarian Action](#), 2020

ICRC, [Harmful Information – Misinformation, Disinformation and Hate Speech in Armed Conflict and Other Situations of Violence: ICRC Initial Findings and Perspectives on Adapting Protection Approaches](#), 2021

ICRC, [Protecting Civilians Against Digital Threats During Armed Conflict: Recommendations to States, Belligerents, Tech Companies and Humanitarian Organizations](#), ICRC Global Advisory Board On Digital Threats During Armed Conflict, 2023

IOM, OCHA Centre for Humanitarian Data, IFRC and ICRC, [Tip Sheet on Maintaining Confidential Digital Dialogue During Humanitarian Emergencies](#), ICRC, 2020

OCHA and WEF, [Guiding Principles for Public-Private Collaboration for Humanitarian Action](#), OCHA, 2007

OCHA Centre for Humanitarian Data, IFRC and ICRC, [Tip Sheet On The Responsible Use Of Online Conferencing Tools](#), IFRC, 2021

OHCHR, [Digital Space and Human Rights](#)

OHCHR, [Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework](#), 2012

¹⁵² See also other standards and guidance, including the [Protection Information Management \(PIM\) Core Competencies; Core Humanitarian Competencies Framework](#); or [The Signal Code Obligation 2](#).

¹⁵³ See, for instance, [Technologies in humanitarian settings: digital upskilling of humanitarian actors](#); [GSMA Mobile Internet Skills Training Toolkit \(MISTT\)](#).

- Sphere Project, [Sphere Handbook: Humanitarian Charter and Minimum Standards in Humanitarian Response](#), 4th edition, 2018
- UN Secretary-General Guidance on Human Rights Due Diligence and Digital Technologies, UN, 2024 (forthcoming)
- UN, [Global Principles for Information Integrity](#), 2024
- UNGA [Promotion and Protection of Human Rights in the Context of Digital Technologies](#), [A/RES/78/213, 2023]
- UNHCR, [Using Social Media in Community-Based Protection: A Guide](#), 2021
- Arendt-Cassetta, Leonie, [From Digital Promise to Frontline Practice: New and Emerging Technologies in Humanitarian Action](#), OCHA, 2021
- Bryant, John, [Digital Technologies And Inclusion In Humanitarian Response](#), HPG, 2022
- Campo, Stuart R., Howarth, Caitlin N., Raymond, Nathaniel A., and Scarnecchia, Daniel P., [Signal Code: Ethical Obligations for Humanitarian Information Activities](#), 2018
- Detle, Rachelle, [Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts](#), Global Public Policy Institute, 2018
- Devidal, Pierrick, [‘Back to Basics’ with a digital twist: humanitarian principles and dilemmas in the digital age](#), Humanitarian Law and Policy Blog, 2023
- Düchting, Andrea, [Digital Accountability: The Untapped Potential of Participation when Using Digital Technology in Humanitarian Action](#), CHA, 2023
- Lahman, Henning, [The Future Digital Battlefield and Challenges for Humanitarian Protection: A Primer](#), Geneva Academy, 2022
- Lough, Oliver, [Social Media and Inclusion in Humanitarian Response](#), HPG, 2022
- Oribhabor, Isedua, [Tech and Conflict: A Guide for Responsible Business Conduct](#), Access Now, 2023
- Raftree, Linda, [Digital Safeguarding for Migrating and Displaced Children: An Overview of the Current Context and Trends, Potential Risks and Practical Next Steps](#), Save the Children, 2020
- Rejali, Saman, and Heiniger, Yannick (eds.), [Digital technologies and war](#), International Review of the Red Cross, No. 913, March 2021
- Rodenhäuser, Tilman, Staehelin, Balthasar and Marelli, Massimo, [Safeguarding Humanitarian Organizations from Digital Threats](#), Humanitarian Law and Policy Blog, 2022
- Sandvik, Kristin Bergtora, [Humanitarian Extractivism: The Digital Transformation Of Aid](#), Manchester University Press, 2023
- Sebastián, S., Meléndez Vicente, J., Khan, S., and Vinck, P., [Technologies in Humanitarian Settings: Balanced, Principled and Complementary Partnerships](#), Harvard Humanitarian Initiative, 2022
- Willitts-King, Barnaby, Bryant, John, and Holloway, Kerrie, [The Humanitarian “Digital Divide”](#), HPG, 2019

ANNEX 2: EXAMPLES OF PROTECTION RISKS ENABLED THROUGH THE USE OF DIGITAL TECHNOLOGY

The non-exhaustive list below details some of the key digital risks of which protection actors should be aware.

Harmful information¹⁵⁴

Though there is no internationally agreed upon definition, harmful information is considered as information that can potentially cause or contribute to harm, either physically, psychologically, economically or socially.

Harmful information includes (but it is not limited to) misinformation (false information *unintentionally* spread by individuals who believe the information to be true), disinformation (false information *intentionally* disseminated with malicious intent or for economic gain), malinformation (true information *intentionally* spread to cause harm). In this definition, information or narratives that may be used in violation of legal norms are also considered as harmful information. In addition, while recognizing that information and speech may be different, this umbrella definition term also includes hateful narratives and hate speech.¹⁵⁵ Harmful information is a complex phenomenon that can manifest itself through digital and non-digital means, can pass fluidly between online and offline worlds and can easily and cheaply be amplified by various actors.

Harmful information can significantly impact the trust dynamics between protection actors, media, government as well as humanitarian and human rights sectors. Harmful information also has direct implications for the way armed conflicts are waged, altering public perceptions, political discourse and military decision-making. While harmful information is far from a new phenomenon, it can be used by militaries and third parties as a tactic during wartime to gain a military advantage. Some purveyors of harmful information may also be motivated by financial gain, benefiting from the monetization systems that underpin digital platforms. The digital dimension of harmful information (which is reinforced by offline realities and dynamics) has become a protection challenge in humanitarian and human rights settings because of the speed, reach and influence of malicious content on already explosive and volatile environments. In those contexts, information can be a matter of life and death.

Key concerns include:

- **Humanitarian consequences affecting the civilian population.** Harmful information can cause harm to people's physical, psychological, economic and social well-being. It can undermine public trust, negatively influence people's beliefs and behaviours, erode their agency and dignity; deprive them of or misdirect them away from life-saving services. Moreover, it can harm their psychological well-being, as they may become targets of harassment, defamation and/or intimidation. It can also contribute to the dehumanization of individuals or people; endanger the safety of civilians by stoking calls for violence against a particular group. In emergencies, access to unreliable or false information may impact people's safety. Finally, it may also influence the behaviour of arms bearers by making them less likely to comply with international legal and protective frameworks.
- **Significant impact on the dynamics of an armed conflict.** As harmful information spreads, it can influence public perception and debates, affect people's behaviour, fuel protests and demonstrations, shape political debates and sway political and military decisions. In time of war, escalatory and other harmful narratives undermine people's protection and resilience and can fuel hatred and violence.

¹⁵⁴ For further reference, see [Harmful Information – Misinformation, disinformation and hate speech in armed conflict and other situations of violence: ICRC initial findings and perspectives on adapting protection approaches](#); [MDH Q&A; Liar's war: Protecting civilians from disinformation during armed conflict](#); [Addressing harmful information in conflict settings: A response framework for humanitarian organizations](#); [The Legal Boundaries of \(Digital\) Information or Psychological Operations Under International Humanitarian Law](#); [Social media and conflict: Understanding risks and resilience, an applied framework for analysis](#).

¹⁵⁵ For the UN's working definition of hate speech, see UN, [Understanding Hate Speech](#).

- **Affect of protective international legal frameworks.** While there is no absolute prohibition on publishing or sharing false or manipulated information during armed conflict, either under IHL, IHRL or other international legal norms, these legal frameworks do impose limits on certain uses of information. For instance, propagating information regarding recruitment of children, spreading fear and terror among civilians, publishing images of prisoners of war in ways that expose them to public curiosity or obstructing humanitarian work.
- **Impact on the trust, acceptance and safety of protection organizations and their efforts.** Harmful information can hinder protection efforts and diminish the space for impartial protection action by spreading false and manipulated information about protection organizations, staff and volunteers and their motivations, mandates and principles. These can cause reputational damage that can rapidly translate into an erosion of trust among affected populations, parties to the armed conflict and other actors and undermine acceptance and access, impeding the delivery of vital protection work. Information campaigns targeting one organization can also have a ripple effect that undermines the space for principled protection action by others. Harmful narratives can lead to security issues in the form of threats or attacks against protection workers and facilities, both in the offline world and in the digital sphere.

Cyber operations¹⁵⁶

A set of activities that occur at least partly within cyberspace, against a computer, a computer system or network or another connected device, using digital/cyber means to disrupt, disable or degrade such a system or achieve an unauthorized effect.

Cyber threats may include unauthorized access to a computer system (“hacking”), data theft, alteration or deletion, system interference and misuse or mismanagement of devices. Common threats include distributed denial-of-service (DDoS), spyware, ransomware, supply chain attacks or phishing. They can be carried out by a variety of threat actors, including criminal organizations, states, hacktivist groups, private people or combinations thereof. The purpose can vary greatly, including espionage, crime, information operations and warfare. Cyber operations can be conducted in support of both information and kinetic operations.

For protection actors, cyber operations can be of concern because they can cause significant harm and consequences depending on the types of targets chosen and the effects they create. Their effects might be first-order, affecting digital assets directly (e.g. impacting the confidentiality, integrity or availability of data and systems) or second-order, affecting individuals and society indirectly (e.g. leading to physical harm or economic hardship or affecting psychological well-being).

Cyber threats can result in surveillance, discrimination, persecution and other harmful consequences for affected populations. They can exacerbate the vulnerabilities of affected groups and individuals, erode trust and compromise the principled delivery of protection work.

Key concerns include:

- **Disrupting, disabling or degrading critical and essential infrastructure.** Cyber operations affecting critical civilian infrastructure, such as hospitals, nuclear facilities, energy networks, water systems, telecommunication or financial services can exacerbate or cause significant harm and human cost. They may impede affected populations’ ability to access vital information or essential services and risk causing physical and psychological harm.
- **Impact on protection operations.** Cyber operations can affect the operational continuity of protection actors, which can threaten the safety and well-being of those they work to protect. Cyber operations may affect access to affected populations or their trust in protection actors, or make it more difficult to coordinate with other actors, assess protection needs and provide aid to affected populations. All of these are likely to exacerbate the needs of people affected by armed conflict and other crises. Such operations may also divert scarce resources from protection work and undermine other work, such as Accountability to Affected People or Communicating with Communities.

¹⁵⁶ For further reference, see [Avoiding civilian harm from military cyber operations during armed conflict](#); [International humanitarian law and cyber operations during armed conflict](#); [Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats](#); [Potential Human Cost of Cyber Operations](#). On ILH and cyber, see, for instance, [Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflict](#); [International humanitarian law and cyber operations during armed conflict](#); [Cyber Law Toolkit](#).

- **Compromising protection data.** Cyber operations can lead to data and cybersecurity breaches that undermine the privacy of the people whose data are compromised, risk exposing sensitive and personal information to malicious actors and erode trust in protection organizations' capabilities. This can also endanger the safety of protection workers.
- **Cybercrime.** Criminal cyber operations can target and exploit crisis- and conflict-affected populations directly, leading to theft, fraud or scams.

Connectivity denial¹⁵⁷

The disruption of internet or digital (tele)communications, slowing them or rendering them inaccessible or effectively unusable, for a specific population or within a location.

Connectivity denial is often used to exert control over the flow of information or to support political or military objectives. It can be intentional or due to spillover effects, such as collateral damage resulting from armed conflict, or a power cut. There are different types of internet shutdown depending on their coverage and on the type of communication affected: e.g. blanket (cutting all access to the internet and/or telecommunication services) and targeted (limiting internet and telecommunication access to specific areas, populations, types of network or services).

Connectivity denials are of concern to protection actors as they not only enable certain vulnerabilities or restrict enjoyment of internationally recognized rights, such as freedom of expression or assembly, but can also have a direct impact on the delivery of (essential) services, the resilience of affected people and their capacity to self-protect.

Key concerns include:

- **Access to information.** Limiting crisis-affected populations' access to life-saving information, such as safe routes, humanitarian camps, food, shelter, health care or ability to communicate and call for help. Connectivity denial can also substantially reduce situational and risk awareness.
- **Risk of separation.** Enhancing the risk of separation, because of the importance of connectivity in maintaining and restoring family links.
- **Disrupting protection work.** Reducing or denying access to protection services and disrupting the operations of protection actors, not only by restricting access to certain populations but also by cutting their own supply chains and services and reducing their ability to coordinate and document, increasing the likelihood of service duplication, service exclusion and inflated service costs.
- **Impacting livelihoods.** Hindering affected populations' access to services and their ability to seize economic opportunities, and undermining economic growth and development.
- **Enabling a sense of impunity.** Fostering a sense of impunity among those participating in conflict or violence, thereby potentially increasing abuse and violations, such as ill-treatment of civilians.

Artificial intelligence and other machine learning technologies¹⁵⁸

These technologies are increasingly used during armed conflict and other situations of violence to automate processes (e.g. data fusion), systems (e.g. autonomous weapon systems) and functions (e.g. decision support, targeting and predictive assessments).

¹⁵⁷ For additional resources, see [Displaced and Disconnected](#); [Connecting with confidence](#); [Keep it on](#); [Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights](#).

¹⁵⁸ See Chapter 7, Annex 2 for an explainer on AI. For additional resources, ethical frameworks and guidance on AI see the [AI standards hub](#); [Recommendation on the Ethics of Artificial Intelligence](#); [Principles for the Ethical Use of Artificial Intelligence in the United Nations System](#); [Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector](#); [Artificial Intelligence Principles for Vulnerable Populations in Humanitarian Contexts](#); [Principles on Artificial Intelligence](#); [AI and machine learning in armed conflict: A human-centred approach](#); [Autonomy, Artificial Intelligence \(AI\) and Robotics: Technical Aspects of Human Control](#); [Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks](#); [Humanitarian AI: The hype, the hope and the future](#); [Chatbots in Humanitarian contexts](#).

Machine learning technologies are typically used to execute specific tasks, via training on large datasets, to deliver outputs that are not explicitly programmed. AI applications include pattern recognition, natural language processing, computer vision (e.g. facial recognition) and large language models, (e.g. certain chatbots).

The uses of AI are extremely varied, including the processing of data, surveillance systems (notably at borders and in migration settings¹⁵⁹) and the generating of social media recommendations. One area of particular concern is its use for the conduct of warfare, specifically in autonomous weapon systems¹⁶⁰ and decision-support systems.¹⁶¹ The use of AI is a matter of concern for protection actors, as it may have serious consequences for people's lives.

Key concerns include:

- **System limitations and harmful consequences.** Biased, poisoned, corrupted or inaccurate datasets or outputs, system errors, algorithmic hallucination or other design limitations can lead to discrimination, mistargeting and death or other physical harm to affected people, depending on the AI system and the context. In armed conflict, this may result in accidental escalation and in any event will heighten the risk of incidental harm to civilians and protected persons. AI – and especially machine learning – also raises concerns related to unpredictability, unreliability, lack of safety and lack of transparency.
- **Loss of transparency, human agency, judgement and control.** Reliance on AI systems can lead to loss of human control, autonomy, accountability or oversight. Automation bias and other factors may degrade the quality of human assessment, alertness, judgement or ability to maintain situational awareness of those using AI during armed conflict or other situations of violence. There is a risk of loss of human judgement in decisions that concern important values (e.g. life, health and dignity) and can have serious consequences for civilians, such as the use of force. These may risk jeopardizing respect for legal frameworks.
- **Enabling other digital risks.** The advent of AI tools may further lower the barrier to conducting digital operations and may exacerbate other digital risks and their consequences, such as the spread of harmful information, the conduct of cyber operations and the surveillance and exclusion of certain populations.

Digital surveillance¹⁶²

Digital surveillance is pervasive, systematic and ubiquitous during armed conflict and other situations of violence. It is the collection, processing, sharing, analysis and use of electronic data, including internet and phone communication, social media activity, location data, metadata¹⁶³ and other forms of digital activity, to monitor individuals or groups, including of (or via) protection actors.

Digital surveillance technologies include those for interception, intrusion or tracking, such as spyware, deep-packet inspection, smart cameras, facial recognition, sensors and predictive analytics. For states and state-like actors, the aims of surveillance can include control, repression or the furtherance of armed conflict or security-related objectives linked with national security, counter-terrorism or migration flow.

Digital surveillance can also be motivated by commercial interests and conducted and enabled by private entities, such as social media companies, ad technology companies, data aggregators and vendors and service providers (e.g. internet and telecommunication providers).

159 See [Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance](#); [Border Management and Human Rights](#).

160 See, for instance, ICRC, [ICRC Position On Autonomous Weapon Systems](#).

161 See, for instance, ICRC, [Algorithms Of War: The Use Of Artificial Intelligence In Decision-Making In Armed Conflict](#).

162 For further resources, see [The Right to Privacy in the Digital Age](#); [Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies](#); [Including Peaceful Protests](#); [Surveillance And Human Rights – Report Of The Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression](#); [Aiding Surveillance](#); [Biometrics In The Humanitarian Sector](#); [Digital Technologies as a Means of Repression and Social Control](#).

163 See, for instance, ICRC, [The Humanitarian Metadata Problem: “Doing No Harm” in the Digital Era](#).

The use of these technologies in armed conflict and other situations of violence, and the misuse of data and information collected, raises concerns about affected populations' rights, safety and dignity. Moreover, it is often difficult for protection actors and others to know whether their devices, networks or systems have been compromised or digitally surveilled and whether information has been used against them.

Key concerns include:

- **Undermining fundamental rights.** Digital surveillance may threaten or interfere with the right to privacy, which is an enabler for the enjoyment of other fundamental rights, such as freedom of expression, peaceful assembly and participation. It may also lead to the violation of other rights such as those of refugees and detainees, and of the sanctity of humanitarian infrastructure/data. It may have considerable chilling effects on how people exercise their rights.
- **Enabling other harmful practices.** Forms of digital surveillance, such as profiling, can enable other forms of harm to affected populations such as arbitrary targeting, arrests, detention, torture, persecution, doxing, discrimination, sexual or gender-based violence and other ill-treatment that can affect their dignity and safety. Digital surveillance may also pose threats to people's livelihoods such as having their identity or assets stolen, being denied access to essential or humanitarian services, being commercially exploited or suffering from psychological effects from the fear of being under surveillance. Moreover, it can threaten fairness by potentially leading to biased data collection and analysis, which may lead to unfair treatment of certain groups. Meanwhile, transparency can be compromised as surveillance operations are often not openly disclosed, leaving individuals unaware that their personal data are being processed.
- **Misusing protection data and obstructing protection work.** Digital surveillance of or via protection actors, and the interception of protection data, including by access and lawful request to third parties or illegitimate access attempts, for non-protection purposes, may undermine trust in the affected protection organization, their operations, their credibility and their ability to maintain access to conduct protection activities. It may also obstruct or threaten the impartial, neutral and independent nature of certain protection action.

Militarization of the digital spaces and civilian involvement.¹⁶⁴

Civilians and private actors are becoming increasingly involved in armed conflict and other situations of violence via digital tools, whether or not they are located in the area concerned. Activities include providing digital infrastructure and services to armed conflict actors, crowdsourcing satellite imagery for intelligence, documenting and notifying conflict events and related abuses and engaging and amplifying narratives on social media. Digital communication tools enable the formation, training and coordination of large numbers of people for cyber operations, including operations against civilian targets. They make it increasingly easy for individuals to be involved in or support military operations, such as by repurposing civilian apps for military use. Certain stakeholders encourage or tolerate such practices, either overtly (e.g. by enacting or dispensing legal frameworks) or covertly (e.g. by coordinating their activities).

Key concerns include:

- **Eroding the principle of distinction.** Such behaviour is not only expanding military influence/reach towards civilian spaces but is also fostering the civilian involvement in armed conflict. This may erode the principle of distinction and blurs the line between civilians and combatants, to the detriment of civilians. It also raises concerns related to IHL and IHRL.
- **Harmful consequences.** These activities may bring civilians closer to the conduct of military operations. This creates the risk of exposing them and their families to serious harm, such as being targeted, having their property destroyed, being detained or even being killed. They may also prompt false accusations and suspicions that lead to further harm, to certain liabilities and to the loss of protection from attack and of related safeguards.

¹⁶⁴ For more resources, see [Civilianization of Digital Operations: A Risky Trend](#); [Countering the Erosion of the Principle Of Distinction on the Digital Battlefield](#).

ANNEX 3: GLOSSARY FOR CHAPTER 8

| TERM | DEFINITION |
|------------------------------|--|
| digital risk | A protection risk enabled through the use of digital technologies. |
| digital technology | An information or communication technology, system, tool or device that uses binary language and data. |
| tech company | A company that provides digital platforms, services or infrastructure, including cyber security services. This includes internet service providers. |
| cyber operation | An operation against a computer, computer system, computer network or other connected device through digital means. |
| harmful information | Information that could lead to physical or psychological harm to people during armed conflict or other situations of violence. Harmful information includes, but is not limited to, misinformation, disinformation, malinformation, hate speech and other forms of information that consist of or encourage a violation of IHL or IHRL or that undermine warring parties' ability to respect these international legal norms. |
| information operation | The use of information and communication technologies or other digital means to influence the perception, motives, attitudes or behaviour of adversaries or civilian populations to achieve political and military objectives. |
| internet shutdown | An internet shutdown or an internet blackout is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information. ¹⁶⁵ |

¹⁶⁵ Access Now, [The Language Of Internet Shutdowns: A Glossary Of Terms](#).



9. ENSURING PROFESSIONAL CAPACITY

Ensuring relevant capacities and competencies

- S** 9.1 Protection actors must identify and address gaps in their capacity to carry out protection activities and achieve protection outcomes.
- G** 9.2 Protection actors should secure sufficient resources to support their protection activities at the level and for the duration of their commitment.

Staff training

- S** 9.3 Protection actors must ensure that their staff are adequately trained and have the requisite expertise and capacities.
- S** 9.4 Protection actors must adopt current practices and guidelines of relevance to their protection activities.
- G** 9.5 Protection actors should ensure a conducive learning environment, encouraging protection training, on-the-job application and continuous learning.

Managing staff safety

- S** 9.6 Protection actors must minimize the risks to which their staff (including volunteers) and partners are exposed.

Ensuring professional and ethical conduct by staff

- S** 9.7 Protection actors must adopt an organizational code of conduct and ensure compliance with it.

INTRODUCTION

This chapter deals with the internal processes, competencies and capacities necessary for humanitarian and human rights actors conducting protection work during armed conflict and other 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 objectives, formulate plans for their realization, ensure the requisite means and then implement the plans. While the mandates and mission statements of protection actors express broad organizational goals, operational objectives and plans of action make more specific commitments in a given operational context. For these planning tools to be relevant, the protection actor must have the capacity and expertise to meet those commitments. This chapter emphasizes the need to ensure adequate human resources.

Many protection actors operate using transnational structures. This requires them to ensure consistency of approach and consistent programme quality across these structures, in all the locations where they operate. 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, which includes providing training, developing best practices, managing security and clarifying the conduct expected.

ENSURING RELEVANT CAPACITIES AND COMPETENCIES

S

9.1 Protection actors must identify and address gaps in their capacity to carry out protection activities and achieve protection outcomes.

Protection work is staff-intensive and demands a range of technical competencies. The results of protection work frequently depend on the accuracy of the problem analysis, the precision of subsequent evidence-based advocacy, the strength of staff interpersonal skills and emotional literacy and the consistency of the organization's practice. Those responsible for providing technical advice or for implementing protection activities must be versed in the concepts, approaches and methodologies of protection work and familiar with the legal frameworks applicable, including IHL and IHR. 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 protection needs of populations at risk requires different types of expertise, in areas including:

- 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 is required in the fields of:

- communication
- fact-finding
- interviewing
- intercultural dialogue
- writing, editing and formatting reports

- negotiation
- advocacy
- contextual and political analysis
- law
- data protection
- security management
- statistics
- coordination.

Despite the importance of the specialized skills listed above, organizations still need generalist or all-rounder staff, who have an overview of the various specialist portfolios and can integrate them into a coherent, strategic approach.

In addition to having staff who are directly involved in protection activities, protection actors must build a baseline level of protection capacity among those staff who contribute to protection outcomes, whether through assistance, public communication or governance and leadership (see also Chapter 1 on leadership).

Protection actors must undertake regular and systematic assessments of their professional competencies and those of their teams. This should enable timely identification of gaps and allow organizations to adjust activities or fill gaps in knowledge and skills.

G

9.2 Protection actors should 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 to fulfil their objectives and strategy (see Chapter 3). Before launching any response, they should endeavour to secure resources for an adequate period of time.

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 still protection needs, while avoiding resource-driven programming.

However, there are obvious limitations to this approach: for example, multi-annual funding is seldom obtainable, while seemingly secure funding can dry up suddenly and unexpectedly.

As far as possible, protection actors should plan for such shortfalls and analyse their potential impact on the affected population and implementing partners. When the risk of a shortfall is high, they should take pre-emptive measures and draw up contingency plans. If an interruption is inevitable, they should alert all stakeholders as rapidly as possible. They must make operational adjustments swiftly, in concert with other actors where necessary. If they will be handing activities over to actors with the means and capacity to continue the work, all efforts must be made to minimize any negative consequences for the people at risk resulting from the shortfalls and ensuing interruption of the programme.

STAFF TRAINING

S

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

Protection work can be sensitive and often takes place in complex and fluctuating circumstances. It is the responsibility of each protection actor to ensure that its staff acquire the knowledge required to perform satisfactorily in such environments and develop and maintain the necessary skills and attitudes.

There is an ever-present risk of harming the very people a protection actor aims to help. Furthermore, protection work entails a high level of emotional labour, with the potential to degrade staff mental health. Protection therefore requires staff with appropriate expertise and competencies, including the capacity to properly care for themselves and their peers.

The demanding technical complexities and the rapid evolution of the protection sector 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 with this situation, with training as a core feature. Actors that do not have the means or the desire to develop their own comprehensive training programmes should make it a priority to facilitate access to other opportunities for their staff. They should explore partnerships in the design and delivery of training programmes, as a means of also facilitating cooperation in operations. Other options may also be useful, such as induction courses, on-the-job coaching, communities of practice and mentoring programmes.

S

9.4 Protection actors must adopt current practices and guidelines of relevance to their protection activities.

A wide range of standards and guidelines are now available on protection issues: gender-based violence, child protection, housing, land and property rights, access to justice, mine action, natural disasters, protection of the elderly and people with disabilities, etc.

The proliferation of protection references will continue. In the absence of a centralized quality control process and with nobody 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 interests 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 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 guidance, to ensure response of adequate and consistent quality in all operations.

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

G

9.5 Protection actors should ensure a conducive learning environment, encouraging protection training, on-the-job application and continuous learning.

Only a small percentage of adult learning takes place in a formal training environment. The rest occurs through peer exchange and on-the-job application of what a person has learned. Protection actors should give their staff sufficient time, space and encouragement to undertake formal learning. They should also help staff apply their learning to their work, with the support of mentoring, coaching and peer-to-peer exchanges.

MANAGING STAFF SAFETY

S

9.6 Protection actors must minimize the risks to which their staff (including volunteers) and partners are exposed.

Protection work is inherently dangerous, as it often challenges the status quo of the operational environment and may pose a threat to long-standing practices of violating human rights.

While affected populations may greatly welcome protection work, there is always the risk of an aggressive response (overt or otherwise) from duty bearers or others. Protection work also usually entails cumulative stress, the result of having to regularly confront violations and abuse and interact with victims, survivors and witnesses.

At the organizational level, protection actors have a duty of care towards their staff. They must therefore take adequate measures to minimize the risk to staff health and to mitigate the physical and mental consequences of their work.

An organizational culture in which managers, supervisors and staff are trained to understand and mitigate the potential psychological impact of protection work is essential. Mitigation measures such as frequent rotation, adequate rest, reasonable caseloads, compassionate supervision and an open dialogue on the emotional challenges of the work will help staff remain engaged in their work. Moreover, staff should be encouraged to talk about their distress and should have access to internal and external support systems, including mental health professionals. Such openness is critical for managing these risks and equipping staff to keep themselves safe in sensitive environments.

The actual risks and vulnerabilities to which protection staff are exposed obviously vary according to the context. The threats that their activities might generate must be carefully and regularly analysed. Understanding these threats – their nature, the perpetrators/sources and their motives, capacity 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, and between local/national organizations and international organizations when working with partners, is of particular importance in this analysis. The value of the knowledge, insights and analysis that a local perspective can offer in shaping an effective protection response must be weighed against the risks that national staff might face as a result of being associated with protection activities. In many cases, national staff face different – and often greater – security risks, as they, their friends and their families are part of the communities in which they work.

Certain stakeholders may perceive national staff 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. The role of national staff must be defined clearly, to minimize their exposure to risk.

If such threats arise, the exposure of national staff to circumstances, processes, people or information of a sensitive nature must be reduced, and the distinct roles of national and international staff made clear to all stakeholders.

Staff at all levels must be informed of the risks they may face. No one may be forced to participate in an activity presenting risks they are not willing to take: everyone must have the option of refusing to participate.

Protection actors must also develop clear management policies and guidelines consistent with their duty of care to staff. These guidelines will 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 must be made available to and discussed with all staff – national as well as international. Protection actors must also provide adequate training in security management.

ENSURING PROFESSIONAL AND ETHICAL CONDUCT BY STAFF

S

9.7 Protection actors must adopt an organizational code of conduct and ensure compliance with it.

Protection actors must ensure that 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 action by protection staff causes harm, intentionally or unintentionally, or generates additional risks for affected people or staff members. They also define the parameters of acceptable practice, behaviour and personal conduct.

Protection actors have endorsed a number of policy documents aimed at regulating the behaviour of staff towards affected populations. These include policies to prevent and eradicate harassment and abuse in the workplace, sexual exploitation and abuse of affected populations, with a particular focus on the heightened risk of exploitation that can arise when working with people in situations of vulnerability.

Once a protection actor has adopted a code of conduct, it must ensure compliance.

As a minimum, it must:

- make the policies available to all staff
- brief staff on their content and incorporate them in staff training
- make them available to the public (or at least those parts that relate to interaction between staff and affected people)
- ensure clear, safe and confidential reporting lines for potential breaches of the policies, both for staff and for affected people
- establish accessible monitoring and complaints mechanisms.

Such codes must also feature in the terms of reference for positions, in unit/individual work plans and in performance appraisals.

Ethics board

Ethical dilemmas may arise, the solution of which may be beyond the competence or responsibility of a single individual.

In such instances, guidance may be provided, e.g. by an ethics board, though this may be only one entity within a set of mechanisms and procedures. These mechanisms and procedures should be able not only to respond to requests but also to regularly review whether an organization has the staff support mechanisms and the tools necessary for risk analysis. Organizations should make it clear that working on the basis of standards and ethical considerations is as much an individual as an institutional responsibility.

REFERENCE MATERIAL FOR CHAPTER 9

Global Cluster Coordinator Group, [Cluster Coordination Performance Monitoring – Guidance Note](#), January 2014

Human Rights Law Centre, [Guiding Principles for Human Rights Field Officers Working in Conflict and Post-conflict Environments launched at United Nations in Geneva](#), 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](#), Geneva, 2002

ICRC/IFRC, [Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations \(NGOs\) in Disaster Relief](#), 1994

Oxfam, [Improving the Safety of Civilians: A Protection Training Pack](#), 2009

The Keeping Children Safe Coalition, [Keeping Children Safe: A Toolkit for Child Protection](#), 2011

UNHCR, [Protecting Refugees: A Field Guide for NGOs](#), 1999




Bugnion, Christian, [Analysis of “Quality Management” Tools in the Humanitarian Sector and their Application by the NGOs](#), ECHO, Brussels, 2002

Tough, A.M., *Why adults learn*, Toronto, 1968

Rothschild, Babette, *Help for the Helper: The Psychophysiology of Compassion Fatigue and Vicarious Trauma*, 2022

The ICRC helps people around the world affected by armed conflict and other violence, doing everything it can to protect their lives and dignity and to 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 reference 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 and effectively, without taking sides.

 facebook.com/icrc
 x.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, August 2024