SYNERGISE

D1.2 Ethics, legal, societal and inclusivity framework of FR operations

Date
30.04.2024

Author: Dévika Pérez Medina, Alejandro Nicolás Sánchez, Pablo Cerezo Martínez, Flavia Roteda Ruffino, Francisco J. Castro-Toledo
Organisation: PLUS ETHICS

Co-funded by the European Union

D1.2. Ethics, legal, societal and inclusivity framework of FR operations

Grant Agreement	101121321
Call identifier	HORIZON-CL3-2022-DRS-01
Project full name	SYNERGISE : A novel integrated SYstem of Systems streNgthening tEchnical and logistical capacities to ensure better Response to emerGencies by synergISticallyaddrEssing FRs capability gaps
Due Date	30.04.2024
Submission date	30.04.2024
Project start and end	01.09.2023 – 28.02.2027
Authors	Dévika Pérez Medina, Alejandro Nicolás Sánchez, Pablo Cerezo Martínez, Flavia Roteda Ruffino, Francisco J. Castro-Toledo
Lead Beneficiary	PLUSETHICS

About the document

The SYNERGISE project's D1.2 report examines and assesses the ethical, legal, societal and inclusive framework for First Responder (FR) operations. It emphasises the need to align FR activities with robust legal standards for effective disaster response. It also identifies regulatory disparities and integration barriers, with the aim of tailoring outcomes for end-users and increasing impact. The report also identifies gaps in frameworks and provides recommendations for policymakers to promote collaborative improvements in disaster risk management. This approach is critical to promoting resilience to global threats.

Document revision history

Version	Issue & Date	Reviewer name, Beneficiary short name	Date of approval
0.1	08/04/2024	PLUSETHICS	08/04/2024
0.2	12/04/2024	TNO, GB, THW	12/04/2024
1.0	29/04/2024	PLUSETHICS	30/04/2024

Acknowledgment

The project is jointly funded from the European Union's Horizon Europe research and innovation programme; State Secretariat for Education, Research, and Innovation from Switzerland, R2 Network from the United States of America, the Japan Science and Technology Agency, the Korea Ministry of Science and ICT, and the Korea Electronics and Telecommunications Research Institute.

Nature of the deliverable[1]		R

Dissemination level

PU	Public, fully open. e.g., website	✓
SEN	Sensitive, limited under the conditions of the Grant Agreement	
CL	Classified information under the Commission Decision No2015/444	

[1] Deliverable types:
R: document, report (excluding periodic and final reports). DEM: demonstrator, pilot, prototype, plan designs.
DEC: websites, patent filings, press and media actions, videos, etc. OTHER: software, technical diagrams, etc.

Table of contents

List of tables

Abbreviations

AI	Artificial Intelligence
BDSG	*Bundesdatenschutzgesetz* (Federal Data Protection Act) - Germany
BMBF	*Bundesministerium für Bildung und Forschung* (*Federal Ministry of Education and Research*) - Germany
CBDRM	Community Based Disaster Risk Management
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CSO	Civil Social Organization
DRR	Disaster Risk Reduction
EC	European Commission
ERCC	Emergency Response Coordination Center
EU	European Union
FAIR	Findable, Accessible, Interoperable, Reusable
FR	First Responder
GDPR	General Data Protection Regulation
GNDR	Global Network of Civil Society Organizations for Disaster Reduction
IFAFRI	International Forum to Advance First Responder Innovation
IHL	International Humanitarian Law
IPCC	Intergovernmental Panel on Climate Change
KED	*Κέντρο Διαλειτουργικότητας* (Interoperability Center) - Greece
LGBTQI	Lesbian, gay, bisexual, transgender, queer and intersex
MCDA	Military and Civil Defence Assets
NATO	North Atlantic Treaty Organization
SAMFI	(Cooperation Group for Information Security) - Sweden
UKE	*Urząd Komunikacji Elektronicznej* (Office of Electronic Communications) - Poland
UN	United Nations
UNDRR	United Nations Office for Disaster Risk Reduction
UNFCCC	United Nations Framework Convention on Climate Change
VNG	*Vereniging van Nederlandse Gemeenten* (Association of Dutch Municipalities) - The Netherlands

Executive summary

'D1.2. Ethical, legal, societal and inclusivity frameworks of FR operations' represents a central effort within the SYNERGISE project to meticulously outline and analyse the ethical, legal, societal and inclusivity frameworks relevant to First Responder (FR) operations. This comprehensive review is essential to improving the efficiency, effectiveness and inclusivity of FR operations in an increasingly complex global disaster risk management landscape. This report underscores the multiple challenges and opportunities that lie ahead in optimising FR operations, and highlights several key areas of interest and action.

Firstly, the analysis of European and international regulations relevant to Disaster Risk Reduction (DRR) policy from a general perspective has highlighted the intricate web of legal and ethical standards that govern DRR operations. It reveals a landscape characterised by both robust frameworks and areas requiring further refinement. The importance of aligning FR operations with these regulations cannot be overstated, as it ensures that disaster response activities are not only effective, but also meet the highest standards of ethical and legal accountability.

The report delves into the specifics of regulatory frameworks and guidelines from various international bodies such as the United Nations, the European Union, and other global alliances which affect FR operations. It examines how these bodies' policies and guidelines intersect with national laws to either enable or hinder effective disaster response. In particular, in addressing the complexities of DRR, international and European frameworks largely focus on legal, ethical, inclusiveness, and social dimensions and establish a broad set of standards designed to guide the policies and practices of DRR, ensuring that they are effective, fair, and respectful of human rights and societal norms. The following briefly summarises the common position of the documents discussed above:

- *Legal dimension* underscores the necessity for DRR initiatives to align with higher legislative standards, such as international humanitarian laws and national privacy regulations. This legal emphasis ensures that efforts in disaster management adhere to the principles of jurisdiction, rights, and obligations, thus safeguarding the interests of individuals and communities while fostering a structured approach to emergency responses.

- *Ethical dimension* places a strong focus on transparency, accountability, and justice. These frameworks advocate for DRR policies that promote ethical conduct, ensuring that all operations are carried out with integrity and fairness. The emphasis on ethics helps maintain public trust and confidence in disaster response activities, highlighting the importance of ethical decision-making in scenarios that often involve vulnerable populations and high-stakes situations.

- *Inclusiveness dimension* notes as essential that disaster risk management practices consider and actively include diverse groups, particularly marginalised and vulnerable communities. Frameworks call for equitable participation and accessibility in the development and execution of disaster responses, ensuring that no one is left behind in times of crisis. This focus helps to tailor responses to the needs of all segments of the population, enhancing the effectiveness and equity of interventions.

- *Social dimension* examines the broader impact of disaster risk management on society. They emphasise the need for policies that not only respond to immediate disasters but also contribute to long-term societal resilience. This includes fostering community participation, enhancing communication and transparency, and ensuring that disaster risk management efforts are adaptable to different social contexts and needs.

While these international and European guidelines provide a robust basis for managing legal, ethical, inclusiveness, and social concerns in disaster scenarios, they do not typically specify how advanced technologies should be integrated into DRR. However, the principles they advocate are crucial for guiding the development and implementation of technological solutions. Therefore, in linking these broader guidelines to the specific technological solutions proposed by the SYNERGISE project, the standards set forth are essential for guiding their ethical, legal, inclusive, and socially responsible deployment. This connection ensures that the innovative tools and methods enhance disaster response capabilities without compromising the foundational principles of DRR. By adhering to these guidelines, technology developers and policymakers can ensure that their solutions not only advance the technical aspects of disaster response but also uphold and promote the core values of legality, ethics, inclusiveness, and social welfare. The report also assesses the alignment of SYNERGISE's technological solutions with these diverse regulatory environments, identifying areas where misalignment could potentially lead to inefficiencies or legal challenges. In particular, it describes how SYNERGISE project's solutions could address the different dimensions highlighting the necessary standards and the potential risks, gaps and limitations associated with the deployment of these technologies in FR operations. This integration ensures that the technological solutions provided are not merely about pioneering advances in disaster response but are also embedded with principles that uphold social responsibility, legal compliance, ethical integrity and inclusiveness.

Secondly, the critical examination of the regulatory frameworks of the Consortium's end users highlights the varying degrees to which current project solutions can be seamlessly integrated into different national and organisational contexts. This analysis is essential to identify specific regulatory barriers that may hinder the adoption of innovative solutions proposed by the SYNERGISE project. By assessing these national frameworks, the SYNERGISE project seeks to tailor its technological responses to align seamlessly with localised regulatory standards and cultural nuances, enhancing the effectiveness and acceptance of these tools across diverse operational contexts. This strategic analysis is fundamental in driving the project towards its goals of creating technologically adept, legally compliant, ethically sound, and socially responsible solutions for emergency response.

The document's comprehensive critical analysis also identifies potential gaps and limitations within existing frameworks and provides a roadmap for future improvements. These gaps, ranging from insufficient inclusiveness measures to outdated legislation, represent opportunities for significant progress in the way FR operations are conducted. The analysis highlights technical, regulatory, training and cooperation areas where current frameworks could be improved to ensure a more inclusive approach to DRR. Addressing these issues is critical to ensuring that DRR measures effectively address the needs of all segments of the population, especially the most vulnerable. By identifying and addressing these gaps, the project will be better able to tailor its outputs to the nuanced needs of its end-users, ensuring that its contributions are both practical and impactful. It will not only improve the immediate effectiveness of disaster response, but also contribute to the long-term resilience of communities and nations in the face of evolving global threats.

Furthermore, the development of specific recommendations for policy makers, public sector stakeholders and law enforcement agencies is perhaps one of the most important contributions of this document. These recommendations serve as a catalyst for change, encouraging the adoption of practices and policies that are more in line with today's disaster risk management challenges, taking into account ethical, legal, societal and inclusiveness considerations. By fostering dialogue around these recommendations, the document sets the stage for collaborative efforts to improve the legal, ethical, societal and inclusive dimensions of DRR operations:

Short-term:

- Workshop facilitation for the alignment of technological application with prevailing ethical and legal standards is highly advocated. Such alignment is anticipated to enhance adherence to regulations and ethical guidelines, thus mitigating legal disputes and bolstering public confidence and acceptance of disaster response measures.
- It is advisable to conduct inclusiveness assessments of disaster response strategies. Outcomes of these evaluations are expected to refine services to encompass all populations adequately, prioritizing those most at risk of exclusion, and promoting fairness in disaster response.
- Undertaking societal impact assessments for employed technological solutions is endorsed. This endeavour aims to bolster community trust and participation, optimizing resource utilization, and ensuring that emergency services resonate with public expectations and societal values.

Medium-term:

- The development of training programs dedicated to amplifying inclusivity within disaster risk reduction is recommended. These programs aspire to cultivate an environment where emergency response teams consider the diverse needs of the community, contributing to a reduction in disparities following disasters.
- Hosting workshops for policy development with a wide range of contributors is suggested. The collaborative outcome is projected to yield policies that underpin ethical and legal technology use in disaster management, leading to more adept and agile disaster risk reduction methodologies.

Long-term:

- The establishment of a permanent ethics advisory board to navigate the ethical dimensions of extended disaster risk management is suggested. This board's role is to persistently ensure that disaster risk reduction tactics remain in harmony with the progressive societal ethos, thereby sustaining ethical standards and public confidence.
- It is recommended to proactively refine legal frameworks to align with ongoing technological advancements. Pre-emptive legal adjustments are intended to support innovation and ascertain that disaster risk management approaches are efficacious and maintain legal validity.
- Advisable is the regular refreshment of inclusivity strategies. Adopting such a dynamic method is poised to align with evolving societal demographics and demands, paving the way for communities where equitable access to disaster risk management is realized for all.

In conclusion, document D1.2 of the SYNERGISE project represents a significant step forward in the quest to optimise FR operations within the ethical, legal, societal and inclusivity framework. The lessons learned from this comprehensive analysis provide a solid foundation on which to build future initiatives. As disaster risk management continues to evolve in response to new challenges, the frameworks and recommendations outlined in this document will remain an invaluable resource for all stakeholders involved in DRR operations. The way forward, as outlined in this document, involves a concerted effort to refine regulatory frameworks, embrace inclusivity and uphold the highest standards of ethical and legal responsibility. Through such efforts, the SYNERGISE project not only enhances the capabilities of first responders, but also contributes to the creation of safer, more resilient societies.

1. Introduction

'D1.2. Ethical, legal, societal and inclusivity frameworks of FR operations' aims to provide a comprehensive overview and analysis of the ethical, legal, societal and inclusivity frameworks guiding FR operations in the context of the SYNERGISE project. The project aims to improve emergency response capabilities through a synergistic approach that addresses gaps in technical and logistical capacity.

Structured to provide both broad insights and specific recommendations, the document is divided into the following sections:

- Introduction: establishes the dual focus of analysing relevant European and international regulations affecting disaster risk management policies, and critically examining the regulatory framework from the perspective of the consortium's end-users. It aims to integrate the main project solutions into their regulatory ecosystems and to develop targeted recommendations for different stakeholders.
- Analysis of the international and European regulatory framework for first responders: Dives into the ethical, legal, societal and inclusivity frameworks by reviewing key European and international regulations and guidelines that influence disaster risk management policies. It examines frameworks such as the United Nations Office for Disaster Risk Reduction Strategy, the Sendai Framework for Disaster Risk Reduction and the European Union Civil Protection Mechanism, among others, and provides a multi-level assessment based on legal, ethical, societal impact and inclusivity criteria. This analysis culminates in the advocacy of a set of standards derived from these international arenas to address the broader spectrum of disaster management issues.
- Analysis of the regulatory environment of SYNERGISE first responder end-users: through a critical analysis, it provides insights into the regulatory environment of specific countries of the Consortium's end users, including Poland, Germany, Sweden, Greece and the Netherlands, highlighting how national regulations affect FR operations and assessing the degree of compatibility and integration potential of the project's main solutions within these regulatory frameworks.
- Identification of gaps in national regulations and recommendations: focuses on identifying regulatory gaps or areas that may require further attention or improvement, and formulating targeted recommendations for a range of audiences, including policy makers, public sector stakeholders and law enforcement agencies, in order to address these shortcomings. These recommendations are intended to inform and guide efforts to improve the effectiveness and inclusiveness of FR operations within established ethical, legal, societal and inclusiveness parameters.

The document concludes with a summary of findings, and additional information. It emphasises the importance of a multi-dimensional assessment of FR policies, advocating a holistic approach that incorporates ethical, legal, societal and inclusiveness considerations into FR operations. This analysis is not only crucial for understanding the current regulatory landscape, but also aims to inform future policies and actions to improve the effectiveness of disaster response and management.

2. Analysis of the international and European regulatory framework for first responders

2.1. About this section

This section establishes the ethical, legal, societal and inclusivity frameworks by analysing the most relevant European and international regulations and guidelines applicable to disaster risk management policies.

Firstly, the international frameworks reviewed, identified as such because of their cross-regional character, are outlined below:

- United Nations Office for Disaster Risk Reduction (UNDRR) Strategy Framework 2022-2025;
- Sendai Framework for Disaster Risk Reduction 2015-2030;
- Intergovernmental Panel on Climate Change (IPCC)'s Climate Change Report 2023 Synthesis Report;
- Global Network of Civil Society Organisations for Disaster Reduction (GNDR)'s Making Displacement Safer Cookbook;
- Guidelines on the Use of Foreign Military and Civil Defence Assets In Disaster Relief ("Oslo Guidelines");
- IFAFRI Recommended Method for National Capability Gap Identification and Prioritization.

Followed by the revised European frameworks, identified by their relationship with the European Union institutions, which are detailed below:

- Decision No 1313/2013/EU on a Union Civil Protection Mechanism;
- Commission Implementing Decision (EU) 2019/570 of 8 April 2019 laying down rules for the implementation of Decision No 1313/2013/EU of the European Parliament and of the Council as regards rescEU capacities and amending Commission Implementing Decision 2014/762/EU;
- Commission Implementing Decision (EU) 2021/1956 of 10 November 2021 on the establishment and organisation of the Union Civil Protection Knowledge Network;
- Communication from the Commission to the European Parliament and the Council on the EU's humanitarian action: new challenges, same principles;
- Council Regulation (EU) 2016/369 of 15 March 2016 on the provision of emergency support within the Union;
- Council Regulation (EC) No 1257/96 of 20 June 1996 concerning humanitarian aid.

A multi-level assessment of these documents is carried out based on the following dimensions: legal, ethical, inclusiveness and societal impact. By covering these main aspects of interest comprehensively, the regulatory framework provides a holistic approach to the development and implementation of solutions for FR operations. In this analysis, specific criteria have been used as a reading guide to identify the main obligations and recommendations regarding each area. The criteria chosen for the dimensions of legal assessment, ethics, societal impact and inclusiveness have been selected to provide a comprehensive and nuanced analysis of the regulatory

frameworks governing disaster risk management policies. While some criteria may overlap between dimensions, this categorisation reflects the specific focus and distinctiveness of each dimension:

- Legal: conformity with higher legislation, data protection and privacy, respect for human rights, jurisdiction and scope, rights and obligations, enforcement and compliance mechanisms, appeal and redress procedures, protection against arbitrariness. Legal frameworks ensure the legitimacy and efficacy of disaster response actions, safeguarding individual rights and defining responsibilities within response operations.

- Ethical: transparency and accountability, equity and justice, integrity and anti-corruption, conflict of interest management, compliance and sanctions, sustainability, business responsibility, ethics education and training. Ethical considerations guide decision-making processes, promoting fairness, integrity, and responsible conduct throughout disaster response efforts.

- Social impact: explicit societal objectives, societal impact analysis, monitoring indicators, vulnerability reduction, international cooperation/coordination, community participation, flexibility and adaptability, communication and transparency. Understanding the societal impact of policies ensures that response efforts address the diverse needs of affected communities and promote resilience and well-being.

- Inclusiveness: consideration of diverse groups, accessibility, specific protection measures, equitable participation, impact and evaluation, equality of opportunity, awareness and training, collaboration with representative groups. Inclusivity fosters a more comprehensive and effective response by ensuring that all individuals and communities, including marginalised groups, have equal access to resources, support, and decision-making processes.

By thoroughly analysing the dimensions of ethics, legality, societal impact, and inclusivity within a selection of significant international and European regulations and guidelines regarding disaster risk management policies, this section aims to provide insights into the regulatory frameworks guiding response efforts. All standards established in the international framework will be taken into account in order to adapt them to the specificities of the development of technological innovations in disaster management and first responder operations. The subsequent sections of this deliverable will explore specific aspects of disaster response, leveraging the findings of this analysis to inform strategic recommendations and enhance the effectiveness and inclusivity of disaster risk management practices. Through a comparative examination of multiple regulatory approaches, we endeavour to identify best practices and emerging trends that can facilitate a deeper understanding of the complexities inherent in disaster response operations.

2.2. International frameworks

2.2.1. United Nations Office for Disaster Risk Reduction Strategy Framework 2022-2025[2]

Year	2021
Type of instrument	Manual and Guideline
Status	Non-binding

[2] The relationship between the legal framework of SENDAI and the UNDRR Strategy Framework lies in their mutual focus on disaster risk reduction. The UNDRR Strategy Framework is aligned with the general principles and objectives of SENDAI, and it draws upon the guidelines set forth in the legal framework of SENDAI to implement specific measures within the context of UNDRR activities. More information available at: [https://www.undrr.org/publication/undrr-strategic-framework-2022-2025]

2.2.1.1. Legal framework

Among the objectives of these guidelines is the quality analysis of risks in order to be able to prevent them adequately. To this end, it is specifically stated that governments and other users will support the integration of climate change and natural disaster risk reduction measures into their strategies and policies. Among the measures and actions that governments (both national and local) can take is to raise awareness of climate change and disaster risk reduction.

2.2.1.2. Ethical framework

The UN document emphasises several ethical considerations, including ethics training, transparency, equity and justice, sustainability, integrity, and anti-corruption. It outlines four accelerators aimed at enhancing disaster risk reduction (DRR) efforts: generating robust evidence and innovation, accelerating financing for DRR, scaling up communication and advocacy, and integrating DRR with the climate agenda. Additionally, it lays out four strategic objectives: utilizing quality risk information for decision-making, strengthening DRR governance, catalyzing investment and action through partnerships, and advocating for DRR as central to sustainable development.

Transparency, equity, and sustainability principles permeate the proposed policies, aiming to make them more sustainable, accessible, and inclusive for all affected populations. The document stresses the importance of leaving no one behind, mainstreaming human rights, gender equality, and the rights of persons with disabilities into DRR. Concrete actions to enhance transparency and combat corruption include establishing a global observatory for financial flows toward DRR, designing prevention bonds for vulnerable countries, reviewing national budget allocations, conducting fiscal framework robustness tests, and developing a taxonomy of economic activities that support prevention efforts.

Efforts to enhance capacity through digital platforms and information technology are highlighted, along with the recognition of the Global Platform for Disaster Risk Reduction as the forum for assessing progress on Sendai Framework implementation and advancing concerted action on disaster risk reduction, sustainable development, and climate change adaptation.

2.2.1.3. Inclusiveness framework

The document includes a section (page 16) dedicated to detailing the importance of incorporating human rights, gender equality, and the rights of disabled persons into disaster risk reduction strategies, following the Sendai Framework. This approach focuses on protecting individuals and their properties, while simultaneously promoting all human rights and sustainable development. The interaction between this framework and human rights treaties to address vulnerabilities is underscored, highlighting the work of the Convention on the Elimination of All Forms of Discrimination Against Women and the Committee on the Rights of Persons with Disabilities.

Integrating a gender perspective into risk reduction policies and practices is established as a crucial element and aligns with the Sendai Framework, which emphasises the need to understand the impact of gender norms on society and promote female leadership in disaster prevention and recovery. The UNDRR supports initiatives that not only address specific gender-based needs but also aim to eliminate underlying vulnerabilities, focusing on resilience and female leadership to achieve gender equality.

Furthermore, the essential role of disabled persons and their organisations in disaster risk reduction is recognised, in line with the Sendai Framework advocating for inclusive and accessible policies, demanding the integration of disability perspectives throughout all planning phases and promoting inclusive decision-making. The UNDRR commits to aligning with the United Nations Disability Inclusion Strategy, ensuring consideration of disabled persons in the implementation of the Sendai Framework, promoting their leadership and participation in shaping global and regional agendas.

This multidimensional approach is established in response to the goal of making disaster risk reduction inclusive, equitable, and sustainable, recognising the importance of addressing the needs and capabilities of all society sectors in disaster management.

2.2.1.4. Social framework

This framework acknowledges that humanitarian needs and societal objectives must be on the forefront of disaster risk reduction strategies: "poverty, inequity, and insecurity continue to drive disaster risk, compounding vulnerabilities and increasing its impact" (p. 3). It is these interactions between societal elements, that generate global shocks, stresses, and crises (p. 2). As pointed out several times throughout the text: "risk is systemic, interconnected and cascading" (p. 2), that is, "multi-hazard" (p. 4). This requires coordination with preventive measures in other sectors, such as climate change, regulatory frameworks, investments, humanitarian planning (p. 3, 4), through cross-sectoral dialogue (p. 13).

One of the main priorities of this strategic framework is to focus on governance coordination, providing help and support to UN Member States. To achieve it, "national and local level strategies that build resilience in the medium to long-term" are fostered (p. 3), through UNDRR's work on "strategic, impact-driven partnerships" (p. 5), especially with "regional and sub-regional intergovernmental organisations and regional economic communities" (p. 7).

Similarly, partnerships and engagement with stakeholders and civil society is pursued, within an "all of society approach" (p. 9) and a "cohesive, participatory action" (p. 10). As stated, "UNDRR will also partner with key stakeholders, including the private sector, parliamentarians, civil society, international finance institutions and the international academic and science arena to leverage specific outreach capacities and expertise areas to strengthen risk informed decision-making" (p. 5), and also with "media, youth groups and others in order to leverage their enabling power and universal reach" (p. 7). This proximity to society is also reflected in the area of communication and transparency. In particular, "UNDRR will […] highlight the additional benefits that accrue through disaster risk reduction initiatives and [...] will clearly communicate the role of UNDRR in supporting Member States and wider stakeholders". This will increase the visibility of the political importance of disaster risk reduction and mobilise citizens to demand change (p. 11).

To ensure that this framework and concrete actions are adequate to overcome future challenges that could emerge over time, UNDRR not only promotes disaster risk reduction, but also "climate change adaptation and resilience building" (p. 6), allowing "flexible funding" as an enabler to achieve the objectives (p. 9). Accountability, regular planning and reporting is one of the main drivers of these strategies (p. 5). In a pragmatic way, "UNDRR manages its operational risk through three pillars, (i) a strong accountability framework, (ii) an entity level risk register which is updated annually, and (iii) a robust monitoring and evaluation of its work programme" (p. 12).

Finally, in order to measure its impact, output indicators are put in place for each of the four strategic objectives defined in this document (p. 19-27). Regarding each of the 4 strategic objectives developed in this document, impact and success is defined, as well as what concrete key actions are needed, along some metrics and indicators for measurement (p. 28-35).

2.2.2. Sendai Framework for Disaster Risk Reduction 2015-2030[3]

Year	2015
Type of instrument	Agreement
Status	Non-Binding

[3] More information available at: [https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030#:~:text=The%20Sendai%20Framework%20for%20Disaster,Investing%20in%20disaster%20reduction%20for]

2.2.2.1. Legal framework

On the issue of Human Rights, the document points out in article 19, section III, the importance to promote and protect all human rights, including the right to development. This right consists of promoting and protecting the ability of every person to participate in, contribute to and enjoy development, including its economic, societal, cultural and political aspects.

The text also indicates the steps to be taken by national and local regional institutions in order to achieve the indications of the text. This distinction undoubtedly facilitates the distribution of tasks and obligations in order to comply more efficiently with the guidelines.

In this sense, at national or local level, the preparation, review and regular updating of natural hazards policies, plans and programmes as well as the investment and development of multi-sectoral forecasting and early warning systems are advocated. Also relevant is the development of guidelines for post-disaster reconstruction preparedness, such as land-use planning and improved structural standards. Other issues include the review and strengthening of national laws and procedures for international cooperation, based on the Guidelines for International Cooperation and National Regulations for International Disaster Relief Operations and Initial Disaster Relief Operations.

At the global and regional level, the actions to achieve the aforementioned challenges are different. The creation of codes, operational guides and other guidance instruments is proposed to improve coordinated action. In the same vein, the strengthening of international mechanisms is also highlighted, specifically the International Recovery Platform. It also agrees with national and local efforts to train operators and volunteers in disaster response. Finally, most of the actions at this level are based on general support in terms of resources and cooperation to facilitate the resolution of risk situations.

2.2.2.2. Ethical framework

Throughout this document, numerous ethical issues are addressed, such as sustainability, equity and fairness, transparency, accountability, business responsibility and training. All these principles are reflected on in the first sections on expected results and guiding principles (sections II and III respectively). For this reason, for example, in the second section, point 16 states the following regarding sustainability: "The substantial reduction of disaster risk and disaster losses in lives, livelihoods, health, economic, physical, societal, cultural and environmental assets of individuals, businesses, communities and countries", (p. 12).

Similarly, point 17 proposes as an objective, among others, the following: "To prevent the occurrence of new and reduce existing disaster risks by implementing integrated and inclusive economic, structural, legal, societal, health, cultural, educational, environmental, technological, political and institutional measures that prevent and reduce exposure and vulnerability to hazards, increase preparedness for response and recovery, and thereby strengthen resilience. On the other hand, reference to the guiding principles set out in section III makes clear the importance of international collaboration, or the sharing and exchange of information between different territories as set out in section III(g) when it states: "Disaster risk reduction requires a multi-hazard approach and inclusive decision-making informed by risk identification and based on the open exchange and dissemination of disaggregated data, including by sex, age and disability, as well as easily accessible, up-to-date, understandable, science-based and non-confidential risk information, complemented by traditional knowledge." This has a direct bearing on the principles of transparency, sustainability and, related to training and learning. At the same time, further elaborating on this issue, paragraph h) states: "The development, strengthening and implementation of relevant policies, plans, practices and mechanisms should seek coherence, as appropriate, between the agendas for sustainable development and growth, food security, health

and safety, climate variability and change, environmental management and disaster risk reduction. Disaster risk reduction is essential to achieve sustainable development".

This has a direct bearing on the above-mentioned principles, especially the one related to sustainability. Finally, in section IV, (p. 14), a number of priorities for action are set out, namely: "Priority 1: Understand disaster risk. Priority 2: Strengthen disaster risk governance to manage disaster risk. Priority 3: Invest in disaster risk reduction for resilience. Priority 4: Increase disaster preparedness for effective response and to "build back better" in the areas of recovery, rehabilitation and reconstruction", (p. 14). Each of these priorities has in its more concrete developments an underlying ethical concern. Then, for example, in Priority 1, paragraph 23, it states: "Disaster risk management policies and practices should be based on an understanding of disaster risk in all its dimensions of vulnerability, capacity, exposure of people and assets, hazard characteristics and environment", (p. 16). This highlights the importance of prior consideration of principles related to equity and justice and the importance of companies and agencies undertaking such actions being committed to a range of actions that impact on the well-being of those affected. With regard to Priority 2, it is also important to note the relevance of conflict-of-interest management at national, regional and global levels. Finally, Priority 4, (p. 21), aims to reduce the impact on people and property by enhancing "disaster preparedness for effective response and « «build back better» in the areas of recovery, rehabilitation and reconstruction". This is envisioned by a diverse set of actions that provide a clear outline of what the guiding principles of the Sendai Framework's framework for action should be (p. 21-22):

- Providing continuous training in the different areas related to natural disasters and taking lessons learned from past disasters;
- Promote the further development and dissemination of tools such as standards, codes, operational guides and other guidance tools;
- Strengthening international mechanisms, such as the International Recovery Platform, for the exchange of experience and learning among countries and all relevant actors.
- Eventually turning disaster risk reduction into preparedness and ensuring that sufficient capacity is in place for effective response and recovery at all levels.

2.2.2.3. Inclusiveness framework

The Sendai Framework for Disaster Risk Reduction 2015-2030 includes a wide range of recommendations on inclusivity, among which particularly stand out:

A broad and people-centred preventive approach, requiring practices to be multidisciplinary, multisectoral, inclusive, and accessible to be efficient and effective in achieving disaster risk reduction (p. 10).

Prevention of new risks and reduction of existing ones through integrated and inclusive economic, structural, legal, societal, health, cultural, educational, environmental, technological, political, and institutional measures that decrease exposure and vulnerability to disasters, increase preparedness for response and recovery, thus strengthening resilience (p. 11).

Engagement and partnership of the whole society, involving empowerment and inclusive, accessible, and non-discriminatory participation, with special attention to those most affected by disasters, especially the poorest; and the integration of a gender, age, disability, and cultural perspective in all policies and practices, promoting the leadership of women and youth and improving organised voluntary work (p. 12).

Application of a multi-hazard approach and inclusive decision-making based on open exchange and dissemination of disaggregated data by sex, age, and disability, as well as updated, comprehensible, science-based risk information, complemented by traditional knowledge (p. 13).

Promotion of community participation integrated with livelihood enhancement programmes and access to basic health, nutrition, housing, and education services, seeking durable solutions in the post-disaster phase and empowering those most affected, to strengthen the design and implementation of inclusive policies and societal safety-net mechanisms (p. 19).

Collaboration of civil society, volunteers, and community-based organisations with public institutions to provide specific knowledge and pragmatic guidance in the development of normative frameworks and plans for disaster risk reduction; participate in the implementation of plans and strategies; contribute to and support public awareness and education on disaster risk; and advocate for resilient communities and an inclusive and all-of-society disaster risk management (p. 23).

Good practices by the media, which are given an active and inclusive role at all levels, contributing to public awareness and disseminating risk information in a clear, comprehensible, and accessible manner, in cooperation with national authorities, supporting early warning systems, and promoting a culture of prevention and strong community involvement in educational campaigns and public consultations (p. 24).

2.2.2.4. Social framework

The Sendai Framework for Disaster Risk Reduction 2015-2030, extensively highlights the following key areas related to societal impact concerns, identifying problems and ways to address them:

It explicitly reaffirms that one of its objectives and expected outcomes is “the substantial reduction of disaster risk and losses in lives, livelihoods and health and in the economic, physical, societal, cultural and environmental assets of persons, businesses, communities and countries (art. 16)”. A strong focus is placed on protecting societal and cultural spheres and building resilience “within the context of sustainable development and poverty eradication” (art. 2). Therefore, societal impact analyses are stated as necessary, and are clearly established throughout the text. Article 18 states that “to support the assessment of global progress in achieving the outcome and goal of the present Framework, seven global targets have been agreed”. Also, art. 24 (b) "to periodically assess possible sequential effects"; art. 30 (c) "taking into account economic, societal, structural, technological and environmental impact assessments". Each of this global target has been divided into several indicators (38 in total) for monitoring and tracking progress of the Sendai Framework implementation.

Vulnerability reduction is also considered an essential issue: "it is urgent and critical to anticipate, plan for and reduce disaster risk in order to more effectively protect persons, communities and countries, their livelihoods, health, cultural heritage, socioeconomic assets and ecosystems, and thus strengthen their resilience" (p. 5). An integrated, coherent across all sectors, multidimensional and multi-hazard strategy is recurrent throughout the text, as art. 6 displays: “more dedicated action needs to be focused on tackling underlying disaster risk drivers”.

Cooperation and coordination between mechanisms and institutions as well as communities and businesses are at the forefront and remain pivotal (art. 8). Technology and information sharing, international voluntary mechanisms for monitoring, and assessment and nationally compatible regional multi-hazard early warning mechanisms, are examples of how cooperation is promoted in this framework. Also, community participation is described as necessary in article 7: "there has to be a broader and a more people-centred preventive approach to disaster risk [...] including women, children and youth, persons with disabilities, poor people, migrants, indigenous peoples, volunteers, the community of practitioners and older persons [...], public and private sectors and civil society organisations, as well as academia and scientific and research institutions''. That implies a “full and meaningful participation of relevant stakeholders at appropriate levels'' (art. 14). In particular, the text emphasises the importance of communication and transparency with civil society in disaster risk reduction efforts. Article 19 (k) highlights the need for increased public education and

awareness of disaster risk during post-disaster recovery. Article 24 (c, d, e, f, m) establishes key measures, including developing and disseminating location-based disaster risk information, promoting national strategies for public education and awareness campaigns, etc.

In addition, the adaptability of this UN framework to changes, in particular climate change and demographic changes, is frequently mentioned. Article 25 (b) points out that climate change scenarios shall be taken into account, while investing in (i) innovation and technology for long-term research and development, as stated in art 24 (k), in order to overcome new gaps, obstacles and challenges.

2.2.3. Intergovernmental Panel on Climate Change (IPCC)'s Climate Change Report 2023 Synthesis Report[4]

Year	2023
Type of instrument	Report
Status	Non-binding

2.2.3.1. Legal framework

The document outlines the adaptations and mitigations needed to meet the challenges posed by climate change. At the legal level, cities must include climate change impacts and risks in their action plans. For example, the creation of appropriate building and construction plans for these risks.

The effectiveness of multi-level governance for mitigation, adaptation and risk management is also noted. Existing vulnerabilities can be reduced through legislation and policy implementation. Expanding and enhancing the use of regulatory instruments improves mitigation outcomes in line with the national circumstances of each state.

Therefore, effective governance of climate issues, taking advantage of regulatory instruments and the multilevel nature of our environment, helps to improve the objectives, priorities and integration of the actions identified for combating climate change.

On the other hand, special mention is made in the development of these policies of the protection of rights of indigenous people, as a key right to be taken into account.

2.2.3.2. Ethical framework

In this document, the ethical items that clearly stand out are those related to sustainability, equity and justice, and transparency. Special emphasis is placed on the importance of carrying out actions that are committed to the environment and that prioritise risk reduction, equity and justice in decision-making and interdependence.

These principles are reflected in the assumptions made in the document itself when it acknowledges the interdependence of natural elements (climate, ecosystems, biodiversity) and social ones (human societies). Also, when it recognises their linkages (including concepts such as sustainable development, human well-being, adaptation to climate change, etc.), and the increasing diversity of actors in climate action etc (p. 3). The principles dedicated to the above-mentioned issues reappear strongly on p. 30, section C.3.8 when setting out the recommendations on the policies to be implemented: "Policy mixes that include weather and health insurance, societal protection and adaptive societal safety nets, contingent finance and reserve funds, and universal access to early warning systems combined with effective contingency plans, can reduce vulnerability and exposure of human systems. Disaster risk management, early warning systems,

[4] More information available at: [https://www.ipcc.ch/report/ar6/syr/]

climate services and risk spreading and sharing approaches have broad applicability across sectors. Increasing education including capacity building, climate literacy, and information provided through climate services and community approaches can facilitate heightened risk perception and accelerate behavioural changes and planning".

2.2.3.3. Inclusiveness framework

This document states that climate change has caused widespread adverse impacts and related losses and damages to nature and people, which are unevenly distributed across systems, regions, and sectors (p. 51). As a consequence, economic damages due to climate change have been identified in climate-exposed sectors such as agriculture, forestry, fishery, energy, and tourism, impacting individual livelihoods. The destruction of homes and infrastructure, and the loss of property and income, human health, and food security, with adverse effects on gender and societal equity are highlighted as some of the main consequences (p. 51).

A section titled "Equity and Inclusion in Climate Change Action" (p. 101) is also included, referring to the following goals: Prioritising equity, climate justice, societal justice, inclusion, and just transition processes.

It advocates for increased support for regions and people with the highest vulnerability to climatic hazards, the integration of climate adaptation into societal protection programs to improve resilience, aiming for intensive emission consumption, including changes in behaviour and lifestyle, with co-benefits for societal well-being.

Lastly, the document emphasises the integration of governance systems and decision-making from an inclusive perspective.

2.2.3.4. Social framework

In their Climate Change 2023 Synthesis Report, the IPCC addresses the following societal aspects regarding DRR:

Firstly, the observed changes in climate extremes are meticulously examined, emphasising their profound impact on human well-being and livelihoods. Vulnerable communities are disproportionately affected by climate change, facing increased risks of food insecurity, water scarcity, and infrastructure damage. Addressing these disparities and protecting the societal fabric of society is a central focus of the report.

However, maladaptation is also a critical concern raised in the reports, where certain mitigation or adaptation strategies inadvertently worsen societal inequalities and decrease ecosystem resilience. Ambitious mitigation pathways may bring disruptive changes, necessitating careful consideration of distributional consequences. There's a caution against actions that focus solely on short-term gains, which may lead to long-term vulnerabilities. Flexible, multi-sectoral, and inclusive planning and implementation of adaptation actions are recommended to avoid maladaptation and achieve sustainable outcomes.

Despite increasing implementation of adaptation measures, vulnerability reduction remains fragmented and uneven across regions and sectors. The reports stress the escalating risks posed by compound and cascading climate-related hazards, advocating for flexible, holistic and long-term adaptation strategies. Effective adaptation options include cross-sectoral measures such as agriculture innovation, sustainable land management approaches, early warning systems and capacity building, among others building synergies with other aspects of sustainable development.

Finally, these documents set the heart of effective disaster risk management and climate action in international cooperation. The reports underscore the indispensable role of coordinated efforts in

enabling the transition towards climate-resilient development (at a sub-national, national and international level), and when decision-making processes, finance and actions are integrated across governance levels, sectors, and timeframes. Enhanced cooperation, particularly in institutional and legal frameworks, finance, technology transfer and capacity building, is deemed essential. In the same vein, cooperation with civil society and meaningful engagement of diverse stakeholders can provide a wealth of knowledge and cultural perspectives, facilitating resilience development and socially acceptable changes. For instance, public awareness is identified as a driving force behind climate action, leading to the integration of adaptation measures into policy frameworks, the mobilisation of finance flows, and the potential increase in education, capacity building, and information that can facilitate heightened risk perception and accelerate behavioural changes and planning.

2.2.4. Global Network of Civil Society Organisations for Disaster Reduction (GNDR)'s Making Displacement Safer Cookbook[5]

Year	2007
Type of instrument	Organisation
Status	Non-binding

2.2.4.1. Legal framework

In the context of displacement management, it is essential to recognise that government authorities play a crucial role in preventing and resolving this issue, although they often face limitations in capacity and resources at the local level. To address this situation, it is crucial to initiate early dialogue with authorities to encourage their engagement and prioritise the needs of displaced persons. In this regard, community leaders and Civil Society Organizations (CSOs) play a fundamental role as they can act as intermediaries between the displaced community and government authorities, building trust and advocating for the rights of this vulnerable population.

To achieve an effective response, collaboration and coordination among different actors, including local authorities, CSOs, and other relevant stakeholders, are suggested. This involves partnering in the provision of services and programs, which can maximise the impact of limited resources available. A coordinated approach facilitates the identification of synergies and prevents gaps in service provision. Additionally, it is crucial to jointly develop a civic engagement platform between government authorities and displaced persons. This process allows for the discussion of both immediate and long-term needs, as well as addressing the risk factors contributing to displacement. CSOs can play a key role in this process by supporting the active participation of displaced persons in decision-making and promoting greater inclusion on the government agenda.

2.2.4.2. Ethical framework

With regard to the ethical dimension, throughout the "Making Displacement Safer Cookbook", there are several references to ethical items such as: transparency and accountability, equity and justice, integrity and anti-corruption and, finally, sustainability. Firstly, transparency is one of the fundamental pillars on which the document is based. For example, when mentioning key approaches, it states that "rights-based solutions include four fundamental principles: meaningful and inclusive participation and access to decision-making; non-discrimination and equality; accountability; and transparency and access to information supported by disaggregated data" (p. 13). Thus, in order to ensure the ethical and correct functioning of the actions that are being carried out by states or different organisations, it must be done in such a way that information can be accessible and there can be accountability.

[5] More information available at: [https://www.gndr.org/making-displacement-safer-cookbook/].

The responsibilities of government authorities also include that they should "promote data collection and monitor advocacy, accountability and evidence-based programming" and that they should act "with transparency in the implementation of their activities and the allocation of budgets within the community" (p.16). In the same way, equity and justice appear as another of the fundamental pillars of any action aimed at addressing the disasters that affect people. Then, one of the main elements of action must be the inclusion and equality of people. In this sense, as mentioned, the main approaches should be based on “participation, inclusion, whole of society and human rights" (p. 12). It is also highlighted that “not only should gender equality be ensured, but also the participation of underrepresented and marginalised groups should be prioritised, including people living with disabilities, younger people, older people, those in the LGBTQI community and others”. With reference to integrity and anti-corruption, although there is no explicit mention of the different mechanisms and bodies that should be in charge of these issues, there is a need for a commitment to effective funding that is useful for local communities and bodies. In this respect, in relation to effective governance, it is mentioned that where possible "effective financing for preparedness, mitigation, response and adaptation is supported". Finally, it is the principle of sustainability that carries the most weight throughout the document.

In the first instance, one of the main recommendations made is to "work to integrate processes and actions that address climate change, sustainable development..." and to "prioritise addressing economic risks and mitigating hazards, taking into account future displacement, to reduce the number of people in protracted displacement" (p.8). The principle of sustainability is also expressed in the search for durable solutions which can be achieved through sustainable reintegration in the place of origin or sustainable local integration among others. Finally, sustainability is also captured in point 4, (p.16) when different principles for "rebuilding livelihoods and resilience" are set out, for example through strengthening skills and entrepreneurship, or developing activities at the local level for income generation and community development.

2.2.4.3. Inclusiveness framework

In the various documents issued by the GNDR, it is possible to find not only definitions affecting different areas that can be included in the category of inclusivity but also some more concrete measures established to ensure their implementation in the diverse activities that countries undertake in relation to disaster risk reduction. The document places particular emphasis on situations involving migration and human displacement. It states that displaced persons (p. 5) often settle in urban areas in high-risk informal settlements, facing challenges such as isolation, exclusion, and discrimination, and lacking access to basic services, which increases their disaster risk. It is highlighted that displaced persons are rarely consulted in the design of policies to reduce disaster risk, lack access to financial resources and timely information, and are often excluded from decision-making.

In terms of societal inclusion (p. 8), the importance of including all societal groups in the decision-making process is emphasised, ensuring that the perspectives of minority or marginalised groups are considered. This involves identifying marginalised groups before starting projects so they can participate from the beginning, defining clear roles for all actors with a decision-making role for community representatives, creating safe spaces for societal groups to express their concerns, and lobbying local leaders to include inclusive plans and budgets. Inclusion is seen as adopting an approach that views marginalised groups as providers of knowledge and human resources.

Furthermore, the inclusive approach (p. 13) underscores the need to ensure that all community members have the opportunity to participate and contribute to collective efforts, which may require additional efforts, such as altering meeting times or locations. Gender equality and the participation of underrepresented and marginalised groups should be prioritised, including people with disabilities, the youth, the elderly, members of the LGBTQI community, and displaced persons from all societal, ethnic, class, gender, age, and backgrounds, identifying them and including them from

the start of any initiative with appropriate societal protection or inclusion mechanisms to promote their active participation.

Regarding cultural inclusion (p. 11), the benefits of community-based disaster risk management and the creation of a common sense of responsibility towards resilience building are recognised. This includes sensitising local political leaders, promoting the role of communities in disaster risk management at national and regional events, and encouraging the inclusion of marginalised groups in disaster risk governance. Cultural changes aim to increase family cohesion, mutual support among marginalised groups and government authorities, and alter perceptions of the roles and capabilities of women.

2.2.4.4. Social framework

The Global Network of Civil Society Organisations for Disaster Reduction, addresses in its various resources the following societal aspects regarding community-based disaster risk management (CBDRM) and people displacement as a potential consequence of disasters, among other causes:

One of the societal objectives of this network is to contribute to the substantial reduction of disaster risk losses in lives, livelihoods and assets for displaced populations in urban areas, thus contributing to Sendai Framework targets. Specific challenges fuel its purpose, such as access to housing and basic provisions and service, lack of infrastructure, exposure to natural hazards and poverty. Other societal objectives represent increasing co-creation and accountability. The network recognises that the response to displacement caused by disasters is often short-term and lacks consideration for the needs of displaced populations. Displaced individuals face numerous challenges, including unawareness of risks in new locations, limited access to services, lack of societal networks, discrimination, limited economic opportunities, mental health issues, conflict, among other challenges. To address them, recommendations are made for coherent approaches, durable solutions, and effective governance. This includes integrating climate change, sustainable development, and displacement risk, prioritising economic risks and hazard mitigation, and promoting community engagement and preparedness. The objective is to integrate village risk management plans into local development policies, in order to build effectiveness in local capacities to cope with disasters, to ensure community's ownership and to include CBDRM in policies and plans promoting synergies, etc.

Community resilience is one of the main pursued outcomes of this network, and that is understood to be achieved through community and stakeholders' participation, to bring the needs of displaced populations to the forefront. It is recommended to continuously and meaningfully engage the community in learning, design and decision-making processes: displaced persons, community members, relevant tiers of government, civil society groups and organisations and the private sector. Fostering cohesion, promoting integration, supporting advocacy to rights, including media campaigns to help being heard, allowing reporting, recognising informal structures as channels for effective engagement, defining roles, among others, are ingredients to fulfil these approaches.

Permanence and adaptiveness are considered crucial for sustainable CBDRM. This involves ensuring that risk management activities continue after external support ends, promoting financial mobilisation and behaviour change within communities. Additionally, project activities must be flexible to respond to changing conditions, with roles designated for monitoring, reporting, and encouraging integration of innovative thinking into traditional practices.

Lastly, transparency is emphasised as a major element for the organisation, supported by a rights-based approach that enhances accountability and access to information. This includes promoting data collection and monitoring, conducting participatory auditing, and creating transparent systems for budget allocation. Government authorities and other actors are encouraged to be transparent in their activity implementation and budget allocation within communities, fostering trust and cooperation with displaced populations.

2.2.5. Guidelines on the Use of Foreign Military and Civil Defence Assets In Disaster Relief ("Oslo Guidelines")[6]

Year	2007
Type of instrument	Guidelines
Status	Non-Binding

2.2.5.1. Legal framework

The document includes some obligations to the state affected by the disaster with respect to the Military and Civil Defence Assets (MCDA). According to these guidelines, MCDA will have immunity from prosecution in certain areas. Also, if the government of the affected state considers that a member has committed a crime, it will inform the head of the operation without delay and present to him the evidence at its disposal. Then, the assisting State must ensure that its jurisdiction will be exercised with respect to crimes that may be committed by members of the MCDA operation.

Finally, as regards civil proceedings against a member of the MCDA operation before any court of the State concerned, the Head of the operation will be notified immediately.

2.2.5.2. Ethical framework

Throughout these guidelines, references to the items under the ethical dimension are scarce. However, the following can be noted in relation to equity, justice, conflict of interest and business responsibility. Specifically, at the beginning of the document, when the principles and concepts are indicated, section 20 includes the principles of humanity, neutrality and impartiality, which are specified as follows: "Human suffering must be addressed wherever it is found, with particular attention to the most vulnerable in the population, such as children, women and the elderly. The dignity and rights of all victims must be respected and protected"; - "Humanitarian assistance must be provided without engaging in hostilities or taking sides in controversies of a political, religious or ideological nature"; "Humanitarian assistance must be provided without discrimination on grounds of ethnicity, gender, nationality, political opinion, race or religion. The alleviation of suffering should be guided solely by need and priority should be given to the most urgent cases of distress" (p.8). With regard to conflict of interest, sections 21, 25, 26 and 32 of the Concepts and Principles also make special reference to respecting the sovereignty of countries when carrying out humanitarian assistance actions.

2.2.5.3. Inclusiveness framework

These guidelines, regarding the impact of inclusivity, solely refer to the application of the principle of impartiality (p. 8) in a holistic manner to the measures contemplated in the document. In this sense, it refers to the definition given by the UN General Assembly Resolution 46/182, which defines Impartiality as “Humanitarian assistance must be provided without discriminating as to ethnic origin, gender, nationality, political opinions, race or religion. Relief of the suffering must be guided solely by needs and priority must be given to the most urgent cases of distress”.

2.2.5.4. Social framework

In relation to societal impact considerations, the UN Guidelines on The Use of Foreign Military and Civil Defence Assets in Disaster Relief, updated and revised in 2007, discusses the following matters:

[6] More information available at: UN Office for the Coordination of Humanitarian Affairs (OCHA), Guidelines on the Use of Foreign Military and Civil Defence Assets In Disaster Relief ("Oslo Guidelines"), November 2007, https://www.refworld.org/policy/opguidance/ocha/2007/en/57053 [accessed 05 April 2024]

The Oslo Guidelines emphasise the importance of a rapid and well-coordinated response to disasters in times of peace. By facilitating the timely deployment of foreign MCDA (Military and Civil Defence Assets), these guidelines help ensure that affected communities receive the assistance they need promptly, reducing the impact of disasters. To this aim, this text defines roles, tasks and responsibilities for each affected state, transit state or partner involved in humanitarian aid, for instance: on requesting assistance; authority, control and management of the aid; coordination duties; monitoring activities, among other tasks. Moreover, bilateral agreements and multilateral treaties are taken into account when deploying MCDA. Also, civil-military coordination will take place in close coordination with the local and national authorities, involving the sharing of information, planning, exchange of liaison personnel, offering training, etc. In particular, "this coordination is defined as "the essential dialogue and interaction between civilian and military actors in humanitarian emergencies that is necessary to protect and promote humanitarian principles, avoid competition, minimise inconsistency, and when appropriate pursue common goals. Basic strategies range from coexistence to cooperation. Coordination is a shared responsibility facilitated by liaison and common training" (art. 8).

Social objectives are established, such as reducing human suffering, with particular attention to the most vulnerable in the population, and that this relief of suffering must be guided solely by needs and priority must be given to the most urgent cases of distress (art. 20). Regarding societal impact of humanitarian activities, it is stated that "the Government of the Affected State undertakes to assist the MCDA operation as far as possible in obtaining equipment, provisions, supplies and other goods and services from local sources required for its subsistence and operations. In making purchases on the local market, the MCDA operation shall, on the basis of observations made and information provided by the Government of the Affected State in that respect, avoid any adverse affect on the local economy" (art. 17).

2.2.6. IFAFRI Recommended Method for National Capability Gap Identification and Prioritization[7]

Year	2017
Type of instrument	Recommendations
Status	Non-Binding

2.2.6.1. Legal framework

States will be responsible for identifying first responders and for ensuring that these groups are varied and diverse in function. In this way, the needs of each population, environmental conditions, response capacity can be observed.

2.2.6.2. Ethical framework

In this document only a few issues related to the principles of transparency and accountability have been identified, especially when citing in step 4 the need for "informed decision-making for incident management". In this regard it is stated that "With multiple streams of information reaching incident command, the ability to make actionable decisions based on accurate information is challenged. This variable relates to any capability gaps that could improve the ability to manage or manipulate information to provide clear pathways to make actionable decisions and trade-offs".

2.2.6.3. Inclusiveness framework

This document does not include any provisions affecting aspects classified as inclusiveness.

[7] More information available at: [https://www.internationalresponderforum.org/system/files/library/2023-06/IFAFRI%20Recommended%20Method%20for%20National%20Capability%20Gap%20Identification%20and%20Prioritization.pdf]

2.2.6.4. Social framework

In addressing societal impact concerns, the Recommended Method for National Capability Gap Identification and Prioritization from the International Forum to Advance First Responder Innovation (IFAFRI), highlights the following issues:

In order to begin with the gap identification method for vulnerability reduction, IFAFRI member nations are recommended to develop their country-specific methodology using an evidence-based approach to address the various challenges and types of events that can have disastrous consequences. With that aim, different operational scenarios would be defined customised to country-specific needs, structures and processes (p. 3), "considering multiple operational environments and incident types" (p. 4), acknowledging that disasters are cross-cutting in nature and that prevention measures should be developed accordingly. Any alternative scenario that more closely aligns with each common national threat shall be taken into account (p. 5). Moreover, as variables that could be considered in this gap identification process, the document highlights, apart from human life, protection of property, assets or the environment (p. 7).

Community participation is considered as the backbone of this method: "it is important to draw on first responder knowledge and experience", proposing a diverse panel with members from "law enforcement, fire services, emergency medical services", among other groups of professionals involved in first responder operations (p. 4). This method suggests asking responders to provide their "input and advice based on their experience and expertise" (p. 4). This "identification of capability gaps can be done in a focus group or workshop setting", and "when possible, responders should provide operational parameters or requirements when discussing capability gaps" (p. 5). Later, "validation of capability gaps may be accomplished through in-person or virtual focus group meetings, surveys, etc." (p. 6), with the intention of ensuring that they have been captured accurately, involving participants "from different response disciplines and areas of the country" (p. 6). For instance, the "ability to incorporate information from multiple and nontraditional sources (e.g. crowdsourcing and societal media) into incident command operations" (p. 6) is shown as an example gap. Finally, "during the prioritisation process, responders are asked to review the full list of capability gaps and assign a level of priority for each" (p. 6).

2.3. European framework

2.3.1. Decision No 1313/2013/EU on a Union Civil Protection Mechanism[8]

Year	2013
Type of instrument	Decision
Status	Binding

2.3.1.1. Legal framework

The following general measures to improve disaster prevention, preparedness and response effectiveness shall be eligible for financial assistance

Studies, surveys, modelling and scenario building to facilitate the sharing of knowledge, best practices and information; training, exercises, workshops, exchange of staff and experts, networking, demonstration projects and technology transfer; monitoring, analysis and evaluation measures; information, education and public awareness, together with related outreach measures, to involve citizens in preventing and minimising the effects of disasters in the Union and helping them to protect themselves more effectively and sustainably; establishment and management of a programme compiling lessons learned from experience in interventions and exercises carried out under the Union Mechanism, including in the areas of prevention and preparedness; and

[8] More information available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013D1313]

communication actions and measures to raise public awareness of the civil protection activity of the Member States of the Union in the field of disaster prevention, preparedness and response.

In the event of a disaster, whether inside or outside the Union, the Commission may assist Member States in obtaining access to equipment or transport resources: by providing and sharing information on equipment and transport resources that may be provided by Member States, with a view to facilitating the pooling of such equipment and transport resources; by assisting Member States in identifying and facilitating access to transport resources that may be available from other sectors, including the commercial sector; or by assisting Member States in identifying equipment that may be available from other sectors, including the commercial sector.

2.3.1.2. Ethical framework

Throughout this decision of the European Parliament, numerous ethical items such as those related to transparency and accountability, fairness and justice, integrity and anti-corruption, conflict of interest management, sustainability and ethics education and training are included. In particular, with regard to the principle of transparency, articles 6, 8, 11, 15, 16, 20, 22, 23, 25(6) and 34 contain some of the most relevant points on this issue. If, for example, we take article 6 as a reference, it states the importance of making "available to the Commission a summary of the relevant elements of the assessments (in relation to developing risk assessments and the assessment of risk management capabilities), focusing on the key risks. For key risks with a cross-border impact and risks related to disasters causing or likely to cause multinational cross-border effects, as well as, where appropriate, for low probability risks with a high impact, Member States shall describe priority prevention and preparedness measures. The summary shall be provided to the Commission by 31 December 2020 and every three years thereafter, as well as whenever significant changes occur". Similarly, other articles contain transparency-oriented actions of the same type. For example, Article 34(2) states that "Every two years, the Commission shall submit a report to the European Parliament and the Council on the operations and progress made under Articles 6(5), 11 and 12...". As regards the principle of equity, it can also be seen in Art. 6(5) when it states that "The Commission, in cooperation with the Member States, shall establish and develop Union disaster resilience targets in the field of civil protection and adopt recommendations to define them as a common non-binding baseline to support prevention and preparedness actions in the event of disasters causing or likely to cause multinational transboundary effects. These objectives will be based on current and prospective scenarios, including the effects of climate change on disaster risks, data on past events and cross-sectoral impact analysis, with particular attention to vulnerable groups. With regard to integrity and non-corruption, Articles 25, 26 and 34 also contain clear references to this issue, stating for example in Art.25(5) that "the annual or multiannual work programmes shall set out the objectives pursued, the expected results, the method of implementation and the total amount.

They shall also contain a description of the actions to be financed, an indication of the amount allocated to each action and an indicative implementation timetable". With reference to the management of conflicts of interest, Articles 15, 26, 27 and 28 address this issue. For example, Article 15(5) states that "The requesting Member State shall be responsible for directing assistance interventions. The authorities of the requesting Member State shall establish guidelines and, where necessary, define the limits of the tasks entrusted to modules or other response capacities. The details of the execution of such tasks shall be left to the person in charge designated by the assisting Member State", which establishes a clear framework for action to deal with problems of this kind. Concerning the ethical items dedicated to sustainability and ethics education and training, these are covered in articles 6, 8, 10, 13 and 3, 5, 8 and 13 respectively. In this respect, with regard to sustainability, we find in article 6(5) that "The Commission, in cooperation with Member States, shall establish and develop Union disaster resilience goals in the area of civil protection, and adopt recommendations to define them as a non-binding common baseline to support prevention and preparedness actions in the event of disasters which cause or are capable of causing multi-country transboundary effects" and, as for the second item mentioned, we can find in Art. 3(a) that "to

achieve a high level of protection against disasters by preventing or reducing their potential effects, by fostering a culture of prevention and by improving cooperation between the civil protection and other relevant services".

2.3.1.3. Inclusiveness framework

Article 13.1 Union Civil Protection Knowledge Network states that "the Commission and the Member States shall promote gender-balanced participation in the establishment and the functioning of the Network".

2.3.1.4. Social framework

With regard to societal impact issues, Decision No 1313/2013 devotes numerous mentions to the following issues:

Article 3.1 defines some of its societal objectives: to improve cooperation between the civil protection and other relevant services, to increase public awareness and preparedness for disasters, and to increase the availability and use of scientific knowledge on disasters, among others. These objectives are materialised throughout the text in several recommendations to apply cross-sectoral impact analysis, as well as some lessons learnt program which includes monitoring of actions. For instance, risk management efforts are encouraged, especially in scenarios with transboundary effects, with particular attention to cross-sectoral impact analysis and monitoring programmes (art. 6.5; art. 13.1). From an economic point of view, article 20 states that these actions shall be eligible for financial assistance. Some indicators for evaluating aspects of societal impact are in place, such as in article 3.2:: "progress in improving the response to disasters: measured by the speed of interventions under the Union Mechanism and the extent to which the assistance contributes to the needs on the ground"; and "progress in increasing public awareness and preparedness for disasters: measured by the level of awareness of Union citizens of the risks in their region".

A significant focus is placed on reducing vulnerabilities across various systems and areas susceptible to disaster impact. Article 1.2 states that "the protection to be ensured by the Union Mechanism shall cover primarily people, but also the environment and property, including cultural heritage" (also biodiversity: article 13.2). Emphasis is placed on developing risk assessments, evidence-based scenario building, and disaster management planning to address cross-sectoral disaster risk management and the adverse effects of climate change (art. 6.1; art. 10). Lastly, in article 26.2, "synergies, complementarity and increased coordination shall be developed with other instruments of the Union such as those supporting cohesion, rural development, research, health, migration and security policies".

International cooperation is highlighted as essential, with mechanisms established for information sharing, consultation, and coordination with third countries and international organisations. Instruments such as the Emergency Response Coordination Centre (ERCC) (art. 7), the European Civil Protection Pool (art. 11), and rescEU (art. 12) are established. Community and civil society participation are also encouraged through the involvement of relevant actors in the Union Civil Protection Knowledge Network (art. 13.1): civil protection and disaster management actors, centres of excellence, universities and researchers", as well as international organisations and entities, third countries and organisations active on the ground, while promoting a gender-balanced participation, including exchanges of professionals and experienced volunteers. Open and transparent communication with civil society regarding risk assessments, disaster management, and the impact of specific actions is promoted. Measures are outlined to support awareness-raising, public information, and education efforts (art. 5.1; art. 11.9; art. 20; art. 20a).

Finally, the regulation aims to be adaptable to emerging changes and challenges. Forward-looking scenarios on risk management and the stimulation of research and innovation are also prioritised,

including the impacts of climate change on disaster risks, data on past events and cross-sectoral impact analysis (art. 5.1; art. 6.5; art. 13.1).

2.3.2. Commission Implementing Decision (EU) 2019/570 of 8 April 2019 laying down rules for the implementation of Decision No 1313/2013/EU of the European Parliament and of the Council as regards rescEU capacities and amending Commission Implementing Decision 2014/762/EU[9]

Year	2019
Type of instrument	Commission Implementing Decision
Status	Binding

2.3.2.1. Legal framework

This decision establishes a legal framework for the development and maintenance of RescEU capabilities. This framework clearly defines the responsibilities and obligations of the Member States and the European Commission in crisis management and emergency response. In its most updated version of July 12, 2022, reference is made to some changes on relevant aspects such as the elaboration of a risk category, the capabilities of the agency in its different fields and some financial provisions. Likewise, in the annex, reference is made to the quality requirements for RescEU capabilities, this annex makes according to each area (firefighting, evacuations, decontamination, storage, etc.) the tasks, capabilities, main components and deployment that are specifically needed in each one.

2.3.2.2. Ethical framework

As far as the ethical dimension is concerned, a link with the item on transparency and accountability could only be established throughout this document when Article 3 describes the financial provisions and sets out the criteria for direct grants to be awarded for costs covered by the actions.

2.3.2.3. Inclusiveness framework

The document takes into account "individuals considered to be at risk" (p. 9), establishing that these may comprise: high risk potential contacts, first responders, laboratory workers, health care workers, family members, and other defined vulnerable groups.

2.3.2.4. Social framework

In relation to societal impact considerations, this Commission Implementing Decision (EU) 2019/570, addresses the following matter, acknowledging the complexity of disasters and their cross-sectoral nature, and emphasising the need to deploy cross-sectoral response measures. In article 3d, "for the purposes of establishing rescEU capacities necessary to respond to low probability risks with a high impact, the Commission shall take into account": (a) "the unpredictability or the extraordinary nature of a disaster"; (b) "the scale of a disaster, including mass casualties, mass fatalities, and mass displacement"; (e) "the potential risk of severely disrupting the functioning of the national government, including the provision of societal, environmental, economic and public health services or the disruption of critical infrastructure"; and (f) "geographical range, including the potential of impacts spreading beyond borders". For that reason, article 2.2 describes the capacities that the initial composition of rescEU, such as medical countermeasures, firefighting capacities, or temporary shelter capacities. The latter, for instance, shall take into account affected population, housing, hygiene and basic medical service, food and water, societal gathering, staff to handle and maintain shelter units, local or international personnel training, and so on (annex: art. 9).

[9] More information available at: [https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2019.099.01.0041.01.ENG]

2.3.3. Commission Implementing Decision (EU) 2021/1956 of 10 November 2021 on the establishment and organisation of the Union Civil Protection Knowledge Network[10]

Year	2021
Type of instrument	Commission Implementing Decision
Status	Binding

2.3.3.1. Legal framework

Disclosure rules applicable to members of the Knowledge Network should comply with professional secrecy obligations. In addition, in the interest of transparency of the activities carried out by the bodies of the Knowledge Network, the Commission should publish the relevant documents of the meetings on the online platform referred to in Article 13(1)(d) of Decision No 1313/2013/EU.

Furthermore, personal data should be processed in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council[11].

2.3.3.2. Ethical framework

The main ethical issues found throughout this Implementing Decision are related to transparency, sustainability and ethics education and training. The main objective of the document is to establish the basis for the creation of a Network of Expertise between EU and non-EU countries which, as stated in the 10th recital, aims to "bring together, promote and strengthen capacity building initiatives relevant to civil protection and disaster management stakeholders, with a particular focus on the EU Mechanism. And, in the scientific field, "to bring together academia, practitioners and decision-makers for multidisciplinary, cross-sectoral and cross-border cooperation to apply scientific knowledge to disaster risk management...". The area of transparency and accountability is covered succinctly in Articles 5, 6, 9, 13 and, more broadly and clearly, in Article 16, which is devoted entirely to transparency, where the actions to be taken to preserve this item are detailed. For example, the second paragraph of this article states that "All documents of the meetings of the Knowledge Network bodies, including agendas, minutes and participants' contributions, shall be made available in the Commission's Register of Expert Groups and published on the online platform referred to in Article 13(1)(d) of Decision No 1313/2013/EU. In particular, agendas and other important background documents shall be published in due time before the meeting and minutes thereafter.

Exceptions to publication shall be limited to cases where disclosure of a document would undermine the protection of a public or private interest as defined in Article 4 of Regulation (EC) No 1049/2001 of the European Parliament and of the Council". There is no direct reference to sustainability, but it is possible to extract, throughout the different articles, different actions aimed at sustainability from an eminently societal point of view. The same is true of the ethics training and education item, as the mere purpose of the document presupposes an item of these characteristics. However, a more concrete reference can be found in paragraph 11 of the initial considerations, where it is stated that "The capacity building pillar should focus on existing and well-known programmes and projects, such as the Union Mechanism's training and exercise programme, the exchange of civil protection experts, the Knowledge Network partnerships and the Union Mechanism's prevention and preparedness programme. These programmes should be consolidated through a gradual and continuous process and complemented by other capacity building activities. The scientific pillar should build on and integrate the existing scientific structures and networks underpinning the Union Mechanism, in particular the Disaster Risk Management

[10] More information available art: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D1956]
[11] Recitals 12, 13 and 15 of the Commission Implementing Decision (EU) 2021/1956 of 10 November 2021 on the establishment and organisation of the Union Civil Protection Knowledge Network.

Knowledge Centre managed by the Joint Research Centre of the European Commission, as well as relevant Horizon Europe programmes funding research and innovation actions and related networking initiatives in the field of disaster risk management.

2.3.3.3. Inclusiveness framework

In Articles 5 and 13, which regulate Membership of the boards and Observers respectively, it is established the promotion of gender-balanced participation.

2.3.3.4. Social framework

This Commission Implementing Decision on the establishment of the Union Civil Protection Knowledge Network addresses societal aspects the following way:

As stated throughout this document, a Union Civil Protection Knowledge Network shall be established with the aim to "aggregate, process, and disseminate knowledge and information relevant to the Union Mechanism by including relevant civil protection and disaster management actors, centres of excellence, universities, and researchers and following a multi-hazard approach" (2). The first main objective of this network is, as established in Decision No 1313/2013, to strengthen cooperation between the Union and the Member States in order to improve the response to disasters. Therefore, the working groups of this network "shall be composed of a representative of the Commission, a representative of each of the Member States and each of the Participating States to the Union Mechanism" (art. 10.1), engaging the necessary institutional actors from an international perspective with the purpose of supporting the "coherence of planning and decision-making processes by facilitating the continuous exchange of knowledge and information involving all areas of activity under the Union Mechanism" (3).

In the field of civil protection, it is also considered relevant in the text to facilitate cooperation and coordination with non-institutional actors, ranging from centres of excellence, to universities and researchers, creating "synergies with other relevant groups and networks" (4). With more detail, two Knowledge Network Pillars are created: "the Capacity Development pillar shall aim to bring together, promote and strengthen capacity development initiatives of relevance to civil protection and disaster management stakeholders, with a special focus on the Union Mechanism" (art. 9.2); and "the Science pillar shall aim to bring together academia, practitioners, and decision-makers for multi-disciplinary cross-sectoral and cross-border cooperation to apply scientific knowledge to disaster risk management, and in particular, to prevention and preparedness activities more efficiently" (art. 9.3). Both focus on involving the community, civil society and relevant stakeholders to create a multi-disciplinary working group that takes into account society's needs and knowledge.

2.3.4. Communication from the Commission to the European Parliament and the Council on the EU's humanitarian action: new challenges, same principles[12]

Year	2021
Type of instrument	Communication
Status	Non-Binding

2.3.4.1. Legal framework

In this scenario, the Union needs to step up its efforts in advocating for a significantly improved humanitarian funding effort and a fairer distribution of responsibility among donors, including EU Member States. Working alongside its Member States and other committed humanitarian donors like the United States, the Union should capitalise on its bilateral, regional, and multilateral engagements with both traditional and emerging donors (particularly those whose economic influence has grown notably in recent times, such as China and Gulf States). These engagements

[12] More information available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0110]

should aim to boost funding levels and ensure more consistent support for the global humanitarian system. It's crucial that these efforts are aligned with the ongoing objective of dedicating 0.7% of gross national income to official development assistance while also urging for increased commitments to humanitarian funding in line with the escalating humanitarian needs seen in recent years. Alongside these efforts, there's a need to advocate for the observance of humanitarian principles, encourage best practices in humanitarian aid, and uphold international humanitarian law.

On the other hand, international humanitarian law (IHL) comprises a set of universally acknowledged rules designed to mitigate the impact of armed conflicts and safeguard civilians and non-combatants. Upholding IHL isn't just a significant goal in itself; it's also crucial for ensuring the effectiveness of humanitarian assistance and can even prevent the need for such aid from arising. Sadly, breaches of these rules are all too common nowadays, with civilians, including humanitarian and medical workers, frequently falling victim to deliberate attacks by warring factions.

The EU has established guidelines aimed at encouraging compliance with international humanitarian law. Additionally, it provides support for the training of military, diplomatic, and security personnel, a commitment that will continue through the Union's new external initiatives spanning from 2021 to 2027. It's imperative that the Union consistently prioritises the promotion and implementation of international humanitarian law in its foreign efforts. In this same way, the EU remains steadfast in its support of the International Committee of the Red Cross, advocating for the effective enforcement of international humanitarian law.

2.3.4.2. Ethical framework

In this European Parliament Communication, the following ethical issues have been identified: equity and justice, sustainability, transparency and accountability, and finally, compliance and sanctions. First of all, it is clear throughout the document that one of the fundamental pillars for the construction of solid foundations for humanitarian aid must be based on the pillar of equity and justice. For example, it states that "protections for people caught in crisis situations, particularly through the prevention, mitigation and response to sexual and gender-based violence and sexual exploitation, abuse and harassment will remain a prominent feature of EU humanitarian aid, in line with the EU Gender Action Plan. The Union will continue to support the call for protection against gender-based violence in emergencies" (p.5) or with regard to the EU humanitarian response which should be based on the principle of "do no harm" to affected populations and the environment and will strive to be sensitive to conflict in order not to inadvertently reinforce it. It will continue to promote and strengthen effective civil-military coordination in the humanitarian field in order to safeguard the humanitarian space" (p.5). Closely related to the principles of equality and justice, the principle of sustainability is also evident when, for example, it is stated that one of the central elements of the development of aid beneficiaries is the safe and continuous schooling of children in crisis situations, or when it is intended to encourage resources to be channelled more clearly and directly to local actors, allowing them to be more autonomous and to take a more active part in decision-making that directly affects their environments

Therefore, priorities include "supporting localised financing models, such as joint multilateral funding mechanisms focused on local actors" or "promoting consortia based on equal partnerships with shared funding and responsibilities between local and international actors" (p. 10). Finally, the principle of sustainability is included when highlighting one of the following challenges and objectives: "addressing governance challenges, respecting the fundamental rights of populations, taking into account inequalities, providing access to basic services, justice, economic opportunities and security, and combating climate and environmental problems", (p. 14). With regard to transparency and accountability, throughout the text there is also a clear emphasis on its importance and relevance. In this regard, the need to improve the "transparency and visibility of donor assistance, and to ensure that the highest possible percentage of funds reaches the people in need of assistance", (p.7). Finally, as regards compliance and sanctions, the European

Parliament's Communication sets the following objective: "to place compliance with international humanitarian law at the centre of the Union's external action to protect civilian populations, support humanitarian actions" (p.20), or "Continue to ensure that the Union's sanctions policy fully reflects international humanitarian law, in particular through the consistent inclusion of humanitarian exceptions in sanctions regimes. Work towards an effective framework for the use of such exemptions by humanitarian organisations receiving EU funding. Provide additional practical support to humanitarian organisations in relation to their rights and responsibilities under the various EU sanctions regimes", (p.20).

2.3.4.3. Inclusiveness framework

The document aligns with the EU Gender Action Plan[13], advocating for the continued integration of protection for individuals caught in crisis situations, including prevention, mitigation, and response to gender-based violence and sexual exploitation, abuse, and harassment. In this regard, it aims to ensure opportunities for meaningful participation of aid beneficiaries in decisions that affect them, and to meet the needs and rights of specific groups, including women, children, older persons, and people with disabilities (p. 4-5).

2.3.4.4. Social framework

This Communication from the European Commission addresses societal impact concerns as follows, establishing key actions to achieve its objectives. The document emphasises the EU's commitment to humanitarian action as an expression of global solidarity, aiming to alleviate human suffering and especially addressing the needs of populations affected by crises, conflicts, and natural disasters due to the rising curve in humanitarian needs. Topics such as poverty, pre-existing fragilities and inequalities remain primordial (p. 1). Also, issues such as gender-based violence, sexual exploitation and harassment (p. 4), schooling for children and child protection (p. 5), and safety nets (p. 7).

One of the main topics of the document is disaster preparedness, risk-informed approaches, climate change adaptation, and environmental resilience, aiming to reduce the vulnerability of affected communities and create synergies between humanitarian aid, development, and peacebuilding and conflict resolution (p. 3-4). This document reflects a comprehensive approach to humanitarian action, considering the importance of addressing immediate humanitarian needs while working towards long-term solutions that address the underlying causes of crises (p. 12). Other socio-economic, governance or environmental issues shall also be tackled "in a holistic manner".

When discussing enhancing humanitarian aid, the importance of international coordination and cooperation is highlighted. "Effective multilateralism and UN-led coordination will remain central to the EU's humanitarian action […] Furthermore, the EU will continue to rely on a strong network of diverse partners, including non-governmental organisations, UN agencies, funds and programmes and other international organisations, as well as specialised agencies of EU Member States. Cooperation with these diverse partners is essential to make a difference and deliver quality results on the ground" (p. 5). The document also underscores the importance of prioritising people and providing opportunities for meaningful participation of aid beneficiaries in decisions affecting them (p. 4). It supports empowering local responders and fostering equitable partnerships between international and local actors (p. 7). The exploration of private sector involvement through innovative initiatives is also highlighted (p. 7, 14). Communication and transparency with civil society is considered "essential for accountability and public support for humanitarian action". In that sense, "the EU commits to promoting the visibility of its humanitarian aid and communicating its actions and principles to the public" (p. 17-18). Then, aid organisations shall keep their

[13] More information available at: [https://ec.europa.eu/commission/presscorner/detail/en/statement_22_7941]; [https://ec.europa.eu/commission/presscorner/detail/en/IP_23_5858]

"commitment to coordinated needs assessments, accountability to beneficiaries and taxpayers, transparency and visibility" (p. 6). Lastly, it is stated the relevance of "guidance and monitoring of visibility obligations, empowering its humanitarian partners to invest more in awareness raising", and that these "communication actions will support the overall principles of transparency, accountability and dialogue with the citizens" (p. 18).

The document advocates for modernised funding mechanisms that offer greater operational flexibility to humanitarian partners, allowing an adaptive response to unforeseen emergencies and natural disasters (p. 6-7), in particular regarding "the impact of climate change, environmental degradation, global population growth and failed governance" (p. 1).

2.3.5. Council Regulation (EU) 2016/369 of 15 March 2016 on the provision of emergency support within the Union[14]

Year	2016
Type of instrument	Council Regulation
Status	In force

2.3.5.1. Legal framework

This regulation establishes the framework for granting emergency assistance from the Union. Such emergency assistance may only be provided where the exceptional nature of the disaster, in terms of its scale and impact, has far-reaching major humanitarian consequences in one or more Member States, and only in exceptional circumstances where no other instrument available to the Member States or the Union is sufficient.

This response shall be based on the needs of the Member States concerned. The assistance may include assistance, relief and, where necessary, protective operations to save and preserve human lives during disasters or any other expenditure directly linked to the implementation including the purchase, preparation, collection, transport, storage and distribution of goods and services in connection with such actions. These actions may be carried out by the Commission or by organisations selected by the Commission.

2.3.5.2. Ethical framework

In regard to ethical aspects, the following have been identified throughout the following regulation: transparency and accountability, fairness and justice, integrity and anti-corruption, conflict of interest management, compliance, and sanctions. The specification of each ethical component, in order, is reflected as follows. Regarding transparency and accountability, it is clearly expressed in the types of financial intervention and procedures for the execution of actions that may be carried out, providing clear guidelines on which actions are fundable, what mechanisms will be used, and the relevant follow-up actions.

This is outlined in articles 4 and 8. Concerning the ethical principles of fairness and justice, they are outlined in article 3 when explicit mention is made that actions will be carried out "in accordance with the fundamental humanitarian principles of humanity, neutrality, impartiality, and independence" (p.3). In terms of integrity and anti-corruption, they are addressed in articles 7 and 8 when the establishment of "preventive measures against fraud, corruption, and any other illegal activity, the implementation of effective controls, and, if irregularities are detected, the recovery of amounts paid..." (p.5), among other measures, is specified. Similarly, in article 8, it explicitly states that actions receiving financial support "must be subject to regular monitoring" (p.6). Likewise, article 7 lays the groundwork for managing potential conflicts of interest through different bodies focused on the financial monitoring of actions that have received funding. Finally, in article 7, it is

[14] More information available at: [https://eur-lex.europa.eu/eli/reg/2016/369/oj]

also mentioned how, through the various bodies responsible for financial monitoring, "actions will be taken to determine whether fraud, corruption, or any other illegal activity affecting the financial interests of the Union has occurred," (p. 6).

2.3.5.3. Inclusiveness framework

This document does not include any provisions affecting aspects classified as inclusiveness.

2.3.5.4. Social framework

The principal objectives of the humanitarian aid operations are described in article 2, referring to clear societal aspects, such as preserving life, providing assistance and relief, helping finance aid, carrying out short-term rehabilitation and reconstruction work while taking long-term development objectives into account, coping with migration consequences and ensuring preparedness. Also, article 1 explicitly defines that this aid shall comprise assistance on a non-discriminatory basis to help people in third countries, particularly the most vulnerable among them, and as a priority those in developing countries.

Regarding societal impact assessments, it is discussed during the document that this aid shall also finance "the assessment of humanitarian projects and plans, operations to monitor humanitarian projects and plans" (art. 4). Also, it is the Commission who shall appraise, monitor and assess operations under this Regulation (art. 14), and who shall regularly assess humanitarian aid operations financed in order to establish whether they have achieved their objectives and to produce guidelines for improving the effectiveness of subsequent operations (art. 18).

International cooperation is one of the main features of this regulation. Coordination with Member States, donor countries, international humanitarian organisations and institutions, non-governmental organisations, shall be strengthened (art. 4). These agencies, institutions, organisations and third countries can lead and request for humanitarian aid operations financed by this mechanism (arts. 6, 8, 9). Additionally, a system for exchange of information and activities' coordination shall be operated between Member States and the Commission (art. 10).

Lastly, public awareness and information campaigns are pursued and can be financed by this mechanism (art. 4): these shall be "aimed at increasing understanding of humanitarian issues, especially in Europe and in third countries where the Community is funding major humanitarian operations".

2.3.6. Council Regulation (EC) No 1257/96 of 20 June 1996 concerning humanitarian aid[15]

Year	1996 (26/07/2019 Update)
Type of instrument	Act
Status	Binding

2.3.6.1. Legal framework

The European Union provides humanitarian aid to people from third countries who are victims of natural disasters. This aid ranges from rescue to financial and rehabilitation aid. This aid takes the form of grants and can be implemented at the request of international organisations or non-governmental organisations.

According to this regulation, humanitarian aid means assistance, relief and protection operations on a non-discriminatory basis to help people in third countries, in particular the most vulnerable and, as a matter of priority, those in developing countries, who are victims of natural disasters and

[15] More information available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01996R1257-20190726]

man-made crises. It shall do so for as long as is necessary to respond to the needs of the people of third countries, such as wars and outbreaks of fighting, or exceptional situations or circumstances comparable to natural or man-made disasters. It shall do so for the time necessary to meet the humanitarian needs resulting from these different situations. Such assistance shall also include operations to prepare for or prevent disasters or comparable exceptional circumstances.

Agreed to Article 18, the Commission shall regularly evaluate humanitarian aid operations financed by the Community in order to assess whether they have achieved their objectives and to draw up guidelines for improving the effectiveness of subsequent operations. The Commission shall submit to the Committee a summary, including the status of the experts employed, of the evaluation exercises carried out, which it may, if necessary, examine. The evaluation reports shall be made available to Member States on request.

2.3.6.2. Ethical framework

In the dimension dedicated to ethical considerations, the principles of transparency and accountability, fairness and justice, integrity and anti-corruption, sustainability, and ethics education and training are articulated throughout the regulation. In articles 1 and 2, the principles of fairness and justice, as well as sustainability, are outlined. For instance, it is stated in article 1 that "Community humanitarian aid will consist of non-discriminatory actions of assistance, relief, and protection in favour of populations, particularly the most vulnerable, in third countries and especially in developing countries, victims of natural disasters, events of human origin such as wars or conflicts, or situations and circumstances similar to natural or man-made disasters, for the time necessary to address the humanitarian needs resulting from these different situations." In article 2, sections a) and c) among others, address planned humanitarian aid actions with the goal of a) saving and preserving human lives in emergency situations or immediately following natural disasters that have caused loss of human lives, physical, psychological, and moral suffering, and significant material damage; c) contributing to the financing of the transportation of aid and its free delivery to recipients through all available logistical means, while protecting humanitarian aid assets and personnel, excluding actions with defence implications. Additionally, in the same article, sections e) and g) introduce the principle of sustainability, stating: e) addressing the consequences of population displacement (refugees, displaced persons, and repatriates) resulting from natural disasters or caused by humans and undertaking repatriation actions and assistance with reinstatement in their countries of origin, as long as conditions specified in current international agreements are met; f) ensuring preparedness for the risks of natural disasters or similar exceptional circumstances and using a rapid alert system and appropriate intervention.

Focusing on the principle of transparency, it is captured in articles 4, 14, 16, 18, and 20, detailing which actions are fundable and specifying the type of actions to be taken for the monitoring of funded actions. For example, in article 16, it is stated that "Once a year, the Committee referred to in Article 17 will hold an exchange of views, based on a presentation by the Commission representative, on the general guidelines for humanitarian action to be carried out in the following year, and a review of the overall coordination issues of community and national humanitarian aid actions, as well as any general or specific matters relating to humanitarian aid in this field. In article 18, section 1, it is mentioned that "The Commission shall conduct periodic assessments of humanitarian aid actions funded by the Community to determine whether the objectives set for these actions have been met and to provide guidelines for improving the effectiveness of future actions. The Commission shall submit to the Committee a summary of the evaluations carried out, which, if necessary, may be examined by the Committee, indicating the status of the experts involved. Evaluation reports will be made available to requesting Member States." Regarding the principles of integrity and anti-corruption, articles 7, 12, and 16 provide guidelines for compliance with European regulations. For example, in article 12, it is stated that "Every financing contract concluded under this Regulation shall provide, in particular, that the Commission and the Court of Auditors may carry out on-the-spot checks at the headquarters of humanitarian partners and in the

field, in accordance with the usual arrangements established by the Commission under the applicable provisions, and in particular those of the Financial Regulation applicable to the general budget of the European Communities." Finally, the ethical aspects dedicated to ethics education and training can be observed in article 4, where actions aimed at raising awareness and disseminating information to increase knowledge about humanitarian issues are considered, highlighting the importance of knowledge exchange between humanitarian organisations and entities.

2.3.6.3. Inclusiveness framework

This document does not include any provisions affecting aspects classified as inclusiveness.

2.3.6.4. Social framework

As stated throughout the regulation, all the emergency support receiving financial support under this Regulation, as "specific measures appropriate to the economic situation in the event of an ongoing or potential nature or man-made disasters […] that gives rise to severe wide-ranging humanitarian consequences" (art. 1.1), shall be subject to regular financial monitoring (art. 8.1). This monitoring activity, and those related to preparation, control, audit and evaluation necessary for the management of this emergency support may also be covered by the Union's financing (art. 5.3).

Regarding the synergies with other regulations, preventive measures and areas, article 1.2 points out the following: "emergency support provided under this Regulation shall be in support of, and complementary to, the actions of the affected Member State". Also, article 3 includes a preventive perspective when defining that "addressing needs in the aftermath of a disaster or preventing its resurgence" are also eligible actions. In article 6, it is stated that "synergies and complementarity shall be sought with other instruments of the Union, in particular with respect to those instruments under which some form of emergency assistance or support may be offered", giving a consistent quality to the European Union's capacity for action.

International and regional cooperation is enhanced in article 1.2: "close cooperation and consultation with the affected Member State shall be ensured". To this end, also, art. 3.4 states that "the Commission may in particular select, as partner organisations, non-governmental organisations, specialised services of Member States, national authorities and other public bodies, international organisations and their agencies", allowing that any direct and indirect cost from these partner organisations may be covered by the Union (art. 5). In this sense, community involvement is also promoted through art. 3.4: "other organisations and entities having the requisite expertise or active in the sectors relevant for disaster relief, such as private service providers, equipment manufacturers as well as scientists and research institutions".

2.4. General remarks on International and European Framework

In addressing the complexities of DRR, international and European frameworks largely focus on legal, ethical, inclusiveness, and social dimensions and establish a broad set of standards designed to guide the policies and practices of DRR, ensuring that they are effective, fair, and respectful of human rights and societal norms. The following briefly summarises the common position of the documents discussed above:

- *Legal dimension* underscores the necessity for DRR initiatives to align with higher legislative standards, such as international humanitarian laws and national privacy regulations. This legal emphasis ensures that efforts in disaster management adhere to the principles of jurisdiction, rights, and obligations, thus safeguarding the interests of individuals and communities while fostering a structured approach to emergency responses.

- *Ethical dimension* places a strong focus on transparency, accountability, and justice. These frameworks advocate for DRR policies that promote ethical conduct, ensuring that all operations are carried out with integrity and fairness. The emphasis on ethics helps maintain public trust and confidence in disaster response activities, highlighting the importance of ethical decision-making in scenarios that often involve vulnerable populations and high-stakes situations.

- *Inclusiveness dimension* notes as essential that disaster risk management practices consider and actively include diverse groups, particularly marginalised and vulnerable communities. Frameworks call for equitable participation and accessibility in the development and execution of disaster responses, ensuring that no one is left behind in times of crisis. This focus helps to tailor responses to the needs of all segments of the population, enhancing the effectiveness and equity of interventions.

- *Social dimension* examines the broader impact of disaster risk management on society. They emphasise the need for policies that not only respond to immediate disasters but also contribute to long-term societal resilience. This includes fostering community participation, enhancing communication and transparency, and ensuring that disaster risk management efforts are adaptable to different social contexts and needs.

While these international and European guidelines provide a robust basis for managing legal, ethical, inclusiveness, and social concerns in disaster scenarios, they do not typically specify how advanced technologies should be integrated into DRR. However, the principles they advocate are crucial for guiding the development and implementation of technological solutions. Therefore, in linking these broader guidelines to the specific technological solutions proposed by the SYNERGISE project, the standards set forth are essential for guiding their ethical, legal, inclusive, and socially responsible deployment. This connection ensures that the innovative tools and methods enhance disaster response capabilities without compromising the foundational principles of DRR. By adhering to these guidelines, technology developers and policymakers can ensure that their solutions not only advance the technical aspects of disaster response but also uphold and promote the core values of legality, ethics, inclusiveness, and social welfare.

Table 1 describes how SYNERGISE project's solutions could address the different dimensions (i.e. legal, ethical, inclusive and social) highlighting the necessary standards and the potential risks, gaps and limitations associated with the deployment of these technologies in FR operations.

Table 1. International standards for SYNERGISE' technological solutions

TECHNOLOGY	LEGAL	ETHICAL	INCLUSIVENESS	SOCIAL
Robots and drones	Compliance with aviation and privacy regulations is crucial to avoid legal actions and maintain public trust.	Ensuring ethical data use and operational transparency to avoid misuse and biases, enhancing trust and integrity in operations.	Designing technology accessible to all first responders, preventing unequal rescue efforts and addressing diverse needs during disasters.	Societal acceptance is key; addressing fears of surveillance and job displacement to prevent hindering the effectiveness of emergency responses.
Wearable devices for monitoring	Adherence to health and safety regulations ensures that devices are safe and data handling complies with personal data regulations, preventing legal issues.	Managing health data with high confidentiality and informed consent to maintain trust and integrity.	Ergonomic design for various body types and usability by all first responders enhances team capabilities and response effectiveness.	Addressing concerns about privacy and autonomy to prevent hesitancy in device usage among first responders.
Infrastructure-less	Legal compliance with data protection	Transparent operation and ethical use of	Tailoring systems to function in diverse	Community trust is crucial; addressing

localization systems	regulations ensures lawful management of sensitive location information, avoiding legal repercussions.	location data prevent violations of personal privacy and maintain ethical standards.	environments ensures effective operation across different disaster scenarios, aiding all first responders.	privacy concerns and the perception of being monitored enhances community support for disaster response initiatives.
Augmented reality for tactical response	Ensuring accuracy and reliability in augmented reality content is legally necessary to prevent misinformation and potential operational failures.	Maintaining information integrity in augmented reality aids in making ethically sound decisions, crucial in high-stakes environments.	Intuitive and adaptable design caters to diverse user needs, promoting interoperability among responders with different technological fluency.	Reducing dependency on augmented data to maintain traditional skills among responders, addressing societal concerns about over-reliance on technology.
AI-enabled information synthesis	Complying with data regulations ensures lawful AI operation, crucial for maintaining legitimacy and avoiding legal repercussions.	Developing explainable AI with accountable decision-making processes addresses ethical concerns, crucial for acceptability in high-stakes disaster management.	Ensuring AI systems are trained on diverse data sets avoids biased outputs and ensures fair and effective response strategies for all communities.	Aligning AI development with societal values prevents public opposition, particularly concerning replacement of human decision-making.
High bandwidth communication systems	Compliance with telecommunications regulations ensures secure and reliable communication, crucial for coordinated disaster response.	Integrity and confidentiality in communications are vital for maintaining trust and operational coherence across disaster management efforts.	Support for multilingual capabilities and accessibility features ensures effective communication across diverse responder groups, enhancing inclusiveness.	Reliable communication technology builds public trust in emergency services, ensuring community support during disasters.
Interoperable incident management system	Adhering to international standards for data sharing and interoperability ensures effective integration and coordinated response across different jurisdictions and administrative regions.	Clear data use and sharing protocols are essential for maintaining ethical standards and ensuring cooperative and integrated emergency management.	Adaptable systems that accommodate various operational protocols ensure that diverse teams can integrate and work effectively, promoting equitable disaster response capabilities.	Fostering collaboration and community resilience through effective coordination and information sharing, which is essential for building long-term disaster response and recovery strategies.

By meticulously linking the innovative technologies and methods developed under the SYNERGISE project to the comprehensive dimensions specified in international and European frameworks—legal, ethical, inclusiveness, and social—the project can significantly enhance its potential impact. This integration ensures that the technological solutions provided are not merely about pioneering advances in disaster response but are also embedded with principles that uphold social responsibility, legal compliance, ethical integrity and inclusiveness.

These identified needs highlight the crucial role of examining specific national frameworks, essential for building a robust foundation in operational effectiveness, privacy, security, and ethical governance within modern emergency response technologies. Analysing the national regulations pertinent to SYNERGISE end-users is particularly vital. This examination will sharpen the focus on technological issues that impact the project's solutions directly. By assessing these national frameworks, the SYNERGISE project seeks to tailor its technological responses to align seamlessly with localised regulatory standards and cultural nuances, enhancing the effectiveness and acceptance of these tools across diverse operational contexts. This strategic analysis is fundamental in driving the project towards its goals of creating technologically adept, legally compliant, ethically sound, and socially responsible solutions for emergency response.

3. Analysis of the regulatory framework of SYNERGISE first responder end-users

3.1. About this section[16]

This section provides an analysis of the regulatory framework applicable to FR end-users in five European countries: Poland, Germany, Sweden, Greece, and The Netherlands. The regulatory landscape encompasses a range of legal acts, policies, and standards aimed at ensuring the effective and safe utilisation of the technological solutions developed in SYNERGISE for emergency response operations, namely[17]:

- Cutting-edge, innovative and integrated tools/robots/drones featuring aerial, OWL – legged, ANYmal and crawling/version enabled-SNAKE for autonomous site exploration and victims detection.
- A novel device attached to the garment of First Responders for real-time vitals monitoring of first responders, gas/environmental sensing for potential toxics and explosives detection and identification.
- A reliable infrastructure-less advanced localisation system (as a wearable for FRs) to locate the first responders indoors and outdoors, seamlessly patched with outdoor positioning infrastructure.
- Advanced augmented reality services to operational & tactical response teams for robotic control, visualisation and remote collaboration.
- AI enabled synthesis and fusion of information for acquiring mission intelligence
- A ubiquitous, ad-hoc, rapidly deployable, high bandwidth field and HQ communications system to allow for quick information exchange and human-machine interaction for optimisation of exchange between devices and first responders.
- An interoperable Incident Management and Command and Control System to enhance multi-agency response and allow for effective mission deployment, resources and assets utilisation whilst enhancing situational awareness and sense-making at all times.

In this analysis, specific criteria have been applied to evaluate how regulatory provisions impact the development and implementation of technological solutions within the context of first responder operations. This analysis includes criteria from regulatory areas relevant to the technological solutions developed for FR operations, which complement each other by addressing different facets. Each regulatory area serves a distinct purpose in ensuring the effectiveness, safety, and ethical considerations of the implemented solutions:

- Data protection and privacy: this area ensures that personal and sensitive data collected during emergency response operations are handled in compliance with privacy laws and regulations. It protects the rights of individuals involved in emergencies while allowing for the necessary data exchange and utilisation for effective response.
- Cybersecurity and information protection: with the integration of cutting-edge technology like drones, robots, and wearable devices, cybersecurity becomes paramount. This regulatory area ensures that the systems and networks used by first responders are secure

[16] The web links of the regulatory frameworks analysed in this section have been verified to be functional at the date of submission of the report (i.e. April 2024).
[17] Extracted and merged from SYNERGISE's Grant Agreement (pp. 113-123, which refer to sections 1.1.3, 1.1.4, 1.2.1, and 1.2.2), and from SYNERGISE's webpage: [https://www.synergise-project.eu/coverage/press-release-new-international-consortium-to-design-disaster-management-solution/; https://www.synergise-project.eu/aims-and-objectives/]

from cyber threats, preventing unauthorised access and potential disruptions during critical operations.

- Interoperability and technical standards: in emergency response scenarios, seamless communication and coordination among different agencies and technologies are essential. Interoperability standards facilitate the integration of diverse technological solutions, enabling smooth data exchange and collaboration between first responders and various response teams.
- Health and safety: given the nature of emergency response operations, ensuring the health and safety of first responders is of utmost importance. Regulations in this area focus on the design and implementation of technologies to minimise risks to responders, such as real-time vitals monitoring, environmental sensing for toxins, and ensuring ergonomic designs of equipment.
- Ethics and Artificial Intelligence (AI): as AI and robotics play increasingly significant roles in emergency response, ethical considerations become crucial. Regulations in this area ensure that AI algorithms are transparent, fair, and accountable, addressing concerns such as bias, discrimination, and the ethical use of autonomous systems in sensitive situations.

The regulatory areas cover the main aspects of interest in technological solutions for first responder operations by addressing both the technical and ethical dimensions of implementation:

- Technical aspect: regulations on data protection, cybersecurity, interoperability, and technical standards focus on ensuring the reliability, functionality, and compatibility of the technological solutions deployed. They ensure that systems operate securely, communicate effectively, and integrate seamlessly with existing infrastructure.
- Normative aspect: regulations concerning health and safety, as well as ethics and AI, address the ethical considerations inherent in deploying advanced technologies in emergency response. They ensure that the use of technology respects human dignity, prioritises safety, and upholds ethical principles, particularly in sensitive situations where lives are at stake.

By covering these main aspects of interest comprehensively, the regulatory framework provides a holistic approach to the development and implementation of technological solutions for first responder operations. It balances the need for innovation and efficiency with the imperative to protect privacy, ensure security, promote interoperability, safeguard health, and uphold ethical standards. Each country's regulatory environment is examined individually, highlighting relevant legislation, policies, and guidelines. Additionally, the scope and identification of regulatory areas within each country and regulation are outlined to provide a comprehensive understanding of the regulatory framework's implications for FR operations. Through this detailed examination, insights are gained into how end-users' regulatory framework addresses the unique challenges and requirements of FR operations. The subsequent sections of this deliverable will similarly explore the regulatory landscapes of Poland, Germany, Sweden, Greece, and The Netherlands, providing a comparative analysis of the regulatory frameworks across these countries. By examining the regulatory approaches of multiple European nations, this analysis aims to identify commonalities, differences, emerging trends and needs in regulatory practices concerning FR end-users, thereby facilitating a deeper understanding of the regulatory context for technological solutions in emergency response operations.

3.2. Poland

Table 2. Poland's regulatory landscape overview

REGULATION	REGULATORY AREA	LINK
USTAWA z dnia 10 maja 2018 r. o ochronie danych osobowych (ACT of May 10, 2018 on the protection of personal data)	Data protection and privacy.	https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-danych-osobowych-18722262
USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (ACT of July 5, 2018 on the national cybersecurity system)	Cybersecurity and information protection; Interoperability and technical standards; Health and safety.	https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/krajowy-system-cyberbezpieczenstwa-18746756
USTAWA z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (ACT of 16 July 2004 Telecommunications law)	Interoperability and technical standards; Health and safety.	https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/prawo-telekomunikacyjne-17116702
USTAWA z dnia 7 kwietnia 2022 r. o wyrobach medycznych (ACT of April 7, 2022 about medical devices)	Health and safety.	https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/wyroby-medyczne-19238461
Polityka dla rozwoju sztucznej inteligencji w Polsce (Policy for the Development of Artificial Intelligence in Poland)[18]	Interoperability and technical standards; Health and safety; Ethics and AI.	https://www.gov.pl/attachment/928200fa-b1a6-4c0c-b3a8-d1fbf1e1175a

[18] Not a regulation, but a national strategy.

Table 3. Regulatory analysis of Poland's framework

REGULATORY AREA	SCOPE	IDENTIFICATION
Data protection and privacy	*Limited collection: Only collect personal and sensitive data strictly necessary for the response operation.*	This relates to the principle of data minimisation, which stipulates that only personal and sensitive data strictly necessary for the response operation should be collected. This aligns with Article 5 of the GDPR (EU General Data Protection Regulation), which Poland has implemented in its national law. Polish law would require that any processing of personal data by first responders be done in such a way that only data necessary for the specific purposes of the response operations are collected.
	Secure storage: Implement robust security measures to protect stored data.	Provisions on the security of personal data are designed to protect stored data against unauthorised access, disclosure, alteration and destruction. These security measures are detailed in Article 32 of the GDPR, which requires the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Polish law reflects these requirements, requiring controllers and processors of personal data to ensure the protection of personal data.
	Specific use: Use data only for emergency response purposes, ensuring respect for privacy.	The use of personal data exclusively for emergency response purposes ensures respect for privacy. This relates to the purpose limitation principle, which states that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. This is consistent with Article 6 of the GDPR, which provides the legal basis for the processing of personal data, including processing for tasks carried out in the public interest or in the exercise of official authority vested in the controller, which would be applicable in the context of first responders.
Cybersecurity and information protection	*Protection against cyber-attacks: Adopt cybersecurity strategies to safeguard information and communication systems.*	Article 8 of "USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa" (Act on the National Cybersecurity System), establishes the obligation for operators of key services to implement a security management system in information systems used to provide a key service, which includes measures for protection against cyber-attacks.
	Information integrity: Maintain the accuracy and timeliness of critical information.	Although information integrity is a central concept in cybersecurity management and is addressed indirectly through various provisions requiring the implementation of security measures, specific reference to information integrity is not identified in the available excerpts. However, it can be inferred that it is included in the general security obligations set out, for example, in article 8 of the "USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa" (Act on the National Cybersecurity System), by requiring technical and organisational measures for risk management and information security.
	System resilience: Ensure continuity and recovery of operations in the event of security incidents.	Article 8 (Act on the National Cybersecurity System), again, is relevant here as the security management measures to be implemented include not only protection against attacks but also resilience and continuity of key services in the event of security incidents, which contributes to the resilience of the system.

REGULATORY AREA	SCOPE	IDENTIFICATION
Interoperability and technical standards	*Interagency compatibility: Facilitate communication and coordination between different response agencies.*	Article 11 of the "USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa" (Act on the National Cybersecurity System), sets rules for key service operators on the obligation to handle incidents, report serious incidents and cooperate in handling serious incidents and critical incidents. Similarly, art. 18 imposes analogous obligations on digital service providers, art. 22 on public entities, art. 26 on other incident response teams (including cooperation with law enforcement agencies, art. 34), art. 42 on authorities competent in cybersecurity, and, finally, art. 51 on the Minister of National Defense. On the other hand, the "Policy for the Development of Artificial Intelligence in Poland" elaborates an AI ecosystem to include the cooperation between end-users (armed forces, government, healthcare, societal organisations...), public sector, entrepreneurs, industry, research, etc. (p. 83), but there is no particular mention of disaster settings. On the contrary, the "USTAWA z dnia 16 lipca 2004 r. Prawo telekomunikacyjne" (Telecommunications Law), in its Section VIII, sets obligations of telecommunications entrepreneurs in situations of special threats, including cooperation with other telecommunications entrepreneurs, entities and services performing tasks in the field of rescue (art. 176a).
	Adoption of standards: Follow common technical standards to ensure interoperability of equipment and systems.	Article 42.8 of the "USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa" (Act on the National Cybersecurity System), establishes recommendations for authorities competent for cybersecurity on actions aimed at strengthening cybersecurity, including sectoral guidelines on reporting incidents referred to in section 1 point 5, is prepared taking into account in particular the Polish Standards transposing European standards, common technical specifications, understood as technical specifications in the field of ICT products defined in accordance European laws and guidelines. Moreover, the "USTAWA z dnia 16 lipca 2004 r. Prawo telekomunikacyjne" (Telecommunications Law), establishes the content that a telecommunication access agreement should include, art. 31.2: a) "in the field of interoperability of services, network integrity, procedures in situations of special threats and failures, maintaining telecommunications secrecy and data protection in the network". In the field of AI, the Framework for the Polish AI ecosystem of the "Policy for the Development of Artificial Intelligence in Poland" focuses, among other aspects, on technical and organisational standards: technical standards, mutual recognition of certificates and certificates of conformity, rules for interoperability and data management standards (p. 86). Then, one of its next steps is established as "promoting open interoperability standards, including mutual recognition of certificates and compliance protocols" (p. 75). In this topic, international cooperation remains a cornerstone for "ensuring interoperability of AI-based solutions developed in Poland with widespread standards, norms and solutions" (p. 58).
	Operational flexibility: Enable integration and adaptation of new technologies as needs and capabilities evolve.	Scarce references can be found in relation to this item. The "USTAWA z dnia 16 lipca 2004 r. Prawo telekomunikacyjne" (Telecommunications law), states in its art. 139a.4 that when concluding an investment agreement, the President of UKE (Office of Electronic Communications) shall take into account the needs of end users, market needs and the development of telecommunications technology. In the same vein, one of the "Policy for the Development of Artificial Intelligence in Poland" short-term objectives of AI in the public sector is set as "enhancing the ability of the state to use AI in emergency situations to forecast threats and support decision-making, as well as in situations requiring intervention or support from various government bodies at different levels" (p. 70).
Health and safety	*Proven effectiveness: Verify that devices and systems meet performance and security standards.*	In the field of safety, the "USTAWA z dnia 7 kwietnia 2022 r. o wyrobach medycznych" (Medical Devices Act), this aspect is indirectly addressed through the requirements for conformity assessment and clinical studies necessary to demonstrate the safety and performance of medical devices before they are placed on the market. However, a detailed analysis is needed of specific sections such as art. 29 related to the exception to conformity assessment procedures, and art. 31 on the opinion of the bioethics committee, which may involve efficacy assessments for exceptional situations or clinical studies. Also, chapter 13 is devoted to setting out "use and maintenance of products" requirements. From the point of view of artificial intelligence, the "Policy for the Development of Artificial Intelligence in Poland" conclusions and next steps include "supporting projects in the field of e-Health, including activities aimed at the interoperability of existing systems" (p. 75).

REGULATORY AREA	SCOPE	IDENTIFICATION
	Risk prevention: Identify and mitigate potential hazards associated with the use of technologies in emergency contexts.	In the "USTAWA z dnia 7 kwietnia 2022 r. o wyrobach medycznych" (Medical Devices Act), articles relating to the reporting of serious incidents, such as art. 48, indirectly contribute to risk prevention by requiring the reporting of incidents that could negatively impact patient safety. Art. 50 details the process of banning or restricting a medical device, and art. 51 details the process of introducing requirements or restrictions to those devices. On the other hand, the "USTAWA z dnia 16 lipca 2004 r. Prawo telekomunikacyjne" (Telecommunications law), in its Chapter 3, sets requirements for radio devices with a special emphasis on 1) protecting the health and safety of people and pets and protecting property; 2) efficient use of frequency or orbital resources to avoid harmful interference; and 3) electromagnetic compatibility, specified in the regulations on electromagnetic compatibility, to the extent resulting from their intended use" (art. 153.1).
	Training and awareness: Provide the necessary training for the safe and effective use of technologies.	Although the "USTAWA z dnia 7 kwietnia 2022 r. o wyrobach medycznych" (Medical Devices Act) includes provisions on documentation and labelling of medical devices (e.g. art. 12), which could relate to training on the proper use of devices, no direct reference to specific training and awareness was found in the available fragments. On the contrary, although still scarce, we can see in article 51 of the "USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa" (Act on the National Cybersecurity System) that the following are tasks of the Minister of National Defense: 3) developing the skills of the Armed Forces of the Republic of Poland in ensuring cybersecurity by organizing specialised training projects; 4) acquiring and developing tools to build cybersecurity capabilities in the Armed Forces of the Republic of Poland. Finally, in the "Policy for the Development of Artificial Intelligence in Poland", it is established that actions in the ecosystem are supposed to "foster learning, training skills and development of competencies in the field of AI" (p. 81). However, no particular reference to first responder operations and disaster management is described in the above-mentioned regulations.
Ethics and AI	*Algorithmic transparency: Ensure that AI decision processes are understandable and auditable.*	This aspect is reflected throughout the document in different sections and paragraphs. Then, direct references to the ethical requirements of transparency can be found in sections 2 (a), p.72, 2, p.69, 2 (d,f,p), p.25, referring to the short-term objectives and, on the other hand, in section 11, p.75 where the conclusions and next steps regarding the ethical development of AI are set out.
	Accountability in decision-making: Clearly establish accountability for AI-supported decisions.	This aspect is reflected throughout the document in different sections and paragraphs. Then, direct references to the ethical requirements of transparency can be found in sections 2 (a), p.72, 2, p.69, 2 (d,f,p), p.25, referring to the short-term objectives and, on the other hand, in section 11, p.75 where the conclusions and next steps regarding the ethical development of AI are set out.
	Fairness and non-discrimination: Implement measures to avoid algorithmic bias and ensure fair decisions.	The treatment of areas related to equity, non-discrimination and algorithmic biases are treated unevenly throughout the document. Although the issue of bias is mentioned on pp. 25, 69 and 72, it is not extensively developed. Specific actions can be found in articles 2.a, p.69 and 2.a, p.72, where it is stated that measures will be introduced to mitigate potential errors and prevent them. Similarly, on p.72, the creation of a dynamic code of ethics is proposed to help prevent potential algorithmic biases. Regarding non-discrimination, it is mentioned as one of the fundamental pillars of AI development. On the other hand, on pp.25.3.f and 71.8.d in the short-term oriented actions, clear emphasis is placed on the importance of minimising the risk of discrimination in different sectors such as the public sector and the importance of this principle is stressed.

3.3. Germany

Table 4. Germany's regulatory landscape overview

REGULATION	REGULATORY AREA	LINK
Bundesdatenschutzgesetz (BDSG), vom 30. Juni 2017 (Federal Data Protection Act)	Data protection and privacy; Health and safety.	https://www.gesetze-im-internet.de/bdsg_2018/
Gesetz zur Erhöhung der Sicherheit informationstechnischer System (IT-Sicherheitsgesetz), vom 17. Juli 2015 (IT Security Act)	Interoperability and technical standards.	https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1709723965829
Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, vom 18. Mai 2021 (Second law to increase the security of information technology systems)	Cybersecurity and information protection; Health and safety.	https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1709724073613
Cyber Security Strategy for Germany	Cybersecurity and information protection.	https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html
Medizinproduktegesetz in der Fassung der Bekanntmachung (MPG), vom 7. August 2002 (Medical Devices Act)	Health and safety.	https://www.buzer.de/gesetz/3284/index.htm
Telekommunikationsgesetz (TKG), vom 23. Juni 2021 (Telecommunications Act)	Interoperability and technical standards; Health and safety.	https://www.gesetze-im-internet.de/tkg_2021/BJNR185810021.html
Strategie Künstliche Intelligenz der Bundesregierung Fortschreibung 2020 (Artificial Intelligence Strategy of the German Federal Government)[19]	Interoperability and technical standards; Health and safety; Ethics and AI.	https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf
BMBF - Aktionsplan Künstliche Intelligenz (Artificial Intelligence Action Plan)[20]	Health and safety; Ethics and AI.	https://www.ki-strategie-deutschland.de/files/downloads/Aktionsplan_Kuenstliche_Intelligenz_2023.pdf

[19] Not a regulation, but a national strategy.
[20] Not a regulation, but a national strategy.

Table 5. Regulatory analysis of Germany's framework

REGULATORY AREA	SCOPE	IDENTIFICATION
Data protection and privacy	*Limited collection: Only collect personal and sensitive data strictly necessary for the response operation.*	Article 22 of the "Bundesdatenschutzgesetz" (Federal Data Protection Act), states that the processing of special categories of personal data within the meaning of Article 9(1) of Regulation (EU) 2016/679 is allowed if it is necessary to prevent a significant threat to public security; or if it is necessary for imperative reasons of defence or for the fulfilment of supragovernmental or intergovernmental obligations of a federal public body in the field of crisis management or conflict prevention or for humanitarian measures
	Secure storage: Implement robust security measures to protect stored data.	Article 64 of the "Bundesdatenschutzgesetz" (Federal Data Protection Act), establishes requirements for data processing security: the data subjects associated with the processing shall take the necessary technical and organisational measures to ensure a level of protection appropriate to the risk when processing personal data, in particular with regard to the processing of special categories of personal data.
	Specific use: Use data only for emergency response purposes, ensuring respect for privacy.	Article 6 of the GDPR indicates that "processing shall be lawful only if and to the extent that at least one of the following applies": the data subject gave his or her consent to the processing of his or her personal data for one or more specific purposes. However, Federal Data Protection Act (BDSG), Section 49, states that the processing of personal data for a purpose other than that for which they were collected is permitted if the other purpose is one of the purposes specified in Section 45. The processing of personal data for another purpose not mentioned in Article 45 is permitted if it is provided for in a legal provision.
Cybersecurity and information protection	*Protection against cyber-attacks: Adopt cybersecurity strategies to safeguard information and communication systems.*	Throughout the Cyber Security Strategy for Germany, numerous references are made to cyber-attacks, their impact on various sectors, their growing number and the importance of taking them into account in order to improve the security of the systems that may be involved. Then, on different pages, e.g. p.36, p.46, p.49, p.55, p.57, p.70 etc., specific objectives are set out as to what the improvement of cyber security at national level is intended to achieve. For example, as reflected on p.36, it is stated that "Our aim is for consumers to be confident in the knowledge that products and services provide an appropriate level of cyber security and that complying with the required cyber security characteristics is governed by uniform regulation across the EU and later, about the measures, p.36 "The binding IT security requirements will increase the level of cyber security in the European digital single market and strengthen awareness in businesses and the research community of security issues. Infrastructure, employees, products and services will be more resilient in the face of cyber attacks". TThe aim is to create a robust and sustainable digital ecosystem that is able to respond to potential threats from cyber-attacks, and which can be broken down into 4 specific areas of action.
	Information integrity: Maintain the accuracy and timeliness of critical information.	Throughout the law "Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, vom 18. Mai 2021" albeit briefly, provisions are laid down for the control and preservation of the conditions of integrity of information and systems. Section 3 paragraph "The Federal Office promotes security in information technology in order to ensure the availability, integrity and confidentiality of information and its processing" or in § 7c (2) that "The protection objectives in accordance with paragraph 1 sentence 1 are the availability, integrity or confidentiality 1. "The objectives of protection under paragraph 1 sentence 1 are the availability, integrity or confidentiality of the communications technology of the federal government, a critical infrastructure operator, an undertaking with a special public interest or a digital service provider" or, on the other hand, § 8f (8) provides for the need to report "Disturbances in the availability, integrity, authenticity and confidentiality of its information...".

REGULATORY AREA	SCOPE	IDENTIFICATION
	System resilience: Ensure continuity and recovery of operations in the event of security incidents.	In particular, in Action Areas 3 dedicated to Strong and sustainable cyber security architecture for every level of government", p.78 y 4 "Germany's active role in European and international cyber security policy", p.106, different actions at both national and international level to ensure a resilient ecosystem against the threat of potential cyber-attacks. To this end, measures are proposed such as increasing collaboration between NATO member states and the European Union, improving investment and creating common frameworks for development and action in the face of cyber-attacks. In short, the aim is to
Interoperability and technical standards	*Interagency compatibility: Facilitate communication and coordination between different response agencies.*	No mentions of disasters and crisis management. However, there are some articles concerning cooperation that could be applied in these settings. As modified through art. 1.7 of the "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT Security Act), the Federal Office may only provide third parties, upon request, with certain information if this does not conflict with the legitimate interests of the critical infrastructure operator concerned and the information is not expected to adversely affect essential security interests (access to personal data shall not be granted).
	Adoption of standards: Follow common technical standards to ensure interoperability of equipment and systems.	In the "Telekommunikationsgesetz" (Telecommunications Act), Part 10 addresses Public Safety and Emergency Preparedness, while reminding that international standards must be taken into account when making the specifications in the technical guidelines (art. 164). Specifically, art. 165 establishes some technical and organisational protective measures.
	Operational flexibility: Enable integration and adaptation of new technologies as needs and capabilities evolve.	It is stated in the "Artificial Intelligence Strategy of the German Federal Government" that "in some areas of the administration's remits involving ever-higher data volumes, for instance earth observation/remote sensing, further developing automated data analysis procedures with AI methods is a necessary prerequisite for harnessing the potential for the federal administration's work, inter alia in disaster control, to be exploited at all" (p. 21).
Health and safety	*Proven effectiveness: Verify that devices and systems meet performance and security standards.*	Firstly, art. 64 of the "Bundesdatenschutzgesetz" (Federal Data Protection Act) sets out requirements for the security of data processing, including devices and technologies. Also, in art. 1.20 of the "Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (Second IT Security Act), it is established that the national authority for cybersecurity certification is the Federal Office (Das Bundesamt). Concerning technological devices, arts. 6-8 of the "Gesetz über Medizinprodukte" (Medical Devices Act) define requirements as well as harmonised standards and technical specifications for medical devices. In art. 178 of the "Telekommunikationsgesetz" (Telecommunications Act), obligations are established to ensure that data stored is protected against unauthorised access, provision which could be applied to the design and management of this project solutions that would store personal data. Concerning AI, the "Artificial Intelligence Strategy of the German Federal Government" states that "AI-based products and services need to be as safe to use as any other product [...]. The Federal Government is therefore advocating and working towards a suitable regulatory framework, adapted to reflect AI-specific issues if and where appropriate, within which the existing quality infrastructure is expanded and, if necessary, developed further. By setting clear rules, standards, the fundamental rights of citizens can be protected, trust in AI can be strengthened, sustainable deployment of AI as well as innovation and competition can be promoted" (p. 5).
	Risk prevention: Identify and mitigate potential hazards associated with the use of technologies in emergency contexts.	Art. 4 of the "Gesetz über Medizinprodukte" (Medical Devices Act) establishes certain prohibitions to market, install, commission, operate or use medical devices in order to protect the safety and health of patients, users and third parties, which can be applied in emergency settings. Also, the fifth section of the "Gesetz über Medizinprodukte" (Medical Devices Act) is dedicated to monitoring and protection from risks (arts. 25-31). Regarding artificial intelligence and a human-centric point of view, one of the goals established in the BMBF-Aktionsplan Künstliche Intelligenz" (Artificial Intelligence Action Plan) is to increase "civil security through the use of of AI-based and user-friendly digital tools, digital tools" (p. 19).

REGULATORY AREA	SCOPE	IDENTIFICATION
	Training and awareness: Provide the necessary training for the safe and effective use of technologies.	Arts. 26, 30 and 31 of the "Gesetz über Medizinprodukte" (Medical Devices Act) include provisions regarding training for monitoring employees, safety officers and medical device consultants. However, no provisions are specified for first responders' capacity building and training. Additionally, and as above with no references to first responders, it is stated in the "Artificial Intelligence Strategy of the German Federal Government" that AI modules' integration in education and training in the field of healthcare is of utmost importance (p. 11).
Ethics and AI	*Algorithmic transparency: Ensure that AI decision processes are understandable and auditable.*	The treatment of algorithmic transparency throughout the documents turns out to be rather brief. Only a few references emerge from both documents. However, a clear commitment to ensure practices dedicated to compliance with the principle of transparency can be observed. For example, "**The Federal Government is committed to principles such as respect for human rights, data protection and other European and international premises such as transparency and traceability and decisions.p.22 (2). This commitment is expressed when it is stated that model guidelines for "usage and deployment scenarios on topics such as data protection and data management, accountability, control and transparency, as well as inclusion and societal well-being, p. 23 (1)" will be developed. 23 (1)", special actions on high-risk AI tools "must meet special requirements regarding transparency, p. 28 (1) or, finally, when design and development work is intended to introduce a risk-adequate level of transparency and traceability as well as, if necessary, an appropriate control structure and verifiability of AI applications and their results, p. 26(2).
	Accountability in decision-making: Clearly establish accountability for AI-supported decisions.	In the Artificial Intelligence Strategy of the Federal Government there are no references to accountability in decision-making. However, some references - albeit tangential and reduced - can be found in the document BMBF-Aktionsplan Künstliche Intelligenz. Specifically, if we stick to direct references, there is only one on p. 23, where the main objectives are presented and the following is stated: "Develop guidelines for usage and deployment scenarios on topics such as data protection and data management, accountability, control and transparency, as well as inclusion and societal well-being".
	Fairness and non-discrimination: Implement measures to avoid algorithmic bias and ensure fair decisions.	The BMBF-Aktionsplan Künstliche Intelligenz does not contain any references to possible bias or discriminatory elements. In contrast, albeit briefly, there are some references to bias and possible discrimination in the Artificial Intelligence Strategy of the German Federal Government. In particular, on p. 25 it states that "When using AI, effective protection against discrimination, manipulation or other misuse must also be ensured. The more societal diversity - including the proportion of all genders - is reflected in the teams developing AI applications, the more likely it is that prejudice and discrimination will be avoided from the outset. The Federal Government will advocate these principles at the national, European and international levels. Furthermore, the commitment to the development of more ethical AI is reflected in the statement on p. 21 that "It is of great importance to continue to apply high standards to the introduction and use of AI and to design it in a non-discriminatory and comprehensible way in accordance with existing regulations for the protection of personal data, information security requirements and the protection of personal data. personal data protection, information security requirements and the protection of citizens' trust and confidence".

3.4. Sweden

Table 6. Sweden's regulatory landscape overview

REGULATION	REGULATORY AREA	LINK
Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (Act with supplementary provisions to the EU's data protection regulation)	Data protection and privacy.	https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218/ sfs-2008-355/
Patientdatalag (2008:355) (Patient Data Act)	Health and safety.	https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355/
Säkerhetsskyddslag (2018:585) (Security Protective Act)	Interoperability and technical standards; Health and safety.	https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-2018585_sfs-2018-585/
A national cyber security strategy	Cybersecurity and information protection; Interoperability and technical standards; Health and safety.	https://www.government.se/legal-documents/2017/11/skr.-201617213/
Luftfartslag (2010:500) (Aviation law)	Interoperability and technical standards; Health and safety.	https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/luftfartslag-2010500_sfs-2010-500/
Kamerabevakningslag (2018:1200) (Camera Surveillance Act)	Interoperability and technical standards.	https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/kamerabevakningslag-20181200_sfs-2018-1200/
Arbetsmiljölag (1977:1160) (Working environment act)	Health and safety.	https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/arbetsmiljolag-19771160_sfs-1977-1160/
Patientsäkerhetslag (2010:659) (Patient Safety Act)	Interoperability and technical standards; Health and safety.	https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/patientsakerhetslag-2010659_sfs-2010-659/
Lag (2022:482) om elektronisk kommunikation (Law on electronic communications)	Interoperability and technical standards.	https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482/
Nationell inriktning för artificiell intelligens (National approach to artificial intelligence)[21]	Interoperability and technical standards; Health and safety; Ethics and AI.	https://www.regeringen.se/contentassets/cb7f277635ae49bc9a04899c2e1af8cf/national-approach-to-artificial-intelligence-pa-engelska.pdf

[21] Not a regulation, but a national strategy.

Table 7. Regulatory analysis of Sweden's framework

REGULATORY AREA	SCOPE	IDENTIFICATION
Data protection and privacy	*Limited collection: Only collect personal and sensitive data strictly necessary for the response operation.*	Chapter 3 of law (2018/218) on the "processing of certain categories of personal data" talks about sensitive personal data addresses this issue. Specifically, it says: "Sensitive personal data may be processed for archiving purposes in the public interest with the support of Article 9.2 j of the EU data protection regulation, if the processing is necessary for the personal data controller to comply with the archiving regulations."
	Secure storage: Implement robust security measures to protect stored data.	National legislation does not refer to this storage security. However, the directly applicable GDPR, in Article 32 GDPR states that: "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, where applicable".
	Specific use: Use data only for emergency response purposes, ensuring respect for privacy.	Chapter 4 of law (2018/218), regarding "Restrictions on use", states that personal data processed solely for archiving purposes in the public interest may be used to take measures in relation to the data subject only if there are exceptional grounds for doing so, taking into account the vital interests of the data subject.
Cybersecurity and information protection	*Protection against cyber-attacks: Adopt cybersecurity strategies to safeguard information and communication systems.*	With regard to protection and prevention against cyber-attacks, the National Cybersecurity Strategy, on p. 8, mentions several measures to be prioritised: a) ensuring a systematic and comprehensive approach to cybersecurity efforts b) improving the security of networks, products and systems c) improving the capacity to prevent, detect and manage cyber-attacks and other cyber incidents d) increasing the possibility of preventing and combating cybercrime e) increasing knowledge and promoting expertise f) improving international cooperation. In addition, section 2.3, pp. 16-18 on "Improving the ability to prevent, detect and manage cyber-attacks and other cyber incidents" details concrete objectives and measures to prevent, detect and respond to cyber-attacks and other cyber incidents. Specifically, for example, the government will work on the following: a) ensuring coordinated planning between authorities in the event of a cyber attack or other serious cyber incident, b) ensuring that activities requiring continuous monitoring and with particular protection needs are given access to a sensor system or a detection and warning system, c) ensuring the continuous development and strengthening of an effective and seamless cyber defence with the capability to prevent, detect and manage cyber attacks, both for military and civilian activities, which also includes the Swedish Armed Forces developing their capability to defend Sweden against attackers when they are able to detect, detect and manage cyber attacks cyber attacks, both for military and civilian activities, which also includes the Swedish Armed Forces developing their capability to defend Sweden against skilled attackers in cyberspace.
	Information integrity: Maintain the accuracy and timeliness of critical information.	Throughout the Strategy, the importance of "achieving an effective and secure management of information", p. 4 and, in addition, preserving its confidentiality, integrity and availability in case of possible cyber-attacks, p. 5, is stated. As noted in the Strategy, the protection of information is covered by the following regulatory framework: Protective Security Act (1996:627), Ordinance (2015:1052) on Emergency Preparedness and Surveillance Responsible Authorities' Measures at Heightened Alert, Archives Act (1990:782), the Personal Data Act (1998:204) and the Electronic Communications Act (2003:389). Linked to this are future revisions and extensions of legislation to improve and extend the Swedish protection framework, in particular the provisions of (SOU 2015:25) and Directive (EU) 2016/1148 relating to a common level of security of networks and systems across the Union. In addition, as concrete actions, research has also been carried out to understand the state of cybersecurity in Sweden. As mentioned in "Swedish National Audit Office's audits of information security in public administration (RIR 2016:8, RIR 2014:23)" and The report Cyber security in Sweden (SOU 2015:23), p.6. The importance of bodies such as "The Cooperation Group for Information Security (SAMFI)" in preserving and maintaining information integrity and the importance of citizenship is also highlighted.

REGULATORY AREA	SCOPE	IDENTIFICATION
	System resilience: Ensure continuity and recovery of operations in the event of security incidents.	The treatment of this issue in a particular sense is very limited throughout the Strategy, with only one reference to it in the entire document, p. 26, where the commitment to reduce vulnerabilities of systems and improve their resilience is stated. In particular, the concept of resilience seems to be subsumed within the concept of cybersecurity, rather than as a stand-alone concept. Therefore, actions and measures dedicated to cybersecurity in a broad sense can also be understood indirectly as measures to improve the resilience of systems such as those set out on p.21, among others: a) ensure that the law enforcement authorities work systematically to develop expertise and working methods to prevent and combat cybercrime, b) increase the awareness and knowledge of non-law enforcement authorities regarding how they can contribute in the work to prevent cybercrime, c) strengthen the international cooperation against cybercrime in order to increase legal proceedings in Sweden
Interoperability and technical standards	*Interagency compatibility: Facilitate communication and coordination between different response agencies.*	With brief mentions throughout the different documents, this aspect is covered by the following provisions. In "A national cyber security strategy", for the strategic priority of securing a systematic and comprehensive approach in cyber security efforts, the objective is that central government authorities, municipalities, county councils, companies and other organisations are to have knowledge of threats and risks, assume responsibility for their cyber security and conduct systematic cyber security efforts (p. 8). As stated later, collaboration and cyber security information sharing is to be enhanced (p. 10). Also, in the "Patientsäkerhetslag" (2010:659) (Patient Safety Act), chapter 6, section 5: the health and medical care staff must, in matters concerning children who are harmed or at risk of harm, cooperate with community bodies, organisations and others who are affected. Similarly, in the "Säkerhetsskyddslag" (2018:585) (Security Protective Act), chapter 4, section 1 states that a security protection agreement must be entered when collaboration or cooperations include members that can can gain access to security classified information or security-sensitive activities, with more provisions concerning cooperation in the following sections within that chapter.
	Adoption of standards: Follow common technical standards to ensure interoperability of equipment and systems.	This being a parallel area in many of the solutions envisaged, some references can be seen. In "A national cyber security strategy", for the strategic priority of securing a systematic and comprehensive approach in cyber security efforts, the objective is that there is to be a national (common) model to support systematic cyber security efforts (to be able to coordinate and collate regulations, methods, tools, training, etc) (pp. 8-9). In the field of AI, the "National approach to artificial intelligence", acknowledges that Sweden needs to develop rules, standards, norms and ethical principles to guide ethical and sustainable AI and the use of AI and to prevent risks" (p. 10). In addition, the "Lag (2022:482) om elektronisk kommunikation" (Law on electronic communications), sets out in its chapter 5, section 16 that an operator that is a company with significant influence on a market may be ordered to fulfil reasonable requirements for access to and use of networks and associated facilities for the purpose of providing electronic communication services. Such an obligation may mean that the operator must: give access to network parts or services, or technical interfaces, protocols and other key technologies necessary for interoperability between services; offer specified services required to ensure interoperability between services all the way to the end users, or carry out interconnection or otherwise take measures so that networks or associated facilities can be connected, which can clearly relate to a rescue operation, among others.

REGULATORY AREA	SCOPE	IDENTIFICATION
	Operational flexibility: Enable integration and adaptation of new technologies as needs and capabilities evolve.	This need is acknowledged and facilitated through the following provisions. In the "Luftfartslag" (2010:500) (Aviation law), chapter 1, section 9, it is stated that in the case of aircraft that have no pilot on board or are not powered by an engine or that are otherwise of a special nature, the government or the authority designated by the government may issue regulations or, in an individual case, decide on exemptions and otherwise notify the necessary regulations. Exceptions and regulations may not be designed in such a way that they conflict with aviation safety or the public interest. In the case of such objects which are set up for movement in the air but which are not to be considered as aircraft, special regulations apply. That way, the potential usefulness of unmanned aircraft such as drones is considered. Moreover, in the "Kamerabevakningslag" (2018:1200) (Camera Surveillance Act), section 16: information about camera surveillance and information about the processing of personal data that camera surveillance entails do not need to be provided at surveillance conducted in an emergency from an aircraft if the monitoring is important: to prevent or detect a criminal activity; avert an imminent danger of an accident, limit the effects of an accident that has occurred or reduce the risk of new accidents; or investigate a missing person. This special provision facilitates and standardises its use[22].
Health and safety	*Proven effectiveness: Verify that devices and systems meet performance and security standards.*	In the "Patientdatalag" (2008:355) (Patient Data Act), chapter 1, section 2, it is stated that information management in health care must be organised so that it caters for patient safety and good quality and promotes cost-effectiveness. The privacy of patients and other data subjects must be respected, and documented personal data must be handled and stored so that unauthorised persons do not gain access to them. This approach covers the collection and management of medical data from first responders with wearables. Also, from the cybersecurity perspective, in "A national cyber security strategy", for the strategic priority of enhancing network, product and system security, the objective is that electronic communications are to be effective, secure and robust and are to meet the needs of their users (p. 12). "If stakeholders in the areas of public order, safety, health and defence are to be able to fulfil their commissions, they need to be able to communicate securely with each other, both in everyday conditions and in crises. The ambition is to as far as possible be able to maintain electronic communications within the country even in situations where the surrounding region or parts of Sweden have been hit by various types of attack. This means that electronic communications are to be able to function independently of functions in other countries. It also means an increase in the demands on operational reliability and robustness to make us better able to resist attacks and ultimately war" (p. 13). Moreover, access to secure data encryption systems for IT and communications solutions are to meet society's needs (p. 14). Regarding drones, the Luftfartslag (2010:500) (Aviation law), in its chapter 1, section 11: the government or the authority that the government determines may issue regulations that equipment used in or for aviation must comply with certain standards when the equipment is important for flight safety. Finally, regarding work safety, the Arbetsmiljölag (1977:1160) (Working environment act), chapter 2, section 5: machines, tools and other technical devices must be procured and placed and used in such a way that reassuring safety is provided against ill health and accidents. Also, in its chapter 3, section 8: whoever manufactures, imports, transfers or hires out a machine, a tool, protective equipment or other technical device must ensure that the device offers reassuring safety against ill health and accidents.

[22] More information related to unmanned aircraft (drones), with special provisions for emergency services available at: [https://www.transportstyrelsen.se/sv/luftfart/luftfartyg-och-luftvardighet/dronare/regler-for-polis-ambulans-raddningspersonal-och-utryckningar/]
[https://www.transportstyrelsen.se/TSFS/TSFS%202017_110k.pdf]
[https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/skyddslag-2010305_sfs-2010-305/]

REGULATORY AREA	SCOPE	IDENTIFICATION
	Risk prevention: Identify and mitigate potential hazards associated with the use of technologies in emergency contexts.	Regarding risk assessment and minimisation, the following provisions apply. In the "Patientsäkerhetslag" (2010:659) (Patient Safety Act), chapter 6, section 4: The healthcare staff is obliged to contribute to maintaining a high level of patient safety. To this end, the staff must report to the care provider risks of health care injuries as well as events that have caused or could have caused a health care injury. In the Arbetsmiljölag (1977:1160) (Working environment act), chapter 4, section 5: if a job entails a risk of ill health or accidents, the government or the authority that the government determines may issue regulations on the obligation to arrange for a medical examination or vaccination or other preventive treatment against infection of those employed or to be employed in the work. At last, in "National approach to artificial intelligence", it is acknowledged that Sweden needs pilot projects, testbeds and environments for development of AI applications in the public and private sectors, that can contribute to the use of AI evolving in a safe, secure and responsible manner, and that Sweden needs to continue to develop efforts to prevent and manage the risks associated with AI (p. 8).
	Training and awareness: Provide the necessary training for the safe and effective use of technologies.	Although the statements are not clearly directed at the handling of new technologies in disaster contexts, the following can be noted. In the "Säkerhetsskyddslag" (2018:585) (Security Protective Act), chapter 2, section 4: Personnel Security personnel shall ensure that those who participate in security-sensitive activities have sufficient knowledge of security protection. More generally and related to cyberattacks, in "A national cyber security strategy", for the strategic priority of increasing knowledge and promoting expertise, the objective is that the knowledge of individual digital technology users regarding the most urgent vulnerabilities and needs for security measures is to increase (p. 21). "Both cross-sectoral and technical cyber security training is to be carried out regularly in order to enhance Sweden's capability to manage the consequences of serious IT incidents" (p. 23). Also, in the Arbetsmiljölag (1977:1160) (Working environment act), chapter 3, section 3: the employer must ensure that the employee is well informed of the conditions under which the work is carried out, and that the employee is informed of the risks that may be associated with the work. The employer must make sure that the employee has the necessary training and knows what he has to observe in order to avoid the risks at work. The employer must ensure that only workers who have received sufficient instructions are allowed access to areas where there is a significant risk of ill health or accidents.
Ethics and AI	*Algorithmic transparency: Ensure that AI decision processes are understandable and auditable.*	The treatment of this ethical aspect is very brief throughout the document "Nationell inriktning för artificiell intelligens" (National approach to artificial intelligence). The only references to the need for algorithmic transparency are on p.4 and p.8, when it states that the absence of transparency can lead to discriminatory consequences, loss of trust, economic damage and negative consequences for the democratic functioning of the country, and therefore "For these reasons, it is important for Sweden to work actively on the issues that AI is already raising". On the other hand, on p.8, it is stated as a requirement that "The use of AI algorithms must be transparent and comprehensible".
	Accountability in decision-making: Clearly establish accountability for AI-supported decisions.	Although succinct, there is some mention of aspects related to accountability in decision-making. Specifically, they can be seen on pp. 6 and 8. Specifically, on p. 6, the need for the responsible application of technology is set out. On the other hand, p. 8 states the importance of taking into account ethical, moral and legal aspects in the development of automated technologies and, furthermore, by way of an objective that "Sweden needs pilot projects, testbeds and environments for development of AI applications in the public and private sectors, that can contribute to the use of AI evolving in a safe, secure and responsible manner".
	Fairness and non-discrimination: Implement measures to avoid algorithmic bias and ensure fair decisions.	Likewise, this ethical aspect is very briefly and superficially covered in the document, with only one reference on p.4, when it is stated that biases can lead to possible discrimination among others. On the other hand, the specific terms of equity and non-discrimination are not specifically mentioned in the document.

3.5. Greece

Table 8. Greece's regulatory landscape overview

REGULATION	REGULATORY AREA	LINK
Νόμος 4624/2019 (Law on implementation measures of Regulation (EU) 2016/679 for the protection of natural persons against the processing of personal data and incorporation into national legislation of Directive (EU) 2016/ 680)	Data protection and privacy; Health and safety.	https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019
Νόμος 4961/2022 (Lawon emerging information and communication technologies, strengthening digital governance and other provisions)	Interoperability and technical standards; Health and safety; Ethics and AI.	https://www.e-nomothesia.gr/kat-demosia-dioikese/nomos-4961-2022-phek-146a-27-7-2022.html
Νόμος 5002/2022 (Law on procedure for removing the privacy of communications, cyber security and protection of citizens' personal data)	Interoperability and technical standards.	https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-5002-2022.html
Νόμος 4727/2020 (Law on digital Governance and Electronic Communications, and other provisions)	Interoperability and technical standards.	https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/nomos-4727-2020-phek-184a-23-9-2020-1.html
Νόμος 4577/2018 (Law on the incorporation into Greek legislation of Directive 2016/1148/EU for a high common level of security of network and information systems throughout the Union and other provisions)	Interoperability and technical standards.	https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4577-2018-phek-199a-3-12-2018.html
National Cybersecurity Strategy 2020-2025	Cybersecurity and information protection.	https://mindigital.gr/wp-content/uploads/2022/11/E%CE%9D-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf
Νόμος 3850/2010 (Law on the ratification of the Code of Laws for the health and safety of workers)	Health and safety.	https://www.e-nomothesia.gr/kat-ergasia-koinonike-asphalise/n-3850-2010.html
Προεδρικό Διάταγμα 82/2010 (Presidential Decree on Minimum health and safety standards regarding the exposure of workers to risks from natural factors (artificial optical radiation))	Health and safety.	https://www.elinyae.gr/ethniki-nomothesia/pd-822010-fek-145a-192010
Προεδρικό Διάταγμα 120/2016 (Presidential Decree on Minimum health and safety requirements regarding the exposure of workers to risks arising from natural factors (electromagnetic fields))	Health and safety.	https://www.elinyae.gr/ethniki-nomothesia/pd-1202016-fek-203a-26102016
Προεδρικό Διάταγμα 398/1994 (Presidential Decree on Minimum safety and health requirements when working	Health and safety.	https://www.elinyae.gr/ethniki-nomothesia/pd-3981994-fek-221a-19121994

REGULATION	REGULATORY AREA	LINK
with visual display screens)		
Υπουργική Απόφαση ΔΥ8δ/Γ.Π.οικ./130648/2009 (Ministerial Decision about medical technology products)	Health and safety.	https://www.e-nomothesia.gr/kat-ygeia/farmakeia/ya-du8d-gpoik-130648-2009.html
Βίβλος Ψηφιακού Μετασχηματισμού 2020-2025 (Digital Transformation Bible 2020-2025)[23]	Interoperability and technical standards; Ethics and AI.	https://digitalstrategy.gov.gr/vivlos_pdf

[23] Not a regulation, but a national strategy.

Table 9. Regulatory analysis of Greece's framework

REGULATORY AREA	SCOPE	IDENTIFICATION
Data protection and privacy	*Limited collection: Only collect personal and sensitive data strictly necessary for the response operation.*	Article 22 of Law 4624/2019 on the processing of special categories of personal data. Paragraph two provides that such data may only be used where it is absolutely necessary for reasons of essential public interest; necessary to prevent a significant threat to national security or public security or necessary to take humanitarian measures, and in these cases the interest of the processing outweighs the interest of the data subject.
	Secure storage: Implement robust security measures to protect stored data.	Article 22 (3) of Law 4624/2019 mentions that 'in the cases of the previous paragraphs (sensitive data), all appropriate and specific measures shall be taken to safeguard the interests of the personal data subject. "These include procedures for testing, evaluating and periodically assessing the effectiveness of technical and organisational measures to ensure the security of processing. For the security of personal data in general, Article 32 of the GDPR applies, which refers directly to the security of data processing.
	Specific use: Use data only for emergency response purposes, ensuring respect for privacy.	Article 24 of Law 4624/2019 states that the processing of personal data by public bodies for a purpose other than that for which they have been collected is permitted when such processing is necessary for the performance of the functions assigned to them and provided that it is: it is necessary to verify the information provided by the person concerned, because there are reasonable grounds to believe that this information is incorrect; necessary to prevent risks to national security, national defence or public security or to ensure tax and customs revenues; necessary for the prosecution of criminal offences; necessary to avoid serious harm to the rights of another person; e) necessary for the production of official statistics.
Cybersecurity and information protection	*Protection against cyber-attacks: Adopt cybersecurity strategies to safeguard information and communication systems.*	Throughout the National Cybersecurity Strategy, the concrete actions and measures dedicated to the protection against cyber-attacks are described in the 5 strategic objectives and in the 15 specific objectives that are related to them, pp.24-27. Specifically, the five strategic objectives are: 1) a functional cybersecurity governance system, 2) shielding critical infrastructures and securing new technologies, 3) incident management optimisation, fight against cybercrime and privacy protection, 4) a modern environment for cybersecurity investments with emphasis on the promotion of research and development and finally, 5) capacity building, promoting information and awareness raising. Regarding the 15 specific objectives: 1.a.: optimise organisational structures and procedures;1b: apply vigorous risk assessment and effective contingency planning; 1.c.: strengthen national, European and international collaborations; 2.a.: comprehend technological developments and their effects on digital governance; 2.b: upgrade critical infrastructure protection; 2.c.: consolidate systems and applications by implementing enhanced security requirements; 3.1.: optimise methods, techniques and tools utilised in incident analysis, response and reporting; 3.b.: strengthen deterrence mechanisms and enhance operational cooperation; 3.c.: cybersecurity for the protection of privacy;4.a.: encourage R&D initiatives; 4.b.: provide investment incentives; 4.c: utilise PPPs; 5.a. building capacity by organising cybersecurity exercising activities; 5.b.: apply state - of - the - art educational and training methods and tools; 5.c.: promote open - ended cybersecurity information and awareness raising for Entities and citizens.
	Information integrity: Maintain the accuracy and timeliness of critical information.	The measures dedicated to maintaining the integrity of information, although they do not receive specific and special treatment throughout the strategy, can be derived from what is set out in strategic objective n.3 dedicated to "Incidental management optimisation, fight against cybercrime and privacy protection", p.55, and in the specific objectives dedicated in the section. However, there is a problem with this issue, as stated on p.50 when it is stated that "There is no information security framework, no commitment of the Administration for the protection of information systems" and that, as part of the actions of the national cybersecurity authority, it is intended to be remedied by "The issuance of guidelines and instructions regarding Cybersecurity for the protection of information assets, in accordance with security", p.51.

REGULATORY AREA	SCOPE	IDENTIFICATION
	System resilience: Ensure continuity and recovery of operations in the event of security incidents.	The treatment of resilience issues is briefly but specifically addressed in strategic objective 2 "to secure critical infrastructure and secure new technologies" and specifically when it is stated that one of the concrete actions should be "To ensure the resilience of systems supporting critical services against threats, by implementing appropriate testing procedures and technical audits of OES and DSPs, in cooperation with relevant competent entities "p.51 and one of the technical objectives "To ensure resilience and continuity", p.48.
Interoperability and technical standards	*Interagency compatibility: Facilitate communication and coordination between different response agencies.*	Νόμος 4961/2022 establishes and regularises several national bodies for cooperation in security issues, such as the National Cyber Security Certification Authority or the Coordinating Committee on Artificial Intelligence, among others. However, they are not envisaged to be of use in emergency situations in this law. On other side, while focusing on cyber threats, the Νόμος 5002/2022, in its articles 20 and 21, establishes a Coordination Committee for Cyber Security issues, the coordinating body between: a) the General Directorate of Cybersecurity of the General Secretariat of Telecommunications and Posts of the Ministry of Digital Governance; b) the Directorate of Cyber Defense of the General Staff of National Defense, designated as the competent response team for computer security incidents; c) the Directorate of Cyberspace of the E.Y.P. as a cyber attack response team (National CERT); and d) of the Greek Police. It is tasked with planning, monitoring, coordinating actions, intervening in issues related to cyber security from the initial stage of prevention to the stage of effective response to cyber-attack incidents and minimising the impact of cyber threats. Similarly, the Νόμος 4577/2018, article 8, regarding the Computer Security Incident Response Team (CSIRT), states that it is the Competent Response Team for computer security incidents and is responsible for risk management and incidents. It shall ensure a high level of availability of its communications services, avoiding single points of failure and having various ways of inbound and outbound communication with third parties at all times, whilst communication channels are clearly defined and widely known to members of the area of responsibility and collaborating partners.
	Adoption of standards: Follow common technical standards to ensure interoperability of equipment and systems.	With scarce mentions to interoperability through Greece's regulatory ecosystem, it is of note to mention Νόμος 4961/2022, article 38.1, regarding a registry of interconnected devices: each IT operator keeps a register of the IT technology devices it uses, which it updates on an annual basis and, in any case, when it puts a new IT technology device into operation. The operator shall make the register available to the National Cyber Security Authority or the relevant response team when requested. Also, article 84 of the Νόμος 4727/2020, concerning the interoperability of public sector bodies, and article 89 creating an interoperability registry for public sector entities, which should be used as a minimum for the following: (a) the implementation of a single technological framework and interoperability standards, (b) the design and production of new web services of public sector entities, (c) the assurance of interoperability for the exchange of data between information systems of public sector entities, (d) the technical design of complex online services through the Interoperability Center (KED).
	Operational flexibility: Enable integration and adaptation of new technologies as needs and capabilities evolve.	For this item, Νόμος 4961/2022, Part A, Chapter B, lays down the settings for the development of artificial intelligence in Greece. Also, Chapter D regularises the use of unmanned aircraft systems for the provision of postal services, but no mention of emergency settings can be seen. Finally, the "Βίβλος Ψηφιακού Μετασχηματισμού 2020-2025" (Digital Transformation Bible 2020-2025) lays down a strategic axe of intervention on Artificial Intelligence, recognising its benefits, as well as its risks, and promoting its application in the Public Administration, among other fields (pp. 158-165), but no specific mention to rescue operations can be found.

REGULATORY AREA	SCOPE	IDENTIFICATION
Health and safety	*Proven effectiveness: Verify that devices and systems meet performance and security standards.*	References to standards and security of technology and working devices, widely addressed in these laws, are the following. The Νόμος 4961/2022, in its article 36, regarding the responsibilities of the National Cyber Security Authority in cooperation with the competent response team states that they shall check and evaluate the compliance of IT technology devices with the required obligations provided for in this and other laws. Specially, they shall evaluate the compliance in terms of the appropriateness of the measures taken by the IT operators to prevent and limit the impact of events that affect the security of devices. Secondly, the above-mentioned law, in its article 32, regarding cybersecurity measures for Internet of Things (IoT) devices require that technology devices are designed and developed in such a way as to achieve an appropriate level of cyber security throughout their life cycle and to prevent attempts by unauthorised third parties to alter their use or performance, taking into account the use and the potential security risks, whilst software is also timely updated, data is encrypted when necessary, among others. Furthermore, Νόμος 3850/2010, article 34, regarding the prevention of occupational hazards from machines, states that manufacturers, importers and suppliers must ensure that the machines, tools, devices, which they produce, import or market, are in accordance with the applicable health and safety standards and the rules of technique during their design and manufacture. Lastly, Υπουργική Απόφαση ΔΥ8δ/Γ.Π.οικ./130648/2009 sets out standards for medical technological devices and products.
	Risk prevention: Identify and mitigate potential hazards associated with the use of technologies in emergency contexts.	Concerning risk mitigation, the following provisions, while not making specific mention of disaster settings and rescue operations, could be considered relevant. To begin with, from a data protection point of view, the Νόμος 4624/2019, in its article 62.1, states that the controller and the processor, taking into account the available technology, the cost of implementation, the nature, scope, circumstances and purposes of the processing, as well as the likelihood and severity of the processing risks for the data subjects, shall take the necessary technical and organisational measures to ensure a level of security appropriate to the risk when processing personal data, in particular with regard to the processing of special categories of personal data. Similarly, article 65.1: if a form of processing, in particular when new technologies are used, may create a significant risk for the protected legal interests of the interested parties due to the nature, scope, conditions and purposes of the processing, the controller shall first assess the consequences of the execution of the processing for the data subjects. On the other hand, in terms of technology devices development, the Νόμος 4961/2022, article 39 requires that the manufacturer has for each IP technology device a management procedure in the occurrence of an event or a vulnerability, which should include appropriate documentation by the manufacturer on the detailed instructions for dealing with them, as well as the appropriate measures to mitigate any adverse consequences. Besides, article 5, regarding an algorithmic impact assessment requires that: every public sector entity that uses an artificial intelligence system of paragraph 1 of article 4, before the system starts operating, prepares an algorithmic impact assessment, taking into account the following information: purpose; capabilities; technical characteristics and operating parameters; type and categories of decisions made or acts issued with the participation of the system, or supported by it; categories of data collected, processed or introduced into or produced by the system; risks that may arise for the rights, freedoms and legal interests of the natural or legal persons concerned or affected by the taking of the decision; and expected benefit arising for society. Finally, from an occupational safety point of view, the Νόμος 3850/2010 establishes measures to protect workers against risk that machines could generate (e.g. arts. 8, 33, 34, 35, 38, 49...), while, in addition, the following regulatory instruments set down standards for safety and health requirements and provisions to reduce and prevent risk regarding the following specific issues: artificial optical radiation (Προεδρικό Διάταγμα 82/2010); electromagnetic fields (Προεδρικό Διάταγμα 120/2016); and when working with visual display screens (Προεδρικό Διάταγμα 398/1994). It could be essential to follow these provisions when developing drones[24], telecommunications systems, wearables, robots and augmented reality devices.

[24] Greece has no national laws on drones and unmanned aircraft, but is still subject to Commission Delegated Regulation (EU) 2019/945 and 2020/1058, as well as Implementing Regulation (EU) 2019/947, 2020/639, 2020/746, and other European legislation on aviation and drones.

REGULATORY AREA	SCOPE	IDENTIFICATION
	Training and awareness: Provide the necessary training for the safe and effective use of technologies.	While not including first responders or occupational safety specifications in these provisions, the Νόμος 4961/2022, article 40 indicates that each ICT operator shall ensure that: a) the user of the device is provided with all information for its safe installation, configuration and operation, in a concise, transparent, understandable and easily accessible form; b) the least possible involvement of the user is ensured during installation and operation of the device; and c) the user is provided with detailed instructions for checking the safety of the device. Lastly, regarding the prevention of occupational hazards from machines, article 34 of the Νόμος 3850/2010 states that manufacturers, importers and suppliers must provide the required written instructions for use and maintenance, pointing out the possible risks from the use of their products (machines, tools and devices that they produce, import or market).
Ethics and AI	*Algorithmic transparency: Ensure that AI decision processes are understandable and auditable.*	The provisions to this item are contained in Article 6 of Law 4961/2022 (Νόμος 4961/2022) referring to "Transparency obligations". Without prejudice to the provisions of Articles 12 to 14 of the G.K.P.D. In order to exercise the information rights of natural persons, any public sector entity using an artificial intelligence system referred to in Article 4(1) shall provide, publicly, information on: a) the start-up time of the system, b) the operational parameters, capabilities and technical characteristics of the system, c) the categories of decisions taken or acts issued with the participation of or supported by the system, and d) perform an algorithmic impact assessment. 2. Any public sector entity using an artificial intelligence system referred to in Article 4(1) shall ensure that the natural or legal person to whom the decision is taken or the act is issued is informed of the parameters on which the decision was based. decision or the issuing of the act in an understandable and easily accessible format, including formats that facilitate the provision of information to persons with disabilities.3. The National Transparency Authority (ANT), with the objective of strengthening transparency, integrity and accountability, is responsible for receiving, processing, evaluating and, where appropriate, investigating or filing complaints or denunciations, related to violations of the obligations of paragraphs 1 and 2.
	Accountability in decision-making: Clearly establish accountability for AI-supported decisions.	The provisions relating to this point are contained in Articles 11, 12, 13 and 14 of Law 4961/2022 (Νόμος 4961/2022), which refer to the "Artificial Intelligence Coordination Committee, Responsibilities of the Artificial Intelligence Coordination Committee, Oversight Committee of the National Strategy for the Development of Artificial Intelligence and, finally, Artificial Intelligence Observatory". They all contain different provisions for decision-making and responsibilities to be assumed by each of those in charge of developing and overseeing the implementation of AI in the Greek context.
	Fairness and non-discrimination: Implement measures to avoid algorithmic bias and ensure fair decisions.	The provisions to this item are contained in Article 5 of Law 4961/2022 (Νόμος 4961/2022) referring to "Algorithmic impact assessment. Each public sector entity using an artificial intelligence system referred to in Article 4(1) shall, before the system is put into operation, prepare an algorithmic impact assessment. 2. The preparation of the algorithmic impact assessment shall take into account, in particular, the following information: (a) the intended purpose, including the public interest served by the use of the system, (b) the capabilities, technical characteristics and operational parameters of the system, (c) the type and categories of decisions taken or acts issued with the involvement of, or supported by, the system, (d) the categories of data collected, processed or entered into or generated by the system; (e) the risks that may arise for the rights, freedoms and legal interests of the natural or legal persons concerned or affected by the decision making; and (f) the expected resulting benefit for society as a whole in relation to the possible risks and effects that the use of the system may bring, especially for racial, ethnic, societal or age groups and categories of the population such as persons with disabilities or chronic diseases. 3. The obligation to carry out an algorithmic impact assessment in accordance herewith does not replace the obligation to carry out a data protection impact assessment in accordance with Article 35 of the G.K.P.D.

3.6. The Netherlands

Table 10. The Netherlands' regulatory landscape overview

REGULATION	REGULATORY AREA	LINK
Uitvoeringswet Algemene verordening gegevensbescherming (AVG) (Implementation Act of the General Data Protection Regulation)	Data protection and privacy.	https://wetten.overheid.nl/BWBR0040940/2021-07-01
Wet beveiliging netwerk- en informatiesystemen (Wbni) (Network and Information Systems Security Act)	Health and safety.	https://wetten.overheid.nl/BWBR0041515/2022-12-01
The Netherlands Cybersecurity Strategy 2022-2028	Cybersecurity and information protection; Interoperability and technical standards; Health and safety.	https://english.nctv.nl/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028
Arbeidsomstandighedenwet (Working Conditions Act)	Health and safety.	https://wetten.overheid.nl/BWBR0010346/2023-06-20
Wet op de medische hulpmiddelen (Medical Devices Act)	Health and safety.	https://wetten.overheid.nl/BWBR0002697/2018-08-01
Telecommunicatiewet (Telecommunications Act)	Interoperability and technical standards; Health and safety.	https://wetten.overheid.nl/BWBR0009950/2024-01-01
Strategisch Actieplan voor Artificiële Intelligentie (Strategic Action Plan for Artificial Intelligence)[25]	Interoperability and technical standards; Ethics and AI.	https://wp.oecd.ai/app/uploads/2021/12/Netherlands_Strategic_Action_Plan_for_Artificial_Intelligence.pdf

[25] Not a regulation, but a national strategy.

Table 11. Regulatory analysis of The Netherlands' framework

REGULATORY AREA	SCOPE	IDENTIFICATION
Data protection and privacy	*Limited collection: Only collect personal and sensitive data strictly necessary for the response operation.*	Section 3.1 of the AVG (Articles 22-30) sets out the protection of sensitive data and the exceptions provided for. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic and biometric data for identification purposes. The unique identification of a person, or data concerning his or her health, or data relating to a person's sexual behaviour or sexual orientation is prohibited. These exceptions include general exceptions in the field of national legislation; exceptions for research purposes; exceptions to the processing of data on racial or ethnic origin; exceptions to the processing of data revealing political opinions for the performance of public functions; exceptions for religious beliefs; genetic data; biometric data; or health. It does not seem to envisage the limited use of these data for the specific purposes within the development of national legislation. Therefore, to apply the only reference to the data minimisation principles, one has to refer to Article 5(c) of the GDPR, which states that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, as a general rule.
	Secure storage: Implement robust security measures to protect stored data.	National legislation does not refer to this storage security. However, the directly applicable GDPR, in Article 5(f) states that personal data shall be processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, through the implementation of appropriate technical or organisational measures. Article 30 of the GDPR also provides that the data controller shall carry out a general description of the technical and organisational security measures referred to in Article 32. Article 32 of the GDPR, for its part, makes direct reference to the security of data processing. Measures include pseudo-anonymisation, verification and assessment of technical and organisational measures, etc.
	Specific use: Use data only for emergency response purposes, ensuring respect for privacy.	National legislation does not elaborate on this point, but the GDPR does. Article 18, on restriction of processing, provides that the data subject shall have the right to restrict the processing of data in different circumstances, e.g. opposition to the processing or purpose of the data, contesting the accuracy of the data
Cybersecurity and information protection	*Protection against cyber-attacks: Adopt cybersecurity strategies to safeguard information and communication systems.*	With regard to protection against cyber-attacks, the National Cybersecurity Strategy, p.20 details a series of actions related to action pillar III aimed at "Countering cyber threats posed by states and criminals", which is specified in three key points: improving the understanding of what cyber threats are, increasing investigative capacity in the area of cybercrime and, finally, expanding the diplomatic response and cyber-defence capacity. In addition, pp.18-19 mentions eight strategic decisions that affect the country's cyber security: 1) In respect of the Nationwide Network of Cybersecurity Partnerships 2) It should be possible to alert anyone in the Netherlands who is a (potential) victim or target of a cyberattack 3) In respect of legislation 4) In respect of collaboration 5) In respect of knowledge and innovation 6) In respect of countering cyber threats posed by state actors and criminals 7) Cyber risks for members of the public 8) The government actions

REGULATORY AREA	SCOPE	IDENTIFICATION
	Information integrity: Maintain the accuracy and timeliness of critical information.	Throughout the Strategy, the importance of maintaining the integrity of information, data and systems in the face of a possible cyber-attack is repeatedly mentioned. Then, on p. 9, it states that one of the fundamental pillars of cybersecurity is the availability, integrity and confidentiality of the data that can be handled in different operations. Therefore, concrete actions must be taken to preserve their status. This idea is highlighted again on p.17 when it is stated that "cybersecurity is at a level commensurate with the threat and with the importance of ensuring the continuity, integrity and reliability of digital systems and processes". More specifically, the importance of the integrity of the information and processes carried out in cybersecurity actions is included in Pillar I dedicated to Cyber resilience of the government, businesses and civil society organisations, which can be found on p. 24.
	System resilience: Ensure continuity and recovery of operations in the event of security incidents.	Throughout the Strategy it is clearly stated that "the level of cyber resilience in the Netherlands is insufficient", p.12, due to various factors and therefore needs to be improved in the coming years. As stated, "There is a growing 'cyber resilience gap' between organisations", p.13, which results in greater or lesser vulnerability depending on the sector. In this sense, in order to respond to this problem, pillars I, dedicated to "Cyber resilience of the government, businesses and civil society organisations", p.22, and pillar IV, dedicated to "Cyber security labour market, education and cyber resilience of the public", p.23, are proposed.
Interoperability and technical standards	*Interagency compatibility: Facilitate communication and coordination between different response agencies.*	Regarding extraordinary circumstances, the "Telecommunicatiewet" (Telecommunications act), in its article 14.2 authorises Netherlands' Minister, in agreement with the Minister of Security and Justice, to issue instructions to providers of electronic communication networks and electronic communication services regarding the use of communications from public authorities to warn the public of impending disasters or emergencies and to mitigate the consequences of disasters or emergencies; as well as, more importantly in this case, ensuring communications between and with emergency services and public authorities during disasters or emergencies.
	Adoption of standards: Follow common technical standards to ensure interoperability of equipment and systems.	The "Telecommunicatiewet" (Telecommunications act), chapter 6 regards interoperability, interconnection and access to networks, even though its applicability to disaster settings remains unclear. On the other hand, "Netherlands Cybersecurity Strategy 2022-2028" states that "in the development and application of new technologies, security by design and security by default are always the guiding principles. Furthermore, in the purchasing and procurement of digital products and services, the risk of espionage, influencing or sabotage by state actors is assessed as standard" (p. 20). It is a call for for standardisation and common legislation: "despite efforts to improve the security of digital products and services, there is still no comprehensive system of legislation (EU or otherwise) setting out the necessary standards for digital products, processes and services and geared to the individual responsibility of manufacturers and suppliers" (p. 32). Finally, the Netherlands' "Strategic Action Plan for Artificial Intelligence", highlights the use of "common principles such as the internationally verified and accepted FAIR (Findable, Accessible, Interoperable, Reusable) principles offer a good basis for the standards, tools and training per domain or sector. This can be used to make data suitable, or to determine its suitability for reuse (sharing) by both people and machines under clearly described conditions" (p. 34).

REGULATORY AREA	SCOPE	IDENTIFICATION
	Operational flexibility: Enable integration and adaptation of new technologies as needs and capabilities evolve.	Throughout all the documents, references to this aspect could only be found from the point of view of artificial intelligence. In the Netherlands' "Strategic Action Plan for Artificial Intelligence", it is emphasised that "AI will make a substantial contribution to economic growth, prosperity and well-being of the Netherlands. It will also be of huge assistance in dealing with societal issues in areas such as ageing, climate change, food safety and healthcare" (p. 7), "robotics or unmanned systems" (p. 9)[26], among other public services (pp. 13-18). As stated later, "the labour market is changing rapidly as a result of technological progress and digitalisation. This requires adaptability and flexibility in the labour market [...]" (p.30). Nonetheless, its potential for emergency contexts remains to be clarified.
Health and safety	*Proven effectiveness: Verify that devices and systems meet performance and security standards.*	This aspect is hardly addressed in the envisaged legislation, with no provisions for new technologies or devices that could be related to the project's solutions, apart from article 1 of the "Wet op de medische hulpmiddelen" (Medical Devices Act), that states the following: in the interest of public health, it may be determined by order in council that it is prohibited to import, have available, deliver or use medical devices of a type if they do not meet the requirements set. Similarly, article 5: with regard to medical devices of a designated type, which may constitute a serious health hazard, an order in council may provide that it is prohibited to manufacture, import, have available, deliver or use such devices. In the following articles, penalties for the responsible parties are set out.
	Risk prevention: Identify and mitigate potential hazards associated with the use of technologies in emergency contexts.	Regarding security and controlling risks of networks, article 7 of the "Wet beveiliging netwerk- en informatiesystemen" (Network and Information Systems Security Act), indicates the following: the provider of an essential service and the digital service provider shall take appropriate action and proportionate technical and organisational measures to address security risks of their network and information systems. The measures are of concern to the state of the art, for a level of security that is tailored to the risks that occur, taking the following aspects into account: security, handling, continuity, monitoring and testing, and compliance with standards. Secondly, concerning data protection in networks, the "Telecommunicatiewet" (Telecommunications act), in its article 11.3 sets out the following requirement: the provider of a public electronic communications network shall take appropriate technical and organisational measures for the safety and security of the networks and services they provide in the interests of the protection of personal data and privacy of users (protecting stored or transmitted personal data, ensuring authorised access...). In the same sense regarding general safety, article 10.8: rules can be established regarding special measures concerning the commissioning or use of equipment that complies with the regulations set forth in this chapter or pursuant to it: 1) to remedy an existing or anticipated problem related to the requirements that equipment must meet at a specific location; 2) for safety reasons to protect public electronic communication networks or radio equipment, if they are used for security purposes in clearly defined spectrum situations. Also, rules can be established to terminate or restrict the placing on the market or offering on the market of devices or radio equipment or categories of devices or radio equipment, if there is justified concern that these pose a risk to the health or safety of persons. Still, disaster contexts are not envisaged in the legislation. From occupational hazards legislation, the "Arbeidsomstandighedenwet" (Working Conditions Act), article 10, in order to prevent risk to third parties, notes that if, in or directly related to the work performed by the employer's employees in a company or establishment or in its immediate vicinity, there may be a danger to the safety or health of persons other than those employees, the employer shall take effective measures to prevent that danger. Lastly, it is the "Netherlands Cybersecurity Strategy 2022-2028" that reminds that "vulnerabilities are discovered in software and there are still too many devices and services on the market that can easily be misused for criminal activities, espionage or large-scale attacks" (p. 31), being clearly relevant to the project's solutions.

[26] More regulations potentially related to unmanned aircraft (drones) regulations in The Netherlands:
[https://wetten.overheid.nl/BWBR0019147/2021-04-22]
[https://wetten.overheid.nl/BWBR0005555/2024-01-01]

REGULATORY AREA	SCOPE	IDENTIFICATION
	Training and awareness: Provide the necessary training for the safe and effective use of technologies.	Regarding instructions and training, although there is no specific mention of new technologies and disaster contexts, it is necessary to note art. 8 of the "Arbeidsomstandighedenwet" (Working Conditions Act): the employer shall ensure that workers are effectively informed of the work to be carried out and the associated risks, as well as the measures aimed at preventing or reducing those risks. The employer shall ensure that workers are provided with effective instruction in working conditions appropriate to their various tasks. In particular, where personal protective equipment is made available to employees and where protective devices are fitted to work equipment or otherwise, the employer shall ensure that employees are aware of their purpose and operation and how to use them.
Ethics and AI	*Algorithmic transparency: Ensure that AI decision processes are understandable and auditable.*	Throughout the document, there is an extensive and detailed treatment of the issues related to algorithmic transparency and the different actions that are planned to be carried out in order to achieve it. Then, numerous mentions are made on pp. 14, 19, 20, 35, 40, 42 and 45, which cover the most important aspects of algorithmic transparency and its importance through its use. As a summary, concrete actions are listed on pp.58-59, where it is stated, for example, that "In collaboration with other governmental organisations and the Association of Netherlands Municipalities (VNG), the Ministry of the Interior and Kingdom Relations is conducting two experiments with AI in 2019, focusing on ethics in, by and for the design and transparency of algorithms. The ambition is to create a portfolio of example projects, which will be shared in the knowledge network, p.58, "The Ministry of the Interior and Kingdom Relations is creating a transparency lab for government organisations, where knowledge is exchanged and support is provided in the areas of transparency, explainability and accountability", p.58, "Through research calls for PPPs, the national government is investing in research on the responsible use of AI and the transparency and explainability of algorithms, in collaboration with the VWData programme (NWA route) "p.49.
	Accountability in decision-making: Clearly establish accountability for AI-supported decisions.	With regard to responsibility in decision-making, the document deals with the problem in a general rather than a specific way, pointing out that this is a de facto problem that can affect users and individuals. Then, for example, on p.45, it is mentioned that "Companies and governments have a (legal) responsibility to provide sufficient insight into the AI applications that they use, and the associated procedures". However, when it comes to settling the issue, p.46, the European rather than the national context is referred to. Then, it is stated that "When making a decision or acting with the help of IA, questions of liability for damages may arise. In the case of cross-border issues, which are frequent with AI, these liability issues can best be examined in a European context". On the other hand, if we stick to concrete actions, p.58 states that "The Ministry of Interior and Kingdom Relations is setting up a transparency laboratory for governmental organisations, where knowledge is exchanged and support is provided on transparency, explainability and accountability".
	Fairness and non-discrimination: Implement measures to avoid algorithmic bias and ensure fair decisions.	The treatment of fairness and non-discrimination related to the uses of AI and possible algorithmic discrimination appears briefly but concisely on pp. 7, 35, 41 and 42. Throughout these pages, a brief exposition is made of the problems associated with the biases that may exist in AI tools and, together with this, measures are sought to be established for their mitigation, p. 35, and for the fulfilment of fundamental rights such as non-discrimination, p. 7.

4. Identification of gaps in national regulations and recommendations

The emergency response landscape has dramatically transformed with the introduction of cutting-edge technology. Advanced tools such as autonomous drones, AI-powered analytics, and enhanced communication systems have not only revolutionised how first responders operate but have also highlighted the need for a critical evaluation of the regulatory frameworks that support these technologies. While international regulatory (or recommendations) frameworks tend to be more generic and can serve as a good starting point to identify and exchange good practices, they often fail to adequately address or only superficially treat issues related to advanced technologies (see section 2). Therefore, it is crucial to delve into specific national frameworks that are essential in laying the groundwork for operational effectiveness, privacy, security, and ethical governance in the context of modern emergency response technologies. However, the rapid pace of technological advancement often outpaces the evolution of regulatory structures, leaving potential gaps and limitations that could hinder the seamless adoption and optimal use of these tools in critical emergency scenarios.

This section is dedicated to highlighting these gaps and formulating specific recommendations tailored to policy makers, public sector stakeholders and law enforcement agencies. As we navigate through the complexities of laws and standards, our objective is twofold. First, we seek to identify where current national regulatory frameworks may fall short in addressing the new demands and challenges posed by technological advances in emergency response. These gaps could take the form of outdated privacy laws that fail to account for the data-intensive operations of modern devices, cybersecurity protocols that fail to protect emerging technologies from sophisticated threats, or ethical guidelines that have yet to catch up with the capabilities and implications of AI-driven decision-making.

Certainly, this section aspires to contribute constructively to the ongoing discourse surrounding regulatory adaptation in the realm of emergency response technology. By providing an analysis of the existing frameworks, we intend to spotlight areas that may require attention and thoughtful revision. Our recommendations are presented with the understanding that they are part of a larger, collaborative effort to shape policies that are resilient, responsive, and reflective of our shared values. The guidance we offer aims to support policymakers in navigating the complex interplay between innovation and regulation, help public sector stakeholders in calibrating their strategic approaches to new technologies, and assist law enforcement agencies in fulfilling their duties within a clear and updated legal context. It is with a sense of shared responsibility and a commitment to continuous improvement that we present these insights, hoping they will serve as a catalyst for constructive dialogue and incremental progress towards more robust, equitable, and adaptable regulatory frameworks.

In our methodological approach, we have chosen to structure the gap analysis and subsequent recommendations from two distinct but interrelated perspectives. The first is through the lens of the regulatory areas identified as most relevant to technological applications in emergency response. This allows us to dissect and address the multifaceted nature of the frameworks governing data protection, cybersecurity, interoperability, health and safety, ethics in AI, and more. By applying this cross-sectional analysis nationally, we can provide a comprehensive overview that highlights both common challenges and unique national characteristics. The second perspective is rooted in the specific contexts of the end-user countries within the SYNERGISE project. By delving into the particularities of Poland, Germany, Sweden, Greece and the Netherlands, we are able to tailor our recommendations to the nuanced legal, cultural and operational landscapes of each country. This dual approach ensures that our findings and recommendations are not only relevant to the broad thematic regulatory issues, but are also grounded in the practical realities and needs

of the first responders who rely on these systems every day. Together, these two perspectives form the backbone of our methodology, providing a robust and dynamic framework for our analysis that is both comprehensive in scope and specific in application.

4.1. By Regulatory Area

Table 12. Gaps and Recommendations by regulatory area

ASPECT	GAP ANALYSIS	RECOMMENDATIONS
Data Protection and Privacy	Emergency services require swift access to data. Current regulations may not reflect the urgency and scope of data needed in emergencies.	Amend data protection laws to provide clear provisions for the collection, use, and storage of data during emergencies.
	There may be prohibitions on using data beyond its initial collection purpose, which can hinder the dynamic use of data during unfolding crises.	Establish protocols that allow for the broader collection and use of data in emergencies while maintaining individual privacy rights.
	Regulations may not clearly define how long and in what manner sensitive data can be stored, which can be critical in post-incident reviews or ongoing emergencies.	Develop specific guidelines for data retention that balance the needs of emergency services with privacy concerns.
Cybersecurity and Information Protection	As first responders use more interconnected devices, the risk of cyber threats increases.	Introduce cybersecurity frameworks specific to the technologies used by first responders.
	There are not always explicit regulations governing the cybersecurity of AI, drones, and other advanced tools.	Mandate regular cybersecurity risk assessments for the technologies deployed, ensuring they are resistant to evolving threats.
Interoperability and Technical Standards	Disparate technical standards can lead to incompatibility issues between agencies and countries, impeding collaborative responses.	Work towards unified standards, especially within the EU, to ensure compatibility and cooperation across borders.
	Different communication protocols can prevent efficient coordination.	Establish common communication protocols and technologies to facilitate coordination among various emergency services.
Health and Safety	Current regulations may not account for the health and safety risks specific to new devices like drones and robots.	Update health and safety regulations to address the risks associated with new technologies.
	First responders may lack training on the safe use of new technologies.	Develop training programs focusing on the operation, risks, and safety measures associated with new devices.
Ethics and AI	Ethical guidelines for AI use in emergency scenarios are still nascent and may not cover all potential issues.	Develop an ethical framework for AI in emergency services, addressing transparency, accountability, and fairness.
	There's a risk of bias in AI decision-making, which can have serious implications in emergency situations.	Implement mechanisms to audit algorithms for biases regularly and ensure their decisions are equitable and non-discriminatory.
Training and Capacity Building (additional)	There may be a gap in specialised training for first responders on the use of new technologies.	Establish ongoing education initiatives to keep first responders updated on the latest technologies and their regulatory implications. Include simulations and drills that integrate technology use into standard training protocols.
Public-Private Partnerships (PPP) and R&D (additional)	There may be insufficient collaboration between the public sector and technology providers.	Encourage partnerships with technology firms to leverage their expertise in product development and cybersecurity. Provide grants and incentives for R&D focused on creating solutions tailored to the needs of first responders.

4.2. By SYNERGYSE end-user country

Table 13. Gaps and Recommendations by SYNERGISE end-user country

COUNTRY	SPECIFIC GAPS	RECOMMENDATIONS
Poland	Clarification needed on data processing during emergencies.	Amend privacy laws to specify data use in emergency contexts.
	Alignment with EU cybersecurity standards required.	Harmonise national cybersecurity protocols with EU directives.
	Specific guidelines for AI and robotics in public safety absent.	Create public safety standards for AI and robotics deployment.
Germany	Lack of provisions for data use in crisis management.	Legislate broader data usage allowances for crisis scenarios.
	Cybersecurity strategies outdated for modern responder technologies	Revise cybersecurity strategies to include first responder tech
	AI ethics not integrated into public safety strategies	Incorporate AI ethics into public safety policy development
Sweden	Data usage framework for emergencies is inadequate.	Update legal framework to enhance data use in emergencies.
	First responders' cybersecurity strategies are not technology-specific.	Tailor cybersecurity strategies to first responders' tech needs.
	Interoperability standards for cross-agency operations missing.	Establish interoperability standards for emergency services.
Greece	Data protection laws not aligned with EU GDPR for emergencies.	Adjust national data protection laws to EU GDPR standards.
	Lack of specific cybersecurity strategies for first responders.	Develop cybersecurity guidelines for emergency tech use.
	Ethical framework for AI and robotics in emergencies not developed.	Formulate ethics guidelines for AI and robotics in public safety.
The Netherlands	Data protection laws insufficient for rapid data exchange in emergencies.	Improve legal mechanisms for emergency data exchange efficiency.
	Emergency services' cybersecurity measures outdated.	Update and specify cybersecurity measures for emergency services.
	Lack of ethical AI integration in public safety.	Integrate ethical AI use guidelines into public safety strategies.

5. Conclusions

In concluding the analysis presented in document D1.2 for the SYNERGISE project, the findings can be systematically organised into different thematic areas that reflect the main objectives and lessons learned from the comprehensive assessment of the ethical, legal, societal and inclusiveness frameworks for FR operations. These conclusions are essential to guide future action and improve the effectiveness of disaster risk management strategies.

Regulatory alignment and integration (see section 2 and 3)

- The analysis underlines the need for FR operations to be strictly aligned with European and international regulations. This alignment ensures that responses to disasters are not only efficient, but also meet the highest standards of legal and ethical conduct.
- A critical review of the regulatory environments of the consortium's end users identifies different integration potentials for SYNERGISE project advanced technological solutions (including autonomous exploration robots, real-time health and hazard monitoring devices, indoor and outdoor localization systems, augmented reality for operational control, AI-driven intelligence tools, rapid communication systems, and interoperable command

solutions for efficient multi-agency response management). Tailoring project outputs to these specific regulatory contexts is essential to overcome barriers to adoption and maximise the impact of innovative solutions.

Identifying gaps and constraints (see section 3)

- This report identifies significant gaps in current regulatory frameworks, particularly in adapting to the evolving nature of disaster risks and incorporating advanced technological solutions. These gaps represent opportunities for legislative and policy developments to better support disaster response operations.
- The analysis highlights technical, regulatory, training and cooperation areas where current frameworks could be improved to ensure a more inclusive approach to DRR. Addressing these issues is critical to ensuring that DRR measures effectively address the needs of all segments of the population, especially the most vulnerable.

Recommendations for stakeholders (see section 4)

- The development of targeted recommendations for policy makers and public sector stakeholders is essential. These recommendations aim to address identified gaps, promote regulatory improvements and enhance the overall effectiveness of disaster response.
- The recommendations also focus on practical measures for disaster response agencies to integrate ethical, legal, societal and inclusiveness considerations into their daily operations. This integration is essential to ensure that responses to emergencies are comprehensive and respect the dignity and rights of all persons affected.

Recommended future directions and next steps for the SYNERGISE consortium

Short-term:

- Workshop facilitation for the alignment of technological application with prevailing ethical and legal standards is highly advocated. Such alignment is anticipated to enhance adherence to regulations and ethical guidelines, thus mitigating legal disputes and bolstering public confidence and acceptance of disaster response measures.
- It is advisable to conduct inclusiveness assessments of disaster response strategies. Outcomes of these evaluations are expected to refine services to encompass all populations adequately, prioritizing those most at risk of exclusion, and promoting fairness in disaster response.
- Undertaking societal impact assessments for employed technological solutions is endorsed. This endeavour aims to bolster community trust and participation, optimizing resource utilization, and ensuring that emergency services resonate with public expectations and societal values.

Medium-term:

- The development of training programs dedicated to amplifying inclusivity within disaster risk reduction is recommended. These programs aspire to cultivate an environment where emergency response teams consider the diverse needs of the community, contributing to a reduction in disparities following disasters.
- Hosting workshops for policy development with a wide range of contributors is suggested. The collaborative outcome is projected to yield policies that underpin ethical and legal technology use in disaster management, leading to more adept and agile disaster risk reduction methodologies.

Long-term:

- The establishment of a permanent ethics advisory board to navigate the ethical dimensions of extended disaster risk management is suggested. This board's role is to persistently ensure that disaster risk reduction tactics remain in harmony with the progressive societal ethos, thereby sustaining ethical standards and public confidence.
- It is recommended to proactively refine legal frameworks to align with ongoing technological advancements. Pre-emptive legal adjustments are intended to support innovation and ascertain that disaster risk management approaches are efficacious and maintain legal validity.
- Advisable is the regular refreshment of inclusivity strategies. Adopting such a dynamic method is poised to align with evolving societal demographics and demands, paving the way for communities where equitable access to disaster risk management is realized for all.

In summary, D1.2 from the SYNERGISE project provides a comprehensive basis for improving DRR operations through a nuanced understanding of ethical, legal, societal, and inclusive frameworks. By systematically addressing identified gaps, tailoring recommendations to stakeholder needs, and promoting a culture of collaboration and continuous improvement, the way is paved for more effective, inclusive and adaptive DRR strategies.

Bibliography

Commission Implementing Decision (EU) 2019/570 of 8 April 2019 laying down rules for the implementation of Decision No 1313/2013/EU of the European Parliament and of the Council as regards rescEU capacities and amending Commission Implementing Decision 2014/762/EU. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2019.099.01.0041.01.ENG

Commission Implementing Decision (EU) 2021/1956 of 10 November 2021 on the establishment and organisation of the Union Civil Protection Knowledge Network. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D1956

Council Regulation (EC) No 1257/96 of 20 June 1996 concerning humanitarian aid. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01996R1257-20190726

Council Regulation (EU) 2016/369 of 15 March 2016 on the provision of emergency support within the Union. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/369/oj

Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013D1313

European Commission (2021). Communication from the Commission to the European Parliament and the Council on the EU's humanitarian action: new challenges, same principles. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0110

Germany (2020). Strategie Künstliche Intelligenz der Bundesregierung Fortschreibung 2020 (Artificial Intelligence Strategy of the German Federal Government). https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf

Germany (2021). Cyber Security Strategy for Germany. Federal Ministry of the Interior, Building and Community. https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html

Germany (2023). BMBF - Aktionsplan Künstliche Intelligenz (Artificial Intelligence Action Plan). https://www.ki-strategie-deutschland.de/files/downloads/Aktionsplan_Kuenstliche_Intelligenz_2023.pdf

Germany. Bundesdatenschutzgesetz (BDSG), vom 30. Juni 2017 (Federal Data Protection Act). https://www.gesetze-im-internet.de/bdsg_2018/

Germany. Gesetz zur Erhöhung der Sicherheit informationstechnischer System (IT-Sicherheitsgesetz), vom 17. Juli 2015 (IT Security Act). https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1709723965829

Germany. Medizinproduktegesetz in der Fassung der Bekanntmachung (MPG), vom 7. August 2002 (Medical Devices Act). https://www.buzer.de/gesetz/3284/index.htm

Germany. Telekommunikationsgesetz (TKG), vom 23. Juni 2021 (Telecommunications Act). https://www.gesetze-im-internet.de/tkg_2021/BJNR185810021.html

Germany. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, vom 18. Mai 2021 (Second law to increase the security of information technology systems). https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1709724073613

Global Network of Civil Society Organisations for Disaster Reduction (2024). *Making Displacement Safer Cookbook*. https://www.gndr.org/making-displacement-safer-cookbook/

Greece (2020). National Cybersecurity Strategy 2020-2025. https://mindigital.gr/wp-content/uploads/2022/11/E%CE%9D-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf

Greece (2021). Βίβλος Ψηφιακού Μετασχηματισμού 2020-2025 (Digital Transformation Bible 2020-2025). https://digitalstrategy.gov.gr/vivlos_pdf

Greece. Νόμος 3850/2010 (Law on the ratification of the Code of Laws for the health and safety of workers). https://www.e-nomothesia.gr/kat-ergasia-koinonike-asphalise/n-3850-2010.html

Greece. Νόμος 4577/2018 (Law on the incorporation into Greek legislation of Directive 2016/1148/EU for a high common level of security of network and information systems throughout the Union and other provisions). https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4577-2018-phek-199a-3-12-2018.html

Greece. Νόμος 4624/2019 (Law on implementation measures of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 for the protection of natural persons against the processing of personal data and incorporation into national legislation of Directive (EU) 2016/ 680 of the European Parliament and of the Council of April 27, 2016 and other provisions). https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019

Greece. Νόμος 4727/2020 (Law on Digital Governance (Incorporation into Greek Law of Directive (EU) 2016/2102 and Directive (EU) 2019/1024) - Electronic Communications (Incorporation into Greek Law of Directive (EU) 2018/1972) and other provisions). https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/nomos-4727-2020-phek-184a-23-9-2020-1.html

Greece. Νόμος 4961/2022 (Law on emerging information and communication technologies, strengthening digital governance and other provisions). https://www.e-nomothesia.gr/kat-demosia-dioikese/nomos-4961-2022-phek-146a-27-7-2022.html

Greece. Νόμος 5002/2022 (Law on procedure for removing the privacy of communications, cyber security and protection of citizens' personal data). https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-5002-2022.html

Greece. Προεδρικό Διάταγμα 120/2016 (Presidential Decree on Harmonization with Directive 2013/35/EU "on the minimum health and safety requirements regarding the exposure of workers to risks arising from natural factors (electromagnetic fields) (20th special directive within the meaning of Article 16(1) of Directive 89/391 /EEC) and repealing Directive 2004/40/EC" (OJ L179/1 of 29.06.2013)). https://www.elinyae.gr/ethniki-nomothesia/pd-1202016-fek-203a-26102016

Greece. Προεδρικό Διάταγμα 398/1994 (Presidential Decree on Minimum safety and health requirements when working with visual display screens in compliance with Council Directive 90/270/EEC). https://www.elinyae.gr/ethniki-nomothesia/pd-3981994-fek-221a-19121994

Greece. Προεδρικό Διάταγμα 82/2010 (Presidential Decree on Minimum health and safety standards regarding the exposure of workers to risks from natural factors (artificial optical radiation) in compliance with Directive 2006/25/EC). https://www.elinyae.gr/ethniki-nomothesia/pd-822010-fek-145a-192010

Greece. Υπουργική Απόφαση ΔΥ8δ/Γ.Π.οικ./130648/2009 (Ministerial Decision about medical technology products). https://www.e-nomothesia.gr/kat-ygeia/farmakeia/ya-du8d-gpoik-130648-2009.html

Intergovernmental Panel on Climate Change (2023). *Climate Change Report 2023: Synthesis Report*. https://www.ipcc.ch/report/ar6/syr/

International Forum to Advance First Responder Innovation (2017). *Recommended Method for National Capability Gap Identification and Prioritization*. https://www.internationalresponderforum.org/system/files/library/2023-06/IFAFRI%20Recommended%20Method%20for%20National%20Capability%20Gap%20Identification%20and%20Prioritization.pdf

Poland (2020). Polityka dla rozwoju sztucznej inteligencji w Polsce (Policy for the Development of Artificial Intelligence in Poland). Appendix to the Resolution no. 196 of the Council of Ministers of 28 December 2020. https://www.gov.pl/attachment/928200fa-b1a6-4c0c-b3a8-d1fbf1e1175a

Poland. USTAWA z dnia 10 maja 2018 r. o ochronie danych osobowych (ACT of May 10, 2018 on the protection of personal data). https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-danych-osobowych-18722262

Poland. USTAWA z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (ACT of 16 July 2004 Telecommunications law). https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/prawo-telekomunikacyjne-17116702

Poland. USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (ACT of July 5, 2018 on the national cybersecurity system). https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/krajowy-system-cyberbezpieczenstwa-18746756

Poland. USTAWA z dnia 7 kwietnia 2022 r. o wyrobach medycznych (ACT of April 7, 2022 about medical devices). https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/wyroby-medyczne-19238461

Sweden (2017). A national cyber security strategy. https://www.government.se/legal-documents/2017/11/skr.-201617213/

Sweden (2018). Nationell inriktning för artificiell intelligens (National approach to artificial intelligence). https://www.regeringen.se/contentassets/cb7f277635ae49bc9a04899c2e1af8cf/national-approach-to-artificial-intelligence-pa-engelska.pdf

Sweden. Arbetsmiljölag (1977:1160) (Working environment act). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/arbetsmiljolag-19771160_sfs-1977-1160/

Sweden. Kamerabevakningslag (2018:1200) (Camera Surveillance Act). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/kamerabevakningslag-20181200_sfs-2018-1200/

Sweden. Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (Act with supplementary provisions to the EU's data protection regulation). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218/

Sweden. Lag (2022:482) om elektronisk kommunikation (Law on electronic communications). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482/

Sweden. Luftfartslag (2010:500) (Aviation law). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/luftfartslag-2010500_sfs-2010-500/

Sweden. Patientdatalag (2008:355) (Patient Data Act). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355/

Sweden. Patientsäkerhetslag (2010:659) (Patient Safety Act). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/patientsakerhetslag-2010659_sfs-2010-659/

Sweden. Säkerhetsskyddslag (2018:585) (Security Protective Act). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-2018585_sfs-2018-585/

The Netherlands (2019). Strategisch Actieplan voor Artificiële Intelligentie (Strategic Action Plan for Artificial Intelligence). https://wp.oecd.ai/app/uploads/2021/12/Netherlands_Strategic_Action_Plan_for_Artificial_Intelligence.pdf

The Netherlands (2022). The Netherlands Cybersecurity Strategy 2022-2028. https://english.nctv.nl/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028

The Netherlands. Arbeidsomstandighedenwet (Working Conditions Act). https://wetten.overheid.nl/BWBR0010346/2023-06-20

The Netherlands. Telecommunicatiewet (Telecommunications Act). https://wetten.overheid.nl/BWBR0009950/2024-01-01

The Netherlands. Uitvoeringswet Algemene verordening gegevensbescherming (AVG) (Implementation Act of the General Data Protection Regulation). https://wetten.overheid.nl/BWBR0040940/2021-07-01

The Netherlands. Wet beveiliging netwerk- en informatiesystemen (Wbni) (Network and Information Systems Security Act). https://wetten.overheid.nl/BWBR0041515/2022-12-01

The Netherlands. Wet op de medische hulpmiddelen (Medical Devices Act). https://wetten.overheid.nl/BWBR0002697/2018-08-01

United Nations Office for Disaster Risk Reduction (2015). *Sendai Framework for Disaster Risk Reduction 2015-2030*. https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030#:~:text=The%20Sendai%20Framework%20for%20Disaster,Investing%20in%20disaster%20reduction%20for

United Nations Office for Disaster Risk Reduction (2021). *UNDRR Strategy Framework 2022-2025*. https://www.undrr.org/publication/undrr-strategic-framework-2022-2025

United Nations Office for the Coordination of Humanitarian Affairs (2007). *Guidelines on the Use of Foreign Military and Civil Defence Assets In Disaster Relief ("Oslo Guidelines")*. https://www.refworld.org/policy/opguidance/ocha/2007/en/57053