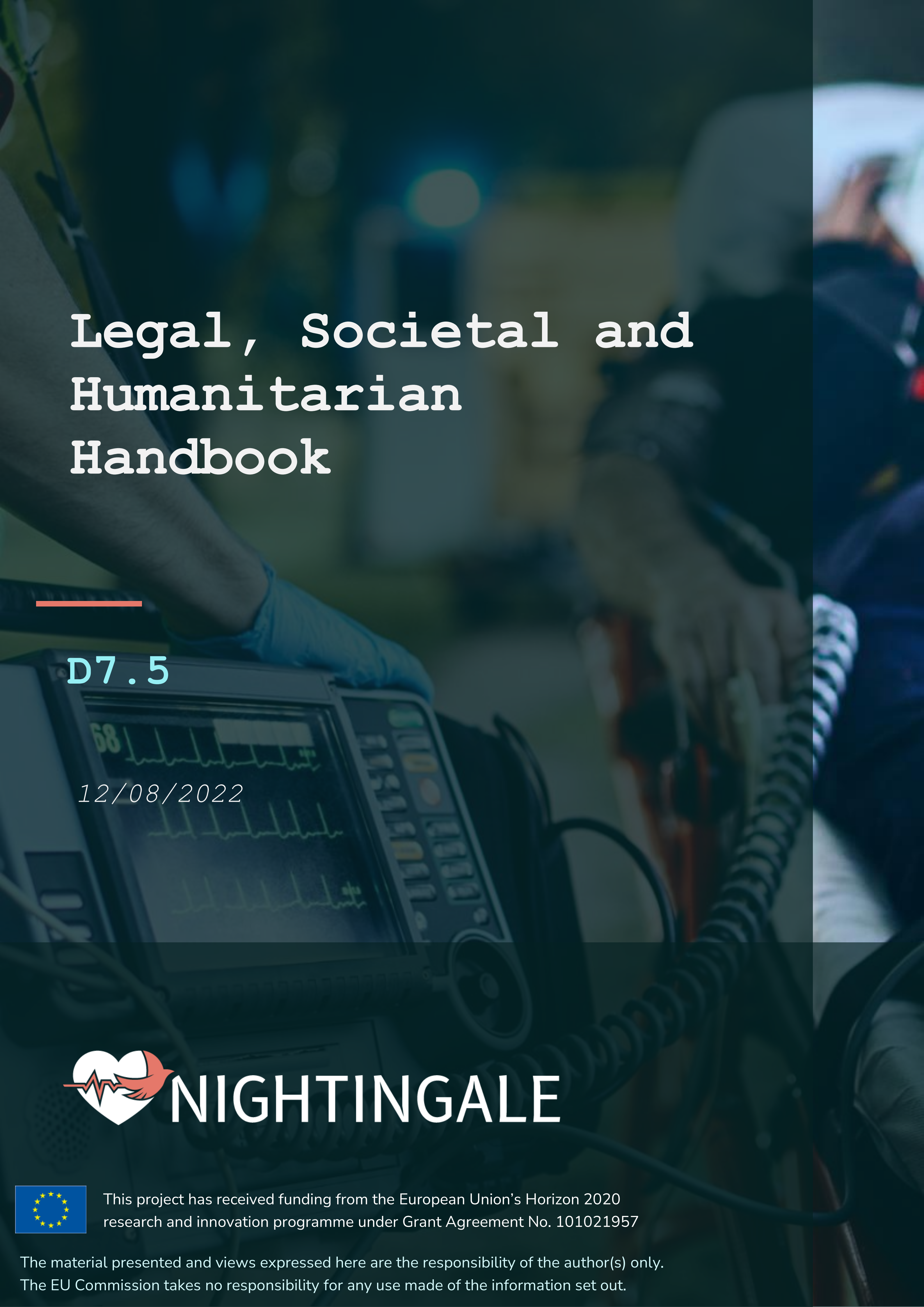


# Legal, Societal and Humanitarian Handbook

D7.5

12/08/2022

NIGHTINGALE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101021957

The material presented and views expressed here are the responsibility of the author(s) only. The EU Commission takes no responsibility for any use made of the information set out.

# DOCUMENT SUMMARY INFORMATION

| | | | |
|---|---|---|---|
| **Grant Agreement No** | 101021957 | **Acronym** | NIGHTINGALE |
| **Full Title** | Novel InteGrated toolkit for enhanced pre-Hospital life support and Triage IN challenGing And Large Emergencies | | |
| **Start Date** | 01/10/2021 | **Duration** | 36 months |
| **Project URL** | https://www.nightingale-triage.eu | | |
| **Deliverable** | D7.5 Legal, Societal and Humanitarian Handbook | | |
| **Work Package** | 7 | | |
| **Deliverable type** | Report | **Dissemination Level** | Public |
| **Due Date of Deliverable** | 31/03/2022 | **Actual Submission Date** | 15/08/2022 |
| **Deliverable Identifier** | | **Deliverable Version** | 1.0 |
| **Lead Beneficiary** | IDC | | |
| **Authors** | Yael Vias Gvirsman (Reichman University IDC) | | |
| **Co-authors** | Lorenzo Marchesi and Saverio Caruso (UCSC- Ethics Manager) of section 5.1. (below);<br>Consortium Partners of Definitions: 'Basic Life Support'; 'Damage Control'; 'Damage Control Resuscitation'; 'Damage Control Surgery'; 'Mass Casualty Incident'; 'METHANE Report'; 'Paramedic'; 'Triage' in section 2.1 below as extracted from Nightingale Medical Glossary, updated version of 4 August 2022 [internal document] | | |
| **Reviewers** | Daniele Gui and Sabina Magalini (UCSC), Luca Ragazzoni, Marta Caviglia and Hamdi Lamine (UPO), Itamar Ashkenazi (ESTES), Chaim Rafalowski (MDA), Dimitra Dionysiou (ICCS) | | |
| **Security Assessment** | ☒ Passed | Rejected | Not Required |
| **Status** | Draft | ☒ Peer Reviewed | ☒ Coordinator Accepted |

# DISCLAIMER

NIGHTINGALE has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021957. The sole responsibility for the content of this document lies with the authors. It does not necessarily reflect the opinion of the European Union. The European Commission is not responsible for any use that may be made of the information contained herein.

© NIGHTINGALE Consortium, 2022. All rights reserved.

## HISTORY OF CHANGES

| Version | Date | Changes |
|---|---|---|
| 0.1 | 01/03/2022 | Table of Contents |
| 0.2 | 31/03/2022 | Initial version |
| 0.3 | 14/04/2022 | Version ready for internal review |
|  | 15-21/4/2022 | Internal reviewers' comments received |
| 0.4 | 25/05/2022 | Internal reviewers' comments addressed. Submission to the Coordinator |
| 0.5 | 31/05/2022 | Coordinator comments received |
| 0.6 | 15/06/2022 | Coordinators comments addressed |
| 1.0 | 12/08/2022 | Final version |

## PROJECT PARTNERS

| No. | Logo | Partner | Short name | Country |
|---|---|---|---|---|
| 1 | | INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS | ICCS | Greece |
| 2 | | TOTALFORSVARETS FORSKNINGSINSTITUT | FOI | Sweden |
| 3 | | LEONARDO – SOCIETA PER AZIONI | LDO | Italy |
| 4 | | C4CONTROLS LTD<br>*[TERMINATED]* | C4C<br>*[TERMINATED]* | UK<br>*[TERMINATED]* |
| 5 | | INTRASOFT INTERNATIONAL SA | INTRA | Luxembourg |
| 6 | | INOV INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES, INOVACAO | INOV | Portugal |
| 7 | | EXUS SOFTWARE MONOPROSOPI ETAIRIA PERIORISMENIS EVTHINIS | EXUS | Greece |
| 8 | | UNIVERSITAT POLITECNICA DE VALENCIA | UPV | Spain |
| 9 | | ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS | CERTH | Greece |
| 10 | | DEVERYWARE | DW | France |
| 11 | | PARTICLE SUMMARY | PARTICLE | Portugal |
| 12 | | TREE TECHNOLOGY SA | TREE | Spain |
| 13 | | EUROPAISCHE GESENLLSCHAFT FUR TRAUMA -UND AKUTCHIRURGIE - ESTES | ESTES | Austria |
| 14 | | INTERNATIONAL MRMID ASSOSIATION | MRMID | Sweden |
| 15 | | UNIVERSITA DEGLI STUDI DEL PIEMONTE ORIENTALE AMEDEO AVOGADRO | UPO | Italy |
| 16 | | ASSISTANCE PUBLIQUE HOPITAUX DE PARIS | APHP-SAMU | France |
| 17 | | UNIVERSITA CATTOLICA DEL SACRO CUORE | UCSC | Italy |
| 18 | | MINISTERO DELL' INTERNO | MININT | Italy |
| 19 | | AZIENDA SANITARIA LOCALE N 2 SAVONESE | ASL2 | Italy |
| 20 | | MAGEN DAVID ADOM IN ISRAEL | MDA | Israel |
| 21 | | CARR COMMUNICATIONS LIMITED | CCL | Ireland |
| 22 | | ASSOCIAZIONE CITTADINANZATTIVA ONLUS | CA | Italy |
| 23 | | INTERDISCIPLINARY CENTER (IDC) HERZLIYA | IDC | Israel |
| 24 | | ASTRIAL GmbH | ASTRIAL | Germany |

© NIGHTINGALE Consortium, 2022. All rights reserved.

## LIST OF ABBREVIATIONS

| Abbreviation | Definition |
|---|---|
| **AI** | Artificial Intelligence |
| **CSC** | Crisis Standard of Care |
| **DoA** | Description of Action (technical annex to the GA) |
| **EC** | European Commission |
| **EU** | European Union |
| **FR** | First Responder |
| **FRT** | Facial Recognition Technology |
| **GA** | Grant Agreement |
| **GDPR** | General Data Protection Regulation (EU Reg. 2016/679) |
| **HRDD** | Human Rights Due Diligence |
| **LSHH** | Legal, Societal and Humanitarian Handbook |
| **LSHM** | Legal, Societal, Humanitarian Aspects Manager |
| **MCI** | Mass Casualty Incident |
| **M1, M2…** | Month 1, Month 2… |
| **NAP** | National Action Plan (integrating UN GPBHR) |
| **NIT-MR** | Novel Integrated Toolkit for Emergency Medical Response |
| **OECD** | Organisation for Economic Cooperation and Development |
| **PSAP** | Public Safety Answering Points |
| **SAB** | Security Advisory Board |
| **SGBV** | Sexual and Gender-Based Violence |
| **T (n.n)** | Task (n.n) |
| **UAV** | Unmanned Aerial Vehicle |
| **UN GPBHR** | United Nations Guiding Principles for Business and Human Rights |
| **WP(n)** | Work Package (n) |
| | |

© NIGHTINGALE Consortium, 2022. All rights reserved.

# Executive Summary

Deliverable 7.5. Legal, Societal and Humanitarian Handbook is a public dissemination level deliverable dealing with legal, societal & humanitarian issues arising from integrating Advanced Technology in view of enhancing First Response in Mass Casualty Incidents (MCIs) and Disasters.

The main focus of the Handbook is based on experience in Mass Casualty Incidents as opposed to Disasters. The legal framework can and should be applied also to Disasters and adapted as necessary.

The aim of the Legal, Societal and Humanitarian Handbook (LSHH) is to devise the landscape across the EU system and identify gaps where relevant frameworks require updating to maximise the project's toolkit adoption rates. Legal, Societal and Humanitarian issues are seen 'holistically' as they are sometimes intertwined. Nevertheless, they are presented separately below.

The deliverable first examines the context of FR in MCIs, providing definitions, mapping inherent challenges in MCIs and where technology may offer improvement or remedy (Section 1); Second, the LSHH examines applicable legal frameworks to the tools and outputs proposed within the Nightingale project. This entails a twofold approach, first, a 'classic' legal framework applicable at all times (e.g. international human rights law, human dignity, gender equality, non-discrimination, etc.), second the specific legal landscape and its challenges relating to advanced technology, namely the legal framework on Data Protection (collecting, processing, storing and sharing personal and sensitive data); Biometrics (e.g. facial recognition, bracelets and earplugs), Artificial Intelligence (AI), Drones (UAVs), as well as Public Safety Answering Points (PSAP) - tracking and localisation.[1] The LSHH provides specific focus on existing gaps and risks, namely of double-use and misuse (Section 2). Third, the deliverable examines societal and humanitarian challenges to the integration of advanced technology to First Response in MCIs understanding the need to create acceptance and enhance the democratic legitimacy of the means used in the Nightingale project (Integrating Advanced Technology) in view of reaching the project's overall objectives: to enhance capacity of First Responders (FRs) in MCIs in order to safeguard life, integrity and dignity of victims of MCIs (Section 3). Finally, Section 4 proposes means in which to mitigate risks based on the Human Rights Due Diligence approach described in detail at the beginning of the Handbook.

Wherever applicable, relevant legal developments in the making are mentioned (e.g., EU proposal on Artificial Intelligence Act), the objective being to keep project partners and associated entities informed of a changing legal environment as the project itself unfolds- so that each partner and associated entities may follow-up on evolving legal obligations, diligently. Additionally, considering this is an EU funded project and that the vast majority of project partners (users, tech) and associated entities are based in the EU– the EU legal framework is prioritised. Also noteworthy is the distinct nature of partners (tech and users), some of them private corporate entities to which the Business

[1] On issues relating to data privacy and security, double-use and misuse of data, the LSHH aims to complement the Ethics, Data and Security Handbook (EDSH). Therefore, the LSHH should be read together with the EDSH on these issues. In order to avoid repetition, content in the EDSH on export and import data extracted from WP8 deliverables the LSHM co-authored are not repeated in the LSHH and are available in the EDSH.

and Human Rights framework, governed by the 2011 UN Guiding Principles for Business and Human Rights, and consecutive developments within the OECD, EU and National Action Plans (NAPs), applies.

Finally, the deliverable offers a set of guidelines and 'checklists' for tech and user partners in designing and/or operating tools and outputs in view of mitigating risk.

Instruments for the monitoring activity are also indicated, namely the legal, societal and humanitarian helpdesk managed by the Leader of Task 7.7. (the LSHM).

Annex 1 provides a Human Rights Due Diligence Checklist.

# Table of Contents

## LIST OF FIGURES

## LIST OF TABLES

© NIGHTINGALE Consortium, 2022. All rights reserved.

# 1 Introduction

In accordance with the Description of Action annexed to the General Agreement of the Nightingale project (GA), this Handbook devises the landscape of legal, societal, and humanitarian issues applicable to the integration of advanced technology (by tech partners of the project) to First Responders (FRs) in Mass Casualty Incidents (MCIs). This is particularly important keeping in mind the project envisages use of the technology by "regular citizens", which is one of the project's ground-breaking objectives. The Legal, Societal and Humanitarian Handbook aims to ensure the overall objectives of the project to safeguard life, integrity and dignity of victims of MCIs.

Responding to legal, societal and humanitarian challenges in implementing the NIGHTINGALE project is an integral part of the Consortium's agreement with and obligations toward the EU HORIZON2020 framework.

Legal, Societal and Humanitarian Management entails to provide a continuous oversight and monitoring on aspects related to legislative frameworks and humanitarian aspects governing the emergency medicine domain- especially when using new technologies and engaging with non-homogeneous actors (medical, paramedical but also volunteers and citizens).

Understanding the applicable legal or normative framework, its gaps and how to mitigate them, as well as understanding the scope and nature of relevant societal and humanitarian considerations calls for an in-depth understanding of the landscape of First Response in MCIs, its nature and inherent challenges. Only then can the needs be assessed as well as the possible remedy Advanced Technology may offer. The project proposal and General Agreement identifies specific technology developed within the framework of this project- a work in progress resulting from the unique cross-fertilisation process between User partners (from the emergency medical or first response field) and Tech partners at the core of the Nightingale project. The Legal, Societal and Humanitarian Handbook (LSHH) provides the general landscape and the Legal, Societal and Humanitarian aspects Manager (LSHM) will continue to monitor developments throughout the lifespan of the project.

D7.5. interacts also with other deliverables in the project, namely confidential and publicly disseminated deliverables relating to the management guidelines of the Nightingale project (D7.1.), Task 1.1. on “Common Denominators and New Paradigm for Trauma care in MCIs” work progress and intermediary results of three working groups on Triage, Pre-hospitalisation and damage control [not publicly available]; Task 1.6. "Technical Requirements, Specifications and Toolkit Architecture" outputs namely, Mock up session at Nightingale Stockholm Workshop and generally deliverables in WP8, namely D8.2. on any legal requirements relating to NIGHITNGALE activities that may engage in research with humans; D8.4 on export/import of data to a third country; D8.5. on dual use and risk mitigation; D8.6 on potential misuse.

The Legal, Societal and Humanitarian Handbook greatly relies on the open discussions, workshops and meetings held between Consortium partners and User Advisory Board periodically as well as at the project kick-off meeting held in Athens in October 2021, followed by the user workshop on 17-18 January 2022 in Paris (online), consecutive WP1 focal working groups discussions and monthly User Teleconferences, and the March 2022 MRMI workshop in Stockholm on decision

© NIGHTINGALE Consortium, 2022. All rights reserved.

making in MCIs and subsequent discussions and mock-up presentations by tech partners, as well as by Round Table discussions in Oslo. The LSHM wishes to thank all participants for their valuable insights that have permitted to shed light alongside the analysis of legal texts and scholarship on existing national, European and (wherever applicable, at times by adaptation) international legal frameworks. Any content relating to these discussions is done following the 'Chatham House Rules',[2] intended to encourage open discussions, whereby only the content of discussions can be referred to without revealing the identity of who said what (i.e. of the specific partner or the individual) but by general reference, e.g., 'Users' or 'Tech partner'.

**As a word of caution, the present LSHH provides a general framework and cannot substitute legal advice provided on a case-by-case basis. Furthermore, the LSHH bears no prejudice to existing legal obligations all partners are bound by. Each Nightingale partner and any associated entity is responsible to comply with its legal obligations independently. This Handbook aims at making legal frameworks accessible, creating awareness to the legal, societal and humanitarian contexts, providing guidelines, and identifying best practices on how to mitigate risks and challenges. This Handbook is designed to assist, namely in the integration of data protection principles and rights in the MCI environment. It does not, however, replace or provide advice in relation to the application of domestic legislation on data protection, licences, intellectual property rights, security requirements and any other obligation impending on the Nightingale partners and associates in their respective domestic legislation.**

The LSHH is publicly disseminated within Task 7.7 on Social and Legal Aspects. Task 7.7. aims to provide a continuous oversight and monitoring on aspects related to legislative frameworks, societal considerations and constraints and humanitarian aspects governing the emergency medicine domain when integrating advanced technology tools and outputs. Oversight evolves around tasks and responsibilities of the various actors (medical and non-medical CP personnel but also citizens and volunteers), the gathering and utilization of sensitive data (such as vitals or images), the common practices and operational procedures and abidance to applicable lawful regime whilst critical input will be provided when and if there is deviation from laws, common standards, directives and best practices.

Designing tools for crisis management (and more specifically emergency medical response) faces two main challenges: the ability to integrate the relevant legal/ethical framework into the specific technological solutions and procedures, and the capacity to understand society’s expectations and values in a way that is conducive to creating safe and cooperative environments; and to maximise the toolkit's potential adoption rates in economies and societies alike. This includes managing a changing legal, societal and humanitarian framework.

[2] For further information please see official Chatham House website explaining Chatham House Rules available at: https://www.chathamhouse.org/about-us/chatham-house-rule?gclid=Cj0KCQjwrs2XBhDjARIsAHVymmTWZ5V4CGbjTE4NBEWJpmmfChOH4JU-7BoBl5qA5ZWeVJHbw-66GsaAjKiEALw_wcB

© NIGHTINGALE Consortium, 2022. All rights reserved.

**Main Objectives:**

To articulate a reasonable legal framework, identifying the main legal, societal and humanitarian issues arising from the underlying characteristics of the project- at the crossroad between applicable legal frameworks relating to the (1) ACTORS in place, medical and non-medical staff and volunteers, i.e. the rights and duties of First Responders when providing medical and life-saving care in MCIs and, (2) the nature of ACTIONS and TECHNOLOGY applied to different stages of first response in MCIs including allocation of resources in available and adequate hospital care.

**Follow-up to the dissemination of the Legal, Societal and Humanitarian Handbook:**

The applicable legal framework will be published in the 'Legal, Societal and Humanitarian Handbook' (LSHH) (deliverable D.7.5. within T7.7). Following publication, the LSHH will be disseminated among all partners of the Consortium, including users and practitioners and after consultation with the User Advisory Board. Each consortium partner will implement the legal framework defined in the LSHH into its internal procedures and outcomes within NIGHTINGALE and report back to the LSHM on how the legal framework is being implemented, any challenges encountered and how they have been mitigated, if relevant. This objective also interacts with `Task 1.2` led by the LSHM.

The LSHM will review the partners' reports periodically and give feedback where necessary. Monthly consultations will take place once the LSHH is published to report on steps forwards and any challenges encountered. The Legal Expert is also available to provide bilateral training to any specific partner where needed.

Annex I provides a Human Rights Due Diligence Checklist for all partners aimed at ensuring an environment of harmonised compliance with a universal sets of norms, identifying gaps and mitigating risks wherever necessary. On issues relating to data privacy and security, double-use and misuse, the LSHH aims to complement the Ethics, Data and Security Handbook. Wherever this Handbook is silent it refers the reader to the Ethics Handbook, so as to avoid repetition.

Section 2 below provides the context of First Response in Mass Casualty incidents, including definitions for the purposes of this project, the nature of MCIs, their inherent challenges and needs and identifying where advanced technology can enhance capacity. Subsequently, in Sections 3, 4 and 5 we examine the landscape of legal, societal and humanitarian aspects, respectively, each identifying challenges and risks, including risks of double-use and misuse. Finally, Section 5 addresses how to mitigate risks followed by Conclusions (Section 6) and Annexe I offering a checklist for partners on their Human Rights Due Diligence obligations.

# 2 Context of Emergency Medical Response or First Response in Mass Casualty Incidents

## 2.1 Definitions

Providing common definitions for Nightingale partners and other participants is necessary in view of ensuring a smooth and efficient working environment in the process and outcomes of the project. As the role of the Legal, Societal and Humanitarian Aspects Manager (LSHM)  is also to devise the landscape, this Handbook proposes several definitions as references for debate, users, tech partners and other participants may rely on as well as differ from – however, aware of the need to clearly specify wherever they apply terms differently from the definitions proposed below. Definitions in this section are proposed solely for the purposes of the NIGHTINGALE Project and do not necessarily reflect other possible definitions outside Nightingale. This is true with the exception of legal terms, such as what is data, processing, anonymization, pseudonimisation, human rights due diligence and so forth, all defined either the GDPR or other legally binding sources.

i. **A, B, C, D, E- TRIAGE [patient cards]:** is the acronym as to how to perform initial assessment and treatment A: Airway; B: Breathing; C: Circulation; D: Disability; E: Exposure – a method developed to quickly provide a diagnosis of the situation of a patient in the process of TRIAGE.

ii. **Anonymization**:  encompasses techniques that can be used to ensure that data sets containing Personal Data are fully and irreversibly anonymized so that they do not relate to an identified or identifiable natural person, or that the Data Subject is not or no longer identifiable.

iii. **Basic Life Support (BLS)**: is a level of medical care which is used for victims of life-threatening illnesses or injuries until they can be given full medical care by advanced life support providers. The term BLS generally refers to the type of care provided to anyone who is experiencing cardiac arrest, respiratory distress or an obstructed airway. It requires knowledge and skills in cardiopulmonary resuscitation (CPR), using automated external defibrillators (AED) and relieving airway obstructions in patients of every age, and can be provided by trained medical personnel and qualified bystanders. On the ambulance, BLS treatments commonly include administering oxygen, some drugs and a few invasive treatments.

iv. **Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images and dactyloscopic data.

v. **Biometrics or biometric recognition** means the automated recognition of individuals based on their biological and behavioural characteristics. In the Nightingale project, relevant technology includes facial recognition, biometrics in hand bracelets or ear plugs etc.

vi. **Consent** means the freely-given, specific and informed indication of a Data Subject's wishes by which the Data Subject signifies agreement to Personal Data relating to him or her being processed. Informed consent is highly unlikely to get from a patient in a Mass Casualty Incident (MCI), especially in the first stages of response to an MCI. The humanitarian considerations behind FR in MCIs allow some flexibility when applying data protection principles in the humanitarian sector- including FR in MCIs.

vii. **Damage Control (DC):** it includes concepts of damage control resuscitation (DCR) and damage control surgery (DCS) that together seeks to minimize blood loss and focus on the temporary prioritization of physiological stabilization over definitive anatomical repair of the trauma patient.

viii. **Damage Control Resuscitation (DCR):** strategy for resuscitating patients from haemorrhagic shock to rapidly restore homeostasis, including the correction of the components of the so-called lethal triad (coagulopathy, hypothermia and acidosis). DCR aides blood recovery using a holistic approach to replace the functionality of whole blood.

ix. **Damage Control Surgery (DCS):** rapid surgical interventions performed in order to control life-threatening bleeding and contamination followed by correction of physiologic abnormalities and definitive management (Schreiber MA. Damage control surgery. Crit Care Clin [Internet]. 2004 Jan 1;20(1):101–18. Available from: https://doi.org/10.1016/S0749-0704(03)00095-2).

x. **Data Analytics** denotes the practice of combining very large volumes of diversely sourced information (Big Data) and analysing them, using sophisticated algorithms to inform decisions.

xi. **Data Controller** means the person or organization who alone or jointly with others determines the purposes and means of the Processing of Personal Data.

xii. **Data Processor** means the person or organization who processes Personal Data on behalf of the Data Controller.

xiii. **Data Protection Impact Assessment** or DPIA means an assessment that identifies, evaluates and addresses the risks to Personal Data arising from a project, policy, programme or other initiative.

xiv. **Data Subject** means a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Personal Data.

xv. **DPO** in the context of this Handbook means a Tech partner's internal data protection office or data protection officer.

xvi. **Drones** are small aerial or non-aerial units that are remotely controlled or operate autonomously. They are also known as **Unmanned Aerial Vehicles (UAVs)** or Remotely Piloted Aircraft Systems (RPAS).

xvii. **Due diligence** is a process business can and sometimes must carry out to identify and respond to real and potential negative impacts related to their own operations as well as throughout their supply chains. Due diligence requires from companies to take appropriate measures ('obligation of means'), in light of the severity and likelihood of different impacts, the measures available to the company in the specific circumstances, and the need to set priorities. Especially relevant in the context of the Nightingale project are inviolable fundamental human rights (Human Dignity, Right to Life and Right to Integrity of Person) as well as Digital rights affecting privacy, family life, children and vulnerable groups, and might affect (in case of misuse) other freedoms such as the right of association, the right to demonstrate, freedom of expression, free elections and non-discrimination.

xviii. **'Expectant' Patient**:[3] By convention, in situations where the number of casualties and their needs do not exceed the treatment capacities, casualties with signs of life suffering from immediate life threatening injuries are treated, even if their possibilities for survival are low. However, in situations where treatment resources do not meet the needs, one way of compensating for this gap would be to provide treatment only to those severely injured with higher prospects of surviving their injury. An expectant category allows the system to differentiate between the two types of severely injured. The decision to implement the 'expectant' category is dynamic and may be reversed on scene and with time if the resources allow it.

xix. **First Responder(s) (FR):** A First Responder under the LSHH[4] refers to medical and non-medical personnel who would usually be the first on a Mass Casualty Incident (MCI) scene. FRs can be part of national authorities' security providers/police, emergency physicians, paramedics, firefighters (e.g. SAMU, France), trained civilian volunteers, citizens and affiliated actors. They generally include Military, Civil protection and Operators of critical infrastructure e.g. transportations.

xx. **Private security contractors** FRs have different functional roles (e.g., role on the scene where there is also an Incident Commander; role in CC centers), different training and different mandates. Different technologies will be relevant to the different roles play by each FR during the stages of response to a MCI.

[3] Drafted by ESTES Chairman

[4] It should be noted, outside the framework of the LSHH, some would argue that the term first responder should only apply to those who are officially delegated to respond to MCIs. These may be medical and non-medical (police, fire-fighters, other agencies). A different classification should recognize the volunteers – whether these are medical or non-medical. Even then, these volunteers are not officially part of the first responders. Nevertheless, in this LSHH First Responder (FR) refers to anyone involved in providing medical response in an MCI, whether officially delegated or volunteer.

xxi. **Further Processing** means additional Processing of Personal Data that goes beyond the purposes originally specified at the time the data were collected.

xxii. **Health Data** means data related to the physical or mental health of an individual, which reveal information about his/her health status

xxiii. **International Data Sharing** includes any act of transferring or making Personal Data accessible outside the country where they were originally collected or processed, including both to a different entity within the same tech or user partner or to a Third Party, via electronic means, the internet, or other means.

xxiv. **Mass Casualty Incident (MCI):** Any situation where immediately available resources are insufficient for the need of medical care to such extent that it involves a risk for life and health can be considered an MCI (Lennquist, S. (2012). Major Incidents: Definitions and Demands on the Health-Care System. In: Lennquist, S. (eds) Medical Response to Major Incidents and Disasters. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21895-8_1.)

xxv. **METHANE Report:** Mnemonic message to identify critical initial information to communicate during an MCI. Major incident notification; Exact location; Type of incident; Hazard involved; Number of casualties; Emergency services required.

xxvi. **MRMI-** The International MRMI Association, MRMI standing for Medical Response to Major Incidents (MRMI) organises courses exercising decision-making in Mass Casualty Incidents. MRMI organised an exercise in Stockholm for the Nightingale partners and associated entities.

xxvii. **Novel Integrated Toolkit for Emergency Medical Response (NIT-MR):** NIGHTINGALE will develop, integrate, test, deploy, demonstrate, and validate a Novel Integrated Toolkit for Emergency Medical Response (NIT-MR) which ensures an upgrade to Prehospital life support and Triage. This will comprise a multitude of tools, services and applications required for 1) upgrading evaluation of injured and affected population and handle casualties (Triage (including first and second triage or pre-triage and triage – according to domestic custom or regulation)-for the purposes If the Nightingale process is the initial evaluation of injured patients in situations of Mass Casualty Incidents) by offering FRs the means to perform digital identification, allow traceability, support fast diagnosis and prognosis, continuous monitoring and enable accurate classification of medical condition; 2) optimizing pre-hospital life support and damage control through Artificial Intelligence (AI)-based tracking, tracing, routing and utilization enhancements of assets, resources and capacities as well as enabling continuous monitoring and correlation of vital signs and actions; 3) allowing shared response across emergency medical services, non-medical civil protection personnel, volunteers and citizens. The NIT-MR is provided at the service of the emergency medical services, non-medical civil protection personnel, volunteers and citizens for extensive testing, training and validation in the framework of a Training and Validation Program.

xxviii. **Paramedic:** health care professional trained and licensed to provide a wide range of emergency services (such as defibrillation and the intravenous administration of drugs) before or during transportation to a hospital. Compared to EMTs (see above), paramedics often have a higher grade with more responsibility and autonomy in the management of patients. As emergency medical services worldwide operates with different models of care, while in some countries (namely those following the anglo-american model) the paramedic has developed into an autonomous health profession, in others there is no equivalent to this role or they have less autonomy.

xxix. **Personal Data** means any information relating to an identified or identifiable natural person.

xxx. **Pre-hospitalization** or prehospital treatment refers to all medical treatment between the initial TRIAGE and until the patient reaches the hospital. In a Mass Casualty Incident, this will usually be limited to Basic Life Support (BLS).

xxxi. **Processing** means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination or erasure.

xxxii. **'profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

xxxiii. **Pseudonymization**, as distinct from anonymization, means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

xxxiv. **Sensitive Data** means Personal Data which, if disclosed, may result in discrimination against or the repression of the individual concerned. Typically, data relating to health, race or ethnicity, religious/political/armed group affiliation, or genetic and biometric data are considered to be Sensitive Data. All Sensitive Data require augmented protection even though different types of data falling under the scope of Sensitive Data (e.g. different types of biometric data) may present different levels of sensitivity. Given the specific situations in which Humanitarian Organizations work and the possibility that some data elements could give rise to discrimination, setting out a definitive list of

Sensitive Data categories in Humanitarian Action is not meaningful. Sensitivity of data as well as appropriate safeguards (e.g. technical and organizational security measures) have to be considered on a case-by-case basis.

xxxv. **Sought Person** is a person unaccounted for, for whom a tracing operation has been launched.

xxxvi. **Sub-Processor** is a person or organization that is engaged by a Data Processor to process Personal Data on its behalf.

xxxvii. **Third Party** is any natural or legal person, public authority, agency or any other body other than the Data Subject, the Data Controller and the Data Processor.

xxxviii. **Triage:** triage is derived from the French word "trier", which means separating, categorising or classifying, and refers to the categorisation, classification, and prioritization of patients and injured people, based on their urgent need for treatment. The process of triage allows the responders, who do not have enough resources to treat everyone, to prioritize care services, so that most services are provided to the greatest number of injured people. Over twenty triage systems are used around the globe and can be found in the literature: (Bazyar, J., Farrokhi, M., & Khankeh, H. (2019). Triage systems in mass casualty incidents and disasters: a review study with a worldwide approach. Open access Macedonian journal of medical sciences, 7(3), 482., namely, Simple Triage and Rapid Treatment (START), SIEVE, SALT, Homebush triage Standard, Careflight, STM, MASS, Revers, CBRN triage, Burn Triage, META Triage, Mass Gathering Triage, SwiFT Triage, MPTT, TEWS Triage, Medical Triage, mSTART, ASAV, CESIRA Protocol, Military Triage, Jump START (pediatric).

xxxix. **Pediatric Triage Tape (PTT) Triage:** Triage (from the French ‘trier”) aims to sort the patients according to their severity of injury and their needs. Many different methods of triage exist. Different systems use either 2, 3 or 4 categories. Their common aim is to allow prioritizing patients so that those who most need the limited resources will receive them first. Triage is a dynamic process and triage category may change following treatment or reassessment on scene.

The reference TRIAGE in the LSHH relies on the MRMI (see definition) exercise held in Stockholm in March 2022 whereby 3 categories were used: RED patient (critical patient- top priority for evacuation from the MCI scene to the hospital), YELLOW patient (severely injured- second in priority for evacuation) and GREEN patient (usually recognized by the ability to walk independently and showing all good vital signs with minor or non-life threatening wounds). Users from different agencies and jurisdictions tend to use the terms: 'pre-triage' and 'triage' (under the German system) or 'primary triage' and 'secondary triage', respectively. Primary triage, secondary triage and the subsequent numbering is used to point out "different purposes of triage" – primary triage is for "initial field care" second for "advanced field care" / transfer to AMP third one – for transportation to a hospital etc.

© NIGHTINGALE Consortium, 2022. All rights reserved.

## 2.2 Devising the landscape: inherent challenges providing emergency medical or first response in MCIs

What is a Mass Casualty Incident (MCI)? Different FR agencies in different domestic jurisdictions define MCIs differently. For some, more than 5 injured is an MCI, others consider there to be an MCI from 24 injured and above, for others, different scales apply still. There seems to be a consensus between users from different national agencies and jurisdictions that an MCI has several common denominators. The first of which is that an MCI entails a casualty incident where the needs are higher than the available resources. This fact affects the capacity to treat, perform TRIAGE, prognosis and diagnosis and overall the decision-making process, i.e. where in regular emergencies treatment would be provided immediately, in MCIs this is not possible- treating one patient immediately would cause additional casualties and loss of life.

Therefore, MCI scene medical management includes many components that need to be implemented as quickly as possible. The FR need to call for help which is proportional to the scope of the event. The site needs to be organized into working areas in order to allow efficient use of incoming personnel. An area from which the injured will be transported to the hospitals should be organized. Except for restricted immediate life-saving treatment (e.g. clearing breathing canal and stopping severe bleeding), the objective is to do a TRIAGE (see definitions) in view of prioritizing those most in need and who can be saved. In view of this point, recent years have pushed health care and public health systems to identify and refine emergency preparedness protocols for disaster response. Scholars in the field have been primarily focused on the ethical justifications for crisis standards of care as well as a need for ethics guidelines for implementing CSCs; the ethical justifications for triage, both as to which criteria to use and the appropriate processes by which to employ triage.

Another common denominator to MCIs is their short timeframe. Unlike humanitarian disasters or humanitarian emergencies that can take weeks or months and are usually on a large area, MCIs usually require no more than several hours (e.g. in the Madrid 11 March 2004 terrorist attacks 1500 were injured, 191 were killed First Response took approximately 3 hours), in rare cases exceeding 24 hours (e.g., case of collapse of a building and people trapped under the rubble, perhaps due to earthquake). MCIs are characterized by high stress levels, possibly dangerous environments, limited capacity and where time and correct decision-making saves lives.

MCIs are either man-made (e.g., incidents occurring within an armed conflict, a terrorist attack, a chemical explosion) or are a result of natural causes (e.g. tsunami, earthquake). Different partners prioritize different kinds of MCIs depending on their experience and working culture. The LSHH relates to the common denominators identified at the early stages of the NIGHTINGALE project.

### 2.2.1 Common denominators in an MCI scene

**What is the landscape of MCIs dictating the reality of FRs?** Below, a few common denominators drawing the structural realities of an MCI:

© NIGHTINGALE Consortium, 2022. All rights reserved.

**The fog of war:** Many FRs in MCIs refer to it under the reference of 'fog of war'. Indeed, unlike any other situation medical and non-medical staff and volunteers composing FR units have to act quickly, in great uncertainty as to the nature of the event, scope and location. For instance, in the 2015 Paris Attacks, on November 13, terrorists attacked different locations in central Paris at short intervals or simultaneously. Emergency calls flooded in and were confused and inaccurate as the callers themselves were in a state of extreme stress and uncertainty. FRs in MCIs act while confusion is on-going, at times having essential information about the MCI scene only in the aftermath (e.g., what happened? Who attacked? How many attackers? Where did attacks take place? How many wounded? Where are the wounded? In several attack scenes- what are the scenes receiving FR and others where FRs have not gotten to yet? )

**Insecure environment**: Despite the relatively short time span of an MCI, FRs can only intervene after the scene is secured. Therefore, they depend on security forces (e.g. national police, military or special forces) to be able to act and save lives. Scenes can be insecure either (man-made MCI) because the attacker is still on the scene and armed, multiple attacks aimed at attacking those providing life-saving assisting and causing great terror and fear; or (natural-made MCI) due to the fact of an unstable environment- fire, toxic material, a building continuing to collapse, earthquake relapsing.

**Scarcity of resources:** inherently, an MCI scene is a scene where FRs have less resources at hand than they would need in order to treat all casualties as they would do in 'regular' emergencies in which a limited number of casualties are attended.

**Working in a highly stressful environment:** MCIs occur under extreme circumstances, strict timeframes, in psychologically and physically stressful environments both for FRs and casualties. This reality affects decision-making processes and emphasizes the need for preparedness and adequate training, taking into consideration the stressful conditions (large amount of severely injured, signs of violence, extremely short time span to act, lack of ambulances, FR staff and so forth).

**MCIs in urban areas**: Urban areas are usually densely populated areas. It can be more challenging to transport to and from an MCI scene in an urban area, receive flight certificates (e.g., for UAVs (e.g., drones)- flight authorisation need to be requested in advance and before an emergency situation occurs. There is a need for clear regulation/protocols for employment of UAVs in emergency situations). On the upside, MCIs in urban areas usually involve proximity to hospitals and emergency or trauma care.

**MCIs in rural areas**: Rural areas will usually be characterised by their remoteness from central hospitals with larger capacity further challenging evacuation from the MCI scene and receiving treatment.

**Nature of response, limited treatment at the MCI scene:** treatment in an MCI scene is usually limited to opening airways enabling the patient to breath, if breathing canals are blocked; and stopping severe or life-threatening bleeding. All other resources are devoted for TRIAGE, evacuating casualties to the hospital and managing resources and prehospital care (e.g., coordinating available emergency transportation and capacity in terms of emergency operation room and trauma, communicating needs and identifying resources under stringent timeframes).

### 2.2.2 Inherent Challenges and NEEDS

Identifying inherent challenges and needs of FR in an MCI is a necessary step in optimally proposing gaps advanced technology can help overcome. Below a list of identified challenges and needs arising from Nightingale project interaction:

a. **Localisation**: an MCI begins as an uncertainty that can take a few minutes sometimes longer, to certify. One of the first challenges is localising the MCI scene with precision. There can also be a multiple scene MCI.

b. **Information flow**: in an MCI there is a high information flow. FRs need to be able to receive reliable information after it has been filtered and distinguished from unreliable information. Needed information relates to the MCI scene (What? Where? Who? How many?) and to resources from FRs to hospitals (FR available, available transportation, ambulances, capacity and localisation of hospitals and adequate staffing and equipment- availability in Emergency, Operation, Trauma or 'stuff, staff and structure'). During MCIs there is often a collapse of cellular networks due to the high number of civilians calling to check on their loved ones- the need for reliable emergency communication settings. Therefore, there are two major needs relating to information flow: an information management need and a telecommunication/technology infrastructure management need.

c. **Overflow of data**: too much data is a situation to avoid, the issue being the need to prioritize data, receive synthesized or raw data, real and false data. The amount of information any FR is able to process is limited under stress at any given moment. There is a need to ensure reliable, accurate, accessible and targeted information flow.

d. **Hands need to be free:** especially during the 'pre-triage' or 'primary triage' but also throughout triage, FRs need to have their hands free to check the patient's situation, stop severe bleeding, open airways. FR gloves will quickly be covered with blood.

e. **Tracking and tracing:** patients on the MCI scene may not be able to communicate or to be identified. FRs need a simple to employ means to identify a patient (using numbers, TRIAGE monitoring (e.g. colours RED, YELLOW, GREEN), Other data) and trace that patient also after the MCI scene regardless of the patient's condition.

f. **Differences in protocols between different FR agencies of the same country:** At times, under the same jurisdiction, several entities are competent to act as FRs. Differences in protocols may exist between different agencies (medical, police, fire-fighters), but may also exist between different agencies in charge of a similar component such as medical (two or more responding health organizations). In an MCI, there needs to be pre-existent and clear regulations as to who is the MCI scene commander, who is the medical coordinator and what protocols will be followed at every stage of First Response (Triage, Pre-hospitalisation life support and Damage Control). Part of the challenge (especially in multi-national rescue teams) is that there is no common TRIAGE system, there are multiple TRIAGE systems. The issue of compliance with existing protocols is a matter for national societies, internal review and monitoring of the different agencies involved.

g. **Psychological strain and debriefing:** An MCI entails working under extreme conditions and psychological strain. There needs to be a configuration not only of training BEFORE an incident and providing FR DURING an incident but also debriefing AFTER an incident, such as, post-trauma resilience (prior and after) and treatment where needed.

h. **Absence of consent:** At the early stages of an MCI consent from patients most in need of evacuation from the scene and treatment is not realistically possible. Under non-emergency situations, consent would be acquired as to the scope and nature of treatment and in relation with personal/sensitive data processing. Considering the emergency context, the priority of course is saving lives. A different question arises as to what would also justify lack of consent with 'Green' patients- who are able to walk and express themselves freely.

i. **Involving bystanders and volunteers in response to MCIs:** part of the project ambitions includes involvement of bystanders and volunteers in view of assisting FRs in MCIs. This may entail questions of liability and need of outreach and training to the public of methods of response in MCIs (e.g., civil training at schools, youth organisations, as a condition to acquiring a driver's licence and so forth).

### 2.2.3 How can advanced technology enhance first response in MCIs?

Based on the needs assessment, below you may find a mapping in telegraphic format of mitigating factors with specific attention to advantages integrating advanced technology may offer, before, during and after an MCI. Of course, how this is to be translated de facto is left to the expertise of the tech partners of the project and is outside the scope of the Legal Handbook.

#### 2.2.3.1 Before

a. Preparedness and training are essential to ensure before a MCI emerges. The MRMI exercise is an excellent example of adequate decisional training (alongside technical training which is equally important), integrating real-time considerations and an overall look at the MCI from the scene to hospital including. After technology trial is completed, future training should integrate the NIT-MR (toolkit) whereby FR User partners will learn to use the toolkit and adapt it to their needs.

b. Agreeing on protocols: every national/regional jurisdiction should adopt a clear protocol to apply in an MCI, including designating the Commander FR in an MCI scene, requiring prior sharing of capacity by hospitals and regularly monitoring and updating the information as an integral part of national/regional preparedness for emergencies of varying scope.

c. Resources management: a clear resource management system, regularly updating capacity in different hospitals across a territory is essential in providing FR in MCIs and should be considered an issue of national security. As such, national security considerations over-ride interests of private actors, providing any limitations are proportionate with the objective at hand.

d. Advantages of advanced technology:

i. enhancing preparedness: advanced technology may be integrated to enhancing preparedness for example when integrating advanced technology to training tools (e.g. in existing MRMI exercises; in enhancing training through simulations of MCIs; augmented reality simulations and so forth).

ii. resource management: AI, information flows and transparency- visual updating of available resources and their geographic location, quality and quantity control and communication to authorized individuals or authorities. Resource management implies not only hospitals but also 'stuff, staff and structure'.

iii. Resilience and treating and preventing Post Traumatic Stress Disorder (PTSD) courses using simulations with advanced technology (outside the scope of the Nightingale project).

#### 2.2.3.2 During an MCI

e. Appointing a Scene Commander and ensuring good, comprehensive communication between different actors linked to the MCI scene;

f. Ensuring timely transparency of the MCI scene

g. Ensuring timely, accurate and transparent resource management- communication between scene, Regional/Area Commander and hospitals according to needs;

h. using available resources optimally

i. Advantages of advanced technology:

   i. rapid and reliable localisation of MCI scene;

   ii. identification of cause of MCI;

   iii. identification of number of affected individuals;

   iv. triage: prioritizing patients for treatment and evacuation; monitoring change in prioritizing according to patients' evolving needs and available resources;

   v. communicating outside the immediate MCI scene and identifying available adequate resources

#### 2.2.3.3 After an MCI

j. Debriefing, lesson learning and team spirit; psychological support and resilience treating and preventing Post-Traumatic Stress Disorder (PTSD);

k. Written reports follow-up implementation in training

l. Outreach and communication with civil society, media, politicians (local, national and EU where relevant)

m. Advantage of advanced technology

   i. lesson learning from the scene- 'fog of war' over: processing data from the scene for future learning and bettering the next response in the next MCI

   ii. comparative learning and self-assessment: knowledge sharing among different agencies and different jurisdictions: on a confidential restricted basis while respecting human dignity, right to privacy (anonymization of information); and national security (authorized individuals only and authorized by national security authorities); augmented reality

iii. can be useful in providing mental resilience training (from post-traumatic disorder PTSD) prior (resilience building methods) and after (PTSD treatment) an MCI for e.g., by using simulations integrating advanced technology.

### 2.2.4 Conclusion

There exist inherent challenges in providing first response in MCIs; Advanced technology add into the existing complexity of First Response in MCIs. The NIGHTINGALE project and in turn the legal, societal and humanitarian landscape assessed is limited to the meeting point between advanced technology and FRs operating in MCIs. Certain inherent challenges to First Response in MCIs are therefore outside the scope of the project, nevertheless, they may be addressed in the societal or humanitarian discussion below.

Integrating advanced technology is aimed at bettering and enhancing response in view of saving lives, indiscriminately of the identity of the patient, of his/her origin, gender or beliefs. The project operates under the principle of 'do more good than harm' and is cognisant of risks of double-use and misuse of technology and data. The present Handbook aims to set out as clear a legal framework as possible, while taking into account also societal and humanitarian challenges, in view of mitigating risk, ensuring the commitment of all project partners, enabling the monitoring of each partner's compliance with existing legal frameworks under each partner’s direct and independent responsibility. The Handbook enables to identify gaps and proposes ways to mitigate them. Furthermore, the Handbook reflects the Nightingale Consortium awareness of the general gap that exists between the inherent value of any technology and the ability to put it to work effectively. This is a particular challenge managers should undertake. Challenges include for instance technologies' inescapably dual role, the variety of internal markets to be served, legitimate resistance to change and the need to build trust, the right degree of promotion, the choice of implementation site, and the need for one person to take overall responsibility.

# 3 Legal Issues and applicable normative framework for Nightingale tools and outputs

Integrating advanced technology into an already sensitive context of first response in MCIs presents several legal challenges. Alongside the 'classic' applicable normative framework, advanced technology presents new challenges for International, EU and national regulator bodies. The activities under the GA of the Nightingale project to which legal frameworks apply include developing, testing and applying advanced technology and recruiting, training FR personnel (either staff or volunteers, medical or non-medical, national authorities or civilians) who will eventually provide the first response on scene in MCIs. The Handbook provides the legal framework followed by an Impact Assessment 'checklist' for Nightingale partner and associates in view of recognizing the effects of their activities on fundamental human rights and other legal considerations, in order to ensure compliance by all Nightingale partners and associated entities, namely when applying the NIT-MR (the integrated toolkit) to FR in MCIs.

## 3.1 Corporate Due Diligence within the Business and Human Rights Paradigm: Standards for Compliance of Users and Tech Nightingale Partners and Associates

International and EU law impose duties on States. Individuals and corporate entities are bound by national laws which can be enforced by national authorities and courts. Domestic law mostly interprets and implements international and EU laws but may go beyond to impose stricter obligations. What international laws are binding on corporate entities in relation with fundamental human rights? What is the standard of obligation binding on private, public and corporate entities and can individuals effectively seek remedy for violations in domestic, EU or international courts? Finally, what is 'Due Diligence'?

The Nightingale project and its partners can play an important role in contributing to economic, environmental and social progress, but to do so they must also ensure that they manage negative impacts associated with their activities.

**Due diligence** is a process business can carry out to identify and respond to real and potential negative impacts related to their own operations as well as throughout their supply chains. It is based on an obligation of means (as opposed to an obligation of result) requiring corporate entities to apply specific measures aimed at identifying and mitigating risks. This Handbook is an example of such measures to be followed by periodic review and monitoring of implementation.

Today's legal landscape already identifies both 'soft' law (aspirational) and binding law on corporate entities, as described herein.

The 2011 UN Guiding Principles on Business and Human Rights (UN GPBHR) were adopted under the hospices of the UN Office of the High Commissioner for Human Rights (OHCHR) and its mechanisms to elucidate the framework for corporate responsibility to respect human rights in their activities and impact.

The UN GPBHR provide a consensual umbrella legal framework for states and corporate entities in terms of Business and their obligation to respect Human Rights. It has three pillars: on the state duty to protect human rights, *corporate responsibility to respect human rights* and access to remedy of victims of business-related abuse. The digital world presents specific challenges in what in 2019 the UN High Commissioner for Human Rights called *'digital centres of power'* that go unregulated and present high risks for fundamental human rights. A clearer legal framework benefits corporate entities and will enable Nightingale project partners to act in compliance with their obligations in view of mitigating risks.

Subsequently, the UN GPBHR were implemented by further binding (or work-in progress) legal instruments, such as the 2018 OECD Due Diligence Guidance for Responsible Business Conduct and most recently, in February 2022 the EU Commission submitted its proposal to the EU Parliament on Due diligence for corporate entities, known as 'the EU Proposal for a Directive on Corporate Sustainability Due Diligence'. While the proposal directly affects only limited liability companies of substantial size and economic power (with 500+ employees and EUR 150 million+ in net turnover worldwide) (Group 1) and other limited liability companies operating in defined high impact sectors, which do not meet both Group 1 thresholds, but have more than 250 employees and a net turnover of EUR 40 million worldwide and more (Group 2) and non-EU companies of the same scale; Small and medium companies (SMEs) are indirectly affected. Nevertheless, seeing SMEs will eventually be affected by the EU Proposal, possibly within the lifespan of the project funding, and in view of voluntarily abiding by the highest available standards- seeing the context of integrating advanced technology (and sensitive data) in MCIs, the Handbook takes into account the EU proposal and sets out guidelines for an impact assessment and mitigating risk. Noteworthy, the proposal provides accompanying measures for SMEs that will be indirectly affected once the proposal comes into effect. In sum, within the Nightingale GA Nightingale partners are effectively committed to:

- integrate due diligence into policies;
- identify actual or potential adverse human rights and environmental impacts;
- prevent or mitigate potential impacts;
- bring to an end or minimise actual impacts;
- establish and maintain a complaints procedure;
- monitor the effectiveness of the due diligence policy and measures;
- and publicly communicate on due diligence (while maintaining confidential restricted information confidential under the Nightingale GA).

Finally, on the legal landscape of due diligence, a number of Members States have already introduced national rules on due diligence and some companies have taken measures at their own initiative. Due diligence extends to the company's own operations, their subsidiaries and their value chains (direct and indirect established business relationships).

More concretely, this means more effective protection of human rights included in international conventions. For example, workers must have access to safe and healthy working conditions, gender equality and strict non sexual violence policies. **Nightingale partners and associates in scope will need to take appropriate measures (‘obligation of means')**, in light of the severity and likelihood of different impacts, the measures available to the company in the specific circumstances, and the need to set priorities. Within the NIGHTINGALE project severity and likelihood of different impacts have to do with human society effects in recruiting and training staff or volunteers, medical and non-medical (e.g. non-discrimination, gender equality and safety); and more importantly effects related to specific advanced technology presenting certain risks, namely through data processing, artificial intelligence, biometrics (data), tracing and tracking, and the use of drones (UAVs).

Outside the Nightingale project, National administrative authorities appointed by Member States are responsible for supervising existing and new rules and may impose fines in case of non-compliance. In addition, victims will have the opportunity to take legal action for damages that could have been avoided with appropriate due diligence measures. Again, the obligation is an obligation of means- this is why the Human Rights Due Diligence Impact Assessment (Annex I) is of high importance.

To ensure that due diligence becomes part of the whole functioning of companies, directors of companies need to be involved. This is why the EU proposal also introduces directors' duties to set up and oversee the implementation of due diligence and to integrate it into the corporate strategy. In addition, when fulfilling their duty to act in the best interest of the company, directors must take into account the human rights, climate change and environmental consequences of their decisions. Where companies' directors enjoy variable remuneration, they will be incentivised to contribute to combating climate change by reference to the corporate plan.

**The due diligence framework provided in the Legal Handbook** aims to ensure that Nightingale partners, including both the private and public sectors, act in full respect of its international commitments in terms of respecting human rights and sustainable development, as well as international trade rules.

Adopting the OECD Due Diligence model the Countries of Origin of which all Nightingale partners are based are members in entails applying the following due diligence process and supporting measures made of five (or six) main steps: embedding responsible business conduct into partner policies and management systems; identify and assess adverse impacts; cease, prevent or mitigate adverse impacts; track implementation and results; communicate how impacts are addressed and where needed provide for or cooperate in remediation. The LSHM will receive communications from Nightingale partners on these stages and on how impacts are addressed in periodic review inscribed in the GA.

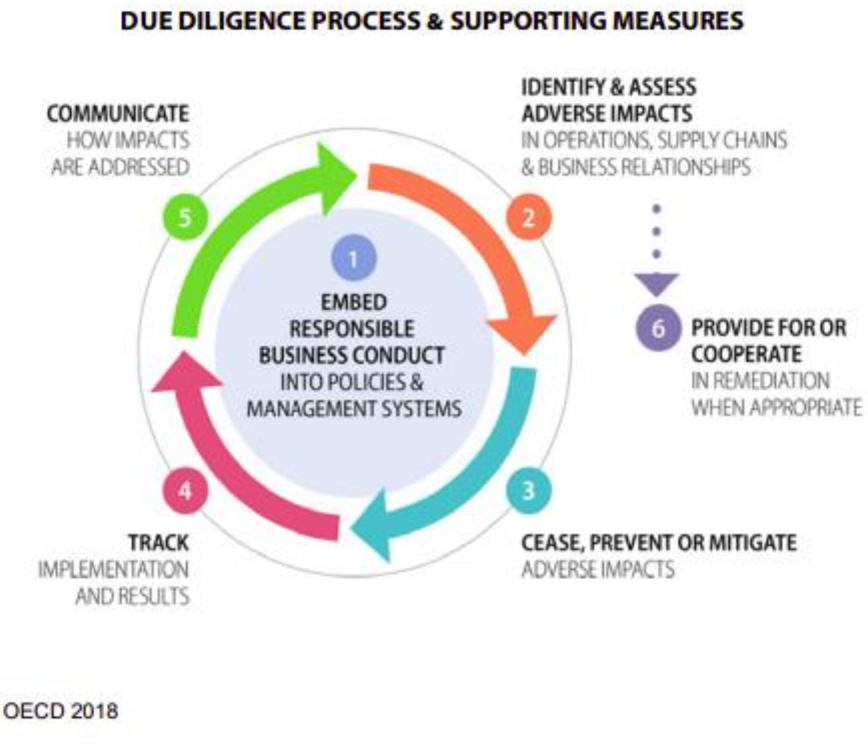

DUE DILIGENCE PROCESS & SUPPORTING MEASURES
1
EMBED RESPONSIBLE BUSINESS CONDUCT INTO POLICIES & MANAGEMENT SYSTEMS
2
IDENTIFY & ASSESS ADVERSE IMPACTS IN OPERATIONS, SUPPLY CHAINS & BUSINESS RELATIONSHIPS
3
CEASE, PREVENT OR MITIGATE ADVERSE IMPACTS
4
TRACK IMPLEMENTATION AND RESULTS
5
COMMUNICATE HOW IMPACTS ARE ADDRESSED
6
PROVIDE FOR OR COOPERATE IN REMEDIATION WHEN APPROPRIATE
© OECD 2018

*Figure 1 Due diligence process and supporting measures*

What are the main legal issues to take into consideration for tools and outputs in the Nightingale project framework? The Classic and the Novel legal issues relevant to Nightingale project activities are consecutively examined below.

## 3.2 Classic legal issues

Classic relevant legal issues applicable at all times and should therefore be included in the HRDD Impact Assessment (see Annex I)- but to a different degree, at different levels and perhaps to different actors within the Nightingale context- include namely, Human Dignity, the Right to Life, Right to the Integrity of the Person, Respect for Privacy and Family Life, Protection of Personal Data, Freedom of thought, conscience and religion, freedom of expression and information, freedom of assembly and of association, right to property (including intellectual property), non-discrimination, cultural, religious and linguistic diversity, equality between men and women, the rights of the child (also affected by decision by a private body, integration of persons with disabilities, workers' right to information and consultation, protection in the event of unjustified dismissal, fair and just working conditions, prohibition of child labour and protection of young people at work, family and professional life (e.g. maternity or paternity leave), social security and social assistance, health care, environmental protection (Nightingale partners must comply with EU/national sustainability policies, as far as possible given other priorities at stake), consumer protection; as well as internal partner and Nightingale review processes.

### The EU Legal Framework

The EU is built on fundamental rights, democracy and the rule of law. Article 2 of the Treaty on European Union (Lisbon Treaty) provides that “The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail”.

These values are closely linked and guide the EU’s internal and external action.

EU action in this area is based on the EU Treaties and on the EU Charter of fundamental rights (ECFHR), which has the same value as the Treaties. The Charter enshrines the fundamental rights people enjoy in the EU. It is a modern and comprehensive instrument protecting and promoting people’s rights and freedoms in the light of changes in society, social progress and scientific and technological developments.

The Charter applies in conjunction with national and international fundamental rights protection systems, including the European Convention on Human Rights (ECHR). What these rights mean in practice can vary from what might seem clear or reasonable application and is based on interpretation by case law and legal developments. This is where the LHSM can provide guidance to Nightingale partners.

Nightingale project activities may directly affect rights enshrined in the European Charter for Fundamental Human Rights and the Nightingale partners have the obligation to respect these rights. The LSHM is readily available to provide specific guidance or training where needed. Monitoring will be practiced through periodic review. Below, a description of relevant rights and action required from partners and associated entities, beyond the general obligations to respect and comply.

### 3.2.1 Human Dignity, Right to life and Right to the Integrity of the Person

The Nightingale project aim is to enhance first response in MCIs by integrating advanced technology increasing the capacity of FRs operating in a humanitarian setting where impartial, lifesaving actions (Triage, life support in Prehospitalisation and Damage Control) are administered. At the core of these actions stand the fundamental human rights of:

i. Human Dignity (Article 1): '*Human dignity is inviolable. It must be respected and protected*';
ii. the Right to Life (Article 2);
iii. the Right to the Integrity of the Person (Article 3) stating, ' *1. Everyone has the right to respect for his or her physical and mental integrity.*'

> And more specifically in the context of first response in MCIs and the tools and outputs Nightingale aims to integrate to first response:
>
> '2. *In the fields of medicine and biology, the following must be respected in particular: (a) the free and informed consent of the person concerned, according to the procedures laid down by law;'*

Unlike other fundamental human rights which may be limited under certain circumstances, for example when weighed with other rights (for example limiting freedom of expression to enable the right to private property when allowing patent/intellectual property rights), human dignity and integrity of the person are inviolable rights. While the right to life is articulated in the EU Charter with less derogations (prohibiting the death sentence) than in other international human rights law instruments, the right to life is not absolute for example the life of combatants in armed conflict, or death by self-defense (violently resisting arrest) in a peacetime situation.

**Specific Action required: Nightingale Users who many are bound by medical deontology have also sworn to these three fundamental rights: the sanctity of life, human dignity and the integrity of the person. All Users must incorporate these three principles including in consent forms from participants, staff and volunteers. Other partners should incorporate these principles into their management and process policies, especially in view of the integration of advanced technology in First Response in a MCI. It should be noted that in MCIs and other emergencies (e.g. humanitarian emergencies) where it is difficult or impossible to receive consent of the patient, consent obligations are more lenient in view of the purpose at hand: to save lives. However, in relation with patients who can communicate and once the emergency status no longer exists, i.e. in the aftermath of an MCI, consent becomes an obligation once more. Nightingale partners and associated entities will remain loyal at all times to the overall objective of saving lives in MCIs and to their own national regulation (laws, protocols, codes of conduct/deontological codes).**

### 3.2.2 Respect for private and family life

Article 7 of the EU Charter for Fundamental Human Rights enshrines the right to private and family life including 'respect for private and family life, home and communications'. It corresponds to rights guaranteed by Article 8 of the ECHR. To take account of developments in technology the word 'correspondence' has been replace by 'communications'.

In accordance with Article 52(3), the meaning and scope of this right are the same as those of the corresponding article of the ECHR. Consequently, the limitations which may legitimately be imposed on this right are the same as those allowed by Article 8 of the ECHR:

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

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

**Action required: Considering the context of MCIs they are included within the scope of exceptions to respect of private and family life. In MCIs it may be necessary to intercept communications for national security, public safety and for the protection of health. Nevertheless, this is made possible through the application of national laws and restriction. Also, limiting private and family life can be done lawfully providing Nightingale partners apply strict data protection policies, especially in view of sensitive data (by using anonymization, pseudonymisation, restricted access personnel, etc. See Ethics, Data and Security Handbook for more detail). An additional condition for the lawfulness of restricting the right to private life is in keeping with the aims of the project, protecting (as much as possible) from misuse of tools and outputs by internal or more realistically external entities to the Nightingale project. Nightingale partners are also responsible to each secure staff and volunteer comply with applicable policies- to be inserted in the consent forms. (see consent form in Ethics, Data and Security Handbook).**

### 3.2.3 Protection of personal data

Article 8 of the EU Charter clearly enshrines the right to protection of personal data and states:

*"1. Everyone has the right to the protection of personal data concerning him or her.*

*2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*

*3. Compliance with these rules shall be subject to control by an independent authority."*

© NIGHTINGALE Consortium, 2022. All rights reserved.

**Action required: Complying with the GDPR consists in complying with Article 8 of the EU Charter, therefore no further details is needed, see the Ethics, Data and Security Handbook for specific guidelines. The principle of minimisation of data to strictly necessary should be applied, anonymization and pseudonymisation is applicable. So for example, in order to provide real-time patient information, the patient may be identified by a number, whereby the patient's personal data (name, address etc.) can be stored in safety, with coded access and/or access to strictly authorised personnel- whereby the patient number is registered and linked to the patient's personal data. Noteworthy: attention should be given to personal data (personal details allowing the identification of individuals) and to sensitive data, including patient data, biometrics (including facial recognition technology) and big data (large-scale collection of data for the purposes of Artificial Intelligence (AI) technology.**

### 3.2.4 Non-Discrimination and cultural diversity policy

The prohibition of discrimination is a non-violable principle. It is enshrined in international human rights treaties (see references) and in European Human Rights Treaties including the EU Charter for Fundamental Human Rights. Discrimination consists in difference of treatment in law or in effect *'based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation'* and shall be prohibited. Furthermore, *'Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.*' (Article 21 of the EU Charter)

Article 22 of the EU Charter further recognizes *'The Union shall respect cultural, religious and linguistic diversity*'.

Nightingale partners are committed to the principle of non-discrimination in their internal policies, when recruiting staff or volunteers, medical or non-medical, when designing technology and in every stage of the AI process of algorithms and in their application in the field. The Nightingale Consortium itself demonstrates diversity of its partners and associated entities and in accordance with the GA.

**Required Action: Nightingale partners shall implement non-discrimination and diversity policies and work to identify where such principles may be affected. Monitoring and periodic review will include reporting on how partners comply with these principles in policies and in effect (e.g. by training staff, having clear non-discrimination internal regulations and internal review of its application in effect as well as the existence of internal, though independent and impartial focal points in case of breach to file and address complaints).**

### 3.2.5 Gender equality, anti-harassment policy and prohibition of any form of sexual violence

Any form of mental or physical violence is prohibited by national laws, including in the workplace. There is specific attention given to sexual-based violence or harassment and to gender equality. For gender equality please refer to the Ethics Handbook. Article 23 of the EU Charter states: *'Equality between women and men must be ensured in all areas, including employment, work and pay. The* *principle of equality shall not prevent the maintenance or adoption of measures providing for specific advantages in favour of the under-represented sex*.'

While it may seem unthinkable, sexual and gender-based violence (SGBV) has been reported, investigated and criminally prosecuted even in humanitarian settings such as humanitarian emergencies. While it is true MCIs occur over a limited time span, due diligence process requires to prevent rather than to punish, notwithstanding the obligation to report and address any SGBV or other forms of violence if it occurs.

**Required Action: Nightingale partners and associated entities will include gender equality policies and zero tolerance to mental, physical or sexual harassment, as well as strict prohibition of SGBV or any other form of violence- at every stage of activity: in the recruitment of personnel, training of FRs, testing of NIT-MR toolkit, designing tools and outputs, in MCIs in the aftermath of the lifespan of the project. Each partner should designate a focal point for gender equality, harassment and SGBV, train and review compliance. Partners will report on how they already comply or have adjusted policies to the LSHM during the periodic review.**

Alongside the 'classic' legal issues applicable at all times and where advanced technology and recruiting and training of FRs may affect fundamental rights, the Handbook examines legal issues arising specifically from the nature of project participants and activity.

## 3.3 Legal Issues specific to the NIGHTINGALE Project

Specific legal issues arise in the context of Integrating advanced technology to First Response in MCIs. This reality adds in to already complex legal settings in FR in MCIs. The scope of devising the legal landscape is limited to the meeting point between advanced technology and First Response in MCIs.

Nevertheless, Nightingale partners and associated entities should be aware of existing legal challenges in MCIs in view of mitigating direct or indirect risks they may entail. Additionally, some of these challenges may also have negative societal effects (see for further societal and humanitarian considerations in Section 3 below). Listing the legal challenges characteristic to MCIs is not exhaustive. For these reasons, legal issues arising in First Response to MCIs independently of integrating advanced technology is addressed succinctly below:

### 3.3.1 Legal Challenges relating to emergency medicine or First Response in MCIs

The main legal challenges FR deal with in MCIs arise in as to the different mandates of different FRs within the same jurisdiction, the scope and nature of liability if at all for decisions taken during an MCI, nationals laws such as 'the Good Samaritan Law', the reality of an 'expectant' patient and the existence of either errors or what sometimes may be commonly referred to as 'medical miracles', to name but a few.

#### 3.3.1.1 Absence of homogeneity in different jurisdictions and among different agencies in the MCI context

As a multinational project, the Nightingale project engages with partners from different jurisdictions. Different jurisdictions apply different legal frameworks to similar situations, even within EU countries. Partners must be aware of national legislative frameworks and apply them, including in terms of who has the authority to declare a patient is deceased, the composition and mandates of different national or local agencies, product certificates and so forth.

Wherever partners physically go to different territory, they are bound by the national legislative framework applicable in that territory. Seeing that travel within the Nightingale project is intended for research, training, learning and development purposes and not to actually administer. First Response in real-time MCIs, there is no immediate risk arising from the differences in regulation between different Users. It should be noted nevertheless that the Nightingale project also has the ambition to provide answers to multi-national emergency medical response settings. Seeing the complexity and challenge in setting guidelines to an under-regulated field, whereby the domestic laws are specific and heterogenic, and in accordance with the General Agreement (GA), the present Handbook aspires to clarify the EU legal framework, identify gaps and risks, and propose methods to mitigate risks.

Wherever a specific difficulty will arise, the relevant partners are welcome to turn to the LSHM who will examine the issue and propose a solution, in cooperation with the partners' legal advisors, DPOs or other relevant entity.

#### 3.3.1.2 'Good Samaritan' laws

Medical staff is exposed to liability. In MCIs, due to emergency situation, this liability is limited to cases of malpractice in emergency situations. Non-medical staff or civilian volunteers may also be liable for damages suffered by treatment provided in pre-hospital emergency medicine, including in MCIs. While certain jurisdictions may shield FRs from liability, others do not. Some jurisdictions impose a duty to intervene to save life sanctioned by criminal law in case of non-compliance. Legal norms vary from one jurisdiction to another.

While civil lawsuits of this nature in the context of MCIs are less common or less likely to occur in the national jurisdictions of the Nightingale partners, it is not impossible. Any entity training personnel (medical or non-medical, staff or volunteer) should include clear and reliable information on the national laws applicable to such personnel's potential liability in case of harm suffered to a patient even in an MCI. Consent forms should be included in the training and notification of applicable law, reflecting knowledge of the applicable legal framework, a commitment to act to the outmost possible for respect of human life, dignity and integrity of the person and consent to act as FRs in MCIs despite possible individual liability for any harm. It should be noted, generally speaking, existing regulation and case law interpreting or applying regulation, takes into account the factual circumstances such as, the bona fide intent of the person intervening to save lives, the context of hardship in an MCI and other mitigating factors. The key concept is transparency in consent forms to potential liability wherever it may exist, reflected in a clear and reliable manner.

If random bystanders spontaneously intervene in MCIs they are subject to applicable national laws.

#### 3.3.1.3 Who is the leader?

In order to prevent confusion, in the absence of national, regional or local legislation (primary or secondary, including administrative regulation) centralising the plan of action in case of MCI between different FR agencies (e.g. firefighter, ambulances, police, national red cross societies, civilian volunteer agencies...), specifying command hierarchy on the ground different FR agencies should attempt to reach common understanding and best practices so as to optimise response in MCIs, closing gaps and preventing repetition of mandates, creating a comprehensive holistic First Response mechanism nationally.

Harmonized regulatory frameworks would also help avoid legal uncertainty and would create greater social confidence and transparency. This way, best practices and understanding will most likely add to achieving the objectives of integrating new technologies in MCIs for the use of FRs.

#### 3.3.1.4 'Expectant' Patient

An expectant patient is a patient with little chances of survival even after receiving medical treatment. The question of administering treatment or preventing over-treatment or leaving it to the choice of the patient or family in regular medical situations unfolds legal and societal complexities but is considered generally as part of the private prerogatives of an individual: the decision not to receive treatment. This is a different case scenario than euthanasia where a physician or other medical staff is asked to actively assist a patient to end life- a phenomena only very few jurisdictions openly accept as lawful and under very strict conditions, namely in Switzerland and in the Netherlands. The European Court of Human Rights has constantly explicitly ruled that the right to life does NOT include the right to (dignified) death or death by choice.

An MCI changes the landscape of the already complex legal situation existing in regular time around an expectant patient (in terms of having to prioritize between the treatment administered to patients). The main change is due to the lack of sufficient resources in a Mass Casualty Incident to treat all needs. Due to this fact, it may occur that a patient identified as 'expectant' in an MCI would have been identified as 'Red' if sufficient capacity was present on the scene. The MRMI exercise on decision-making in MCIs showed identifying expectant patients is a clear sign of the need to further communicate 'above' with regional coordinators for instance in view of calling in additional resources wherever possible. Nevertheless, even the most diligent FR most probably will encounter an expectant patient in an MCI. Some FRs do not have an official policy but do have practices indicating effectively that the specific patient has no chances of survival and is not destined to receive priority treatment.

As far as possible, FR agencies should issue clear guidance to their personnel (whether volunteer or not) as to several questions relevant to the expectant category and how are expectant patients to be identified and treated in a MCI. The legal questions include:

The legal questions at hand are:

1. Who has the legal power to declare an expectant patient? Knowing that in most jurisdictions the authority is restricted to physicians.

2. Is there a process where the use of 'expectant' patients category is authorized and by whom? Is the authorization to be revaluated? How often and by whom?

3. What are the criteria to declare a patient expectant? How often are they to be re-evaluated?

Facing the legal challenges that are merely emphasized in an MCI will allow clarity and transparency that may build trust in view of increasing societal acceptance of the extreme reality of an MCI. The chances for medical mistakes (or even malpractice) are arguably higher during emergencies, due to the inherent challenges. Physicians and other medical/non-medical personnel need protection from abusive lawsuits, while remaining loyal to their deontological oath. Most state laws protect first responders from most lawsuits nevertheless; clearer legal and ethical frameworks should be elaborated.

#### 3.3.1.5 Transparency in resource management

Efficiently responding to an MCI requires efficient and reliable resource management including knowledge about available transportation, information sharing between hospitals and if required an obligation to report to a central national authority. Resource management should be done prior to an MCI, be updated periodically (possibly even daily) and during an MCI through a Coordinator of the response to an MCI.

Unless there is an obligation to report on resource management, hospitals public and private, often in competition over resources might be reluctant to share such information. There is a need of national authority to intervene in view of remedying this reality and in view of bettering the chances of providing an optimal First Response in MCIs.

It is worth underlining that resource management is also relevant in terms of the rights of patients in need of emergency treatment unrelated to the MCI scene. Their rights are equal to those of MCI patients and must be taken into consideration.

### 3.3.2 Specific or novel legal issues arising at the crossroad between FR in MCIs and Advanced Technology

#### 3.3.2.1 Recruiting and training users

Extreme human situations such as MCIs require the participation of individuals of proven moral integrity and embracing of universal humanitarian values (right to life, human dignity, non-discrimination based on racial, ethnic, political, gender, national origin), clean criminal record, Clearance of personnel exposed to sensitive data. **Partners and participants are responsible for training their personnel (either staff or volunteers) to the highest professional standards but also to the highest moral standards in administering life saving care, TRIAGE or any other act in a MCI.**

**Partners are responsible for ensuring continuous training, monitoring and evaluating their personnel to the highest professional but also moral and legal standards: international human rights at the core, sanctity of life, human dignity, right to privacy and to family life, protection of**

**particularly vulnerable population: e.g. children in MCI, their identification and as far as possible tracking them for treatment in order to ensure adult supervision during or after the MCI;**

**Integrating new technology to First Response in MCIs requires user partners and organisations to** include appropriate training for their personnel, ensuring personnel are well-trained in using technology, complying with applicable regulations pertaining to each technology and providing special attention to the management of data (personal or sensitive data) when collecting, processing, storing or sharing data- restricting access to sensitive data to authorised personnel only. Special attention is equally required when using technology exposed to double-use, misuse (e.g. UAVs, facial recognition and other biometric collecting means or methods) and abiding to security configurations of the Security Management and complying with all national laws of the place of activity [where an action is made and the territory of which it has an effect]. In case of doubt or conflict of jurisdictions-training must include knowledge of both jurisdictions, while prioritizing the laws of the territory of effect. [for more information on conflict of laws see- international private law subsection below].

#### 3.3.2.2 International private law issue: Place of conduct or omission

Where does an act occur when it occurs digitally or 'on' the internet (social media, cloud, etc.)? Wherever partners acts (or omits to act) 'on' the internet, digitally and remotely, there may be a conflict of laws, however the preference should be given to the national laws of the place the act (or omission) has an effect in. While at times deciding where an act has an effect may be difficult, these are very limited cases. In case of conflict, the partners will turn to the Consortium Project Coordinator who will decide on the applicable protocols or regulations for the framework of the project. In general, seeing all partners are from EU countries except for Israel, the EU legal framework will apply, including in relation with data protection, and therefore the GDPR will apply. Israel legislation and practice is recognized as complying with the GDPR.

For the purposes of the project Nightingale partners will apply the territory of effect over territory of emission- without prejudice to the competent authorities' (national and international) prerogatives to hold individuals or corporations accountable (for e.g. in criminal events, acts relating to international terrorism, money-laundering or corruption).

**Required Action: Nevertheless, the Nightingale partners should specify in consent forms and other internal or external policies what jurisdiction is competent to resolve possible legal dispute relating to the use of advanced technology and actions or omissions occurring 'on' the internet.**

#### 3.3.2.3 Data collection, processing, storing and sharing

The most comprehensive legal framework for the processing of data is provided by the EU General Data Protection Regulation (GDPR). For detailed guidelines on data protection see also the Ethics Handbook.

At the heart of the GDPR and especially relevant to the Nightingale project is the concept of personal data and sensitive data.

Article 4 of the GDPR defines personal data as: *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'*

#### 3.3.2.4 Sensitive data: patient data

Under the GDPR, personal data is co considered 'sensitive' and is subject to specific processing conditions when it consists in:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- trade-union membership;
- genetic data, biometric data processed solely to identify a human being;
- health-related data;
- data concerning a person's sex life or sexual orientation.

In the Nightingale project context sensitive data is processed, namely biometric data processed solely to identify a human being and health-related data (e.g. patient data). Relevant technology includes any technology used biometric data, namely facial recognition, bracelets and earplugs and and AI based technology.

**Action required: Tech partners will identify the processing of sensitive data in all the 'life-chain' of the technology from design to use. Identifying and mapping sensitive data processing is the first necessary step needed in view of mitigating risks. User partners will be trained to use the proposed technology and process data in accordance with applicable national laws, the GDPR and the instructions of the tech partners (designers). Specific attention needs to be given to instances where sensitive data is processed special measures will be applied including anonimysation, pseudonimisation, restricted access etc. Anonimysation should of course be applied without running counter the objectives of the project, i.e. a patient must be identifiable to the medical staff from MCI scene to hospital (including). Partners will apply good judgement in the use of special protective measures, on the one hand to protect sensitive data from misuse and on the other hand to ensure the medical objectives on FRs in MCIs: saving lives, preserving human dignity and integrity of the person.**

#### 3.3.2.5 Data policy

Every partner will formulate a data policy in accordance with the GDPR. For further detail see the Ethics Handbook.

#### 3.3.2.6 Data sharing among Consortium partners

Sensitive data will not be shared outside the Consortium partners. If sensitive data sharing is needed, partners will turn to the Security Advisory Board (SBA) composed also by the Ethics Manager and the LSHM in view of receiving prior written consent after information the SBA of measures taken in view of compliance with the GDPR requirements for processing sensitive data.

International Data Sharing is any act of transferring or making Personal Data accessible outside the country where they were originally collected or processed, including both to a different entity within the same organisation or to a Third Party, via electronic means, the internet, or other means. Nevertheless, Data sharing between Consortium partners **within the EU** is not considered international data sharing.

‘cross-border processing’ means either:

+processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

+processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State. – EU Member States have committed to ensure cross-border data flows to facilitate trade in the digital economy among EU Member States and associated states (including Norway for e.g.). However, when doing so, they have also committed to apply required data protection measures.

For any data sharing outside the EU to Israel, adequacy decisions apply and so these are permitted.

**Each Nightingale partner will apply the required data protection and security measures aimed to protect personal and sensitive data to avoid ‘personal data breach’. Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;**

#### 3.3.2.7 Artificial Intelligence: EU proposal and decision-making on the basis of AI [See also Section 4.2 below]

Artificial Intelligence presents perhaps one of the most challenging fields to regulate. As the UN High Commissioner for Human Rights stated in a recent report, areas of digital power going unregulated present risks.

The difficulty to regulate is partly due to the fact subjects needing regulation (corporate entities specializing AI) have greater knowledge of AI than the regulators themselves and the area is rapidly developing. The regulation process is done through exchange between the legislators (in different national jurisdictions) and the subjects (AI corporate entities).

On the EU level, the EU Commission states that *'the European approach to artificial intelligence (AI) … focuses on 2 areas: excellence in AI and trustworthy AI. The European approach to AI will ensure that any AI improvements are based on rules that safeguard the functioning of markets and the public sector, and people’s safety and fundamental rights.*

*To help further define its vision for AI, the European Commission developed an AI strategy to go hand in hand with the European approach to AI. The AI strategy proposed measures to streamline research, as well as policy options for AI regulation, which fed into work on the AI package.*

© NIGHTINGALE Consortium, 2022. All rights reserved.

*The Commission published its AI package in April 2021, proposing new rules and actions to turn Europe into the global hub for trustworthy AI. This package consisted of:*

*+ a Communication on Fostering a European Approach to Artificial Intelligence;*

*+ the Coordinated Plan with Member States: 2021 update;*

*+ a proposal for an AI Regulation laying down harmonised rules for the EU (Artificial Intelligence Act)."*

While, the EU AI Act is still a proposal and not yet binding law, it is important to note the AI Act takes a risk-based approach. Certain risks for instance of inherent spying capacity are considered unacceptable. Therefore, a risk-based approached is the approach warranted within the NIGHTINGALE project by all partners and associate entities.

The use of AI in MCIs is overall accepted socially, although this field is still under researched.

**Required Action: Within the overall approach of the LSHM also to other risks, Nightingale partners and associated entities will apply a due diligence approach, assessing risks and mitigating them wherever necessary. Risk assessment is required throughout the 'lifespan' of the AI technology: from design to the user. Nightingale partners will apply the DDHR Risk Assessment (Annexe I) and communicate with the LSHM within the periodic review process on the risks and on measures taken to mitigate them.**

#### 3.3.2.8 Biometrics

Biometrics technologies are used to identify, verify, or confirm a person's identity based on their physiological (external appearance) or behavioural (how they act) characteristics. Physiological characteristics are assessed through morphological identifiers (mainly consisting of fingerprints, the hand's shape, the finger, vein pattern, the eye (iris and retina), and the face's shape) and biological analyses (DNA, blood, saliva, or urine). Behavioural characteristics are commonly assessed using voice recognition, signature dynamics (speed of movement of pen, accelerations, pressure exerted, inclination), gait (i.e. individual walking style) or gestures. Biometrics allows a person to be identified and authenticated based on verifiable unique and specific data.

Nightingale partners should be aware that biometric technology may be considered 'high risk' technology to which stringent security conditions apply. Furthermore, biometric data collected within Nightingale, either with FRs will be considered 'personal data'; and within an MCI is considered 'sensitive data'. Therefore, applying biometric technologies requires complying with respect for private life and protection of personal data through:

+ lawful, fair and *transparent* processing of data

+ processing of *data* for a specific, explicit and legitimate purpose

+ data *minimisation*, data accuracy, storage limitation, data security and accountability

[For further information see 4.2. below and the Nightingale Ethics Handbook]

Rules applicable to biometrics are also applicable to technology applied within the Nightingale project including (but are not limited to and this will be updated as the project evolves), facial recognition technology, triage bracelets and earplugs, augmented reality goggles/glasses and if applicable also to UAVs.

#### 3.3.2.8.1 Facial Recognition Technology (FRT)

As a recent EU Parliament study noted "While there are real benefits to using facial recognition systems for public safety and security, their pervasiveness and intrusiveness, as well as their susceptibility to error, give rise to a number of fundamental rights concerns with regard, for instance, to discrimination against certain segments of the population and violations of the right to data protection and privacy. To address such effects, the EU has already put strict rules in place under the Charter of Fundamental Rights, the General Data Protection Regulation, the Law Enforcement Directive and the EU framework on non-discrimination, which also apply to FRT-related processes and activities." [See above guidelines on 'Classic legal issues'].

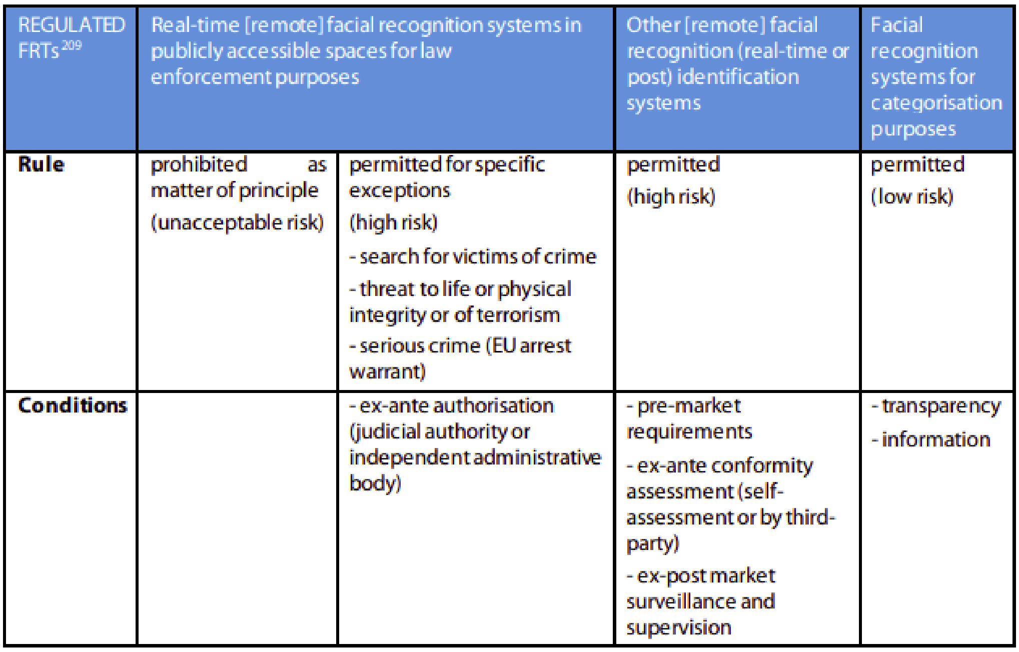
Special attention must be given by the developers of FRT to existing technology bias and disturbing statistics on discrimination against, for e.g. women of colour as opposed to white men, in the accuracy of FRT [35% of error in identifying women of colour v 1% error in recognising white men- according to some studies on US statistics using facial data of over 1 million individuals- see statistics in 'References' below].

Nevertheless, several actors question the effectiveness of the existing EU framework. In April 2021, the EU Commission and EU Parliament unveiled the draft EU artificial intelligence (AI) act, which, aims to limit the use of biometric identification systems including facial recognition that could lead to ubiquitous surveillance. In addition to the existing applicable legislation (e.g. data protection and non-discrimination), the draft AI act proposes to introduce new rules governing the use of FRTs in the EU and to differentiate them according to their 'high-risk' or 'low-risk' usage characteristics. A large number of FRTs would be considered 'high risk' systems which would be prohibited or need to comply with strict requirements. As a rule, the use of real-time facial recognition systems in publicly accessible spaces for the purpose of law enforcement would be prohibited, unless Member States choose to authorise them for important public security reasons, and the appropriate judicial or administrative authorisations are granted.

The classification proposed by the draft EU AI ACT between 'high-risk' and 'low-risk' is disputed. However, in all cases, facial recognition (and biometrics technology) to be used within Nightingale project would fall under 'permitted high-risk' technology. This is because, the use of biometrics and facial recognition would fall under the exceptions to the prohibition of use of real-time facial recognition in law enforcement, needing prior judicial authorisation or entirely prohibited. This is because the use of FRT in MCIs falls under the exception of urgency, saving human life, reacting to terrorist attack, identifying children and victims (and protecting them from paedophiles or other immediate harm).

Permitted high risk technology has to abide by the most stringent requirements in relation with data protection, protection from double-use or misuse, detailed throughout this Handbook. The table below, taken from an EU Parliament Study on the integration of FRT within the EU legal framework, provides further guideline:

*Table 1. Proposed AI regulation: scenarios for facial recognition system regulation*



| REGULATED FRTs[209] | Real-time [remote] facial recognition systems in publicly accessible spaces for law enforcement purposes | | Other [remote] facial recognition (real-time or post) identification systems | Facial recognition systems for categorisation purposes |
|---|---|---|---|---|
| **Rule** | prohibited as matter of principle<br>(unacceptable risk) | permitted for specific exceptions<br>(high risk)<br>- search for victims of crime<br>- threat to life or physical integrity or of terrorism<br>- serious crime (EU arrest warrant) | permitted<br>(high risk) | permitted<br>(low risk) |
| **Conditions** | | - ex-ante authorisation (judicial authority or independent administrative body) | - pre-market requirements<br>- ex-ante conformity assessment (self-assessment or by third-party)<br>- ex-post market surveillance and supervision | - transparency<br>- information |

## 3.3.2.8.2 Triage bracelets and earplug device

Triage bracelets and earplug devices integrate advanced technology and data depending on an on-going process within the Nightingale project. In other words, bracelets may apply AI, tracking, sensorial, sensitive data and other. Depending on the choice of technology and data processing, the relevant sections in the LSHH apply.

Also noteworthy is the possibility of 'communication' between the triage bracelets and/or earplug devices and other technologies (e.g., drones-UAVs, augmented reality glasses, etc.). Precautions need to be applied in the design of the technology and communication ability between devices so as to mitigate risks of misuse and double-use.

## 3.3.2.9 Tracking software incoming information; PSAP situational awareness- location

Software tracking and tracing using other technology even for the purposes of localising an MCI or resource management is considered to amount to sensitive processing activity. National legislation may regulate tracking software, including in connection with Public Safety Answering Points (PSAPs).

**Nightingale partners and associated entities should apply the most stringent measures to protect data and security and prevent misuse.**

## 3.3.2.10 Drones – UAVs

The use of drones is also considered sensitive processing in terms of data protection and avoiding double-use (civil to military) or misuse by ill- intentioned third parties.

Nightingale partners and associated entities should realize that, even when identification of individuals is not possible via the use of Drones, their use may still have substantial implications for the life, liberty and dignity of individuals and communities. Nightingale partners and associated entities should accordingly take precautions to protect Drone-collected data, even if the individuals recorded in them are not immediately identifiable.

For example, if the data from tracking streams of displaced people with Drones are accessed by ill-intentioned Third Parties, vulnerable individuals can be put at risk, even if they cannot be individually identified.

Current challenges to expanding their use in emergency medicine and emergency medical system (EMS) include regulation, safety, flying conditions, concerns about privacy, consent, and confidentiality, and details surrounding the development, operation, and maintenance of a medical drone network.

Flying drones can also cause danger during an MCI as accidents can happen causing bodily injuries, especially when used in urban settings. Taking into account the extreme conditions of an MCI and short time span for response, all flying certificates should be regulated prior to an MCI.

**Nightingale partners designing technology and using drones should recognise risks and act to mitigate them and take an active part in the periodic review.**

### 3.3.3 Dual-use

Dual-use consists in products, services or knowledge that can serve both for civil and military services. The Nightingale project has civilian and humanitarian objectives based on universal values of human dignity, the right to life and the right to integrity of the person.

Nightingale partners will act while respecting their national laws in relation to dual-use products, services and knowledge, namely in the use of drones, tracking and tracing technology, biometric and facial recognition, and other technology that may also be used for spying or illegitimate purposes.

Specific caution should be applied when processing sensitive data as defined in the GDPR (medical or patient information), including among other the transfer of this information between actors (from MCI scene or field to hospital) and between technologies integrated in the toolkit (e.g. bracelet 'communicating' with drones, augmented reality glasses etc.)

What technology will allow processing what data is still work in progress at the time of drafting of the LSHH and periodic monitoring will allow identifying risks and mitigating them.

For complementary information please see also the Ethics Handbook

### 3.3.4 Misuse

Misuse is use other than for the aims described in the Nightingale project GA that can pose threats and dangers to fundamental rights and liberties.

Misuse of data and advanced technology could affect the right to privacy, freedom of expression, freedom of association, electoral freedom and discrimination.

Certain technologies and knowledge or data if were to fall into the wrong hands, namely of non-state actors (terrorists or organized crime groups) could pose danger to life, national security and public health. These technologies, knowledge and data, if were to fall into the hands also of state actors but who are exercising repressive regimes could pose extensive danger to minorities and vulnerable groups, fundamental rights and freedoms.

Cyber Security Breach and Cyber Attacks (Warfare) are also possible dangers. A cyber-attack is defined in the guidelines developed in the 'Tallinn Manual' as relating to an attack in armed conflict which is assessed by its result, as opposed to the means used. A cyber-attack might not use military or kinetic force, but its effects might be loss of military and civilian life. Currently, certain countries are employing the means of cyberattacks against military adversaries, including in the Russian-Ukraine context. The importance of securing and protecting sensitive and personal data, as well as applying highest measures of caution also to specific technology (e.g., drones, biometric data processing) is if high importance.

Specific caution should be applied when processing sensitive data as defined in the GDPR (medical or patient information), including among other the transfer of this information between actors (from MCI scene or field to hospital) and between technologies integrated in the toolkit (e.g., bracelet 'communicating' with drones, augmented reality glasses etc.)

What technology will allow processing what data is still work in progress at the time of drafting of the LSHH and periodic monitoring will allow identifying risks and mitigating them.

**The risks posed by the relevant technology within the Nightingale project are not unacceptable risks, however Nightingale partners and associated entities must ensure data protection and general security at all times. For further guidelines see the Ethics Handbook on Misuse.**

# 4 Societal and Humanitarian considerations

Societal and humanitarian considerations must be taken into account in view of optimising chances of success for the Nightingale project and the potential integration rates of the Nightingale toolkit.

## 4.1 First Response in MCIs operates in humanitarian contexts:

providing impartial life-saving treatment to all without taking into account ethnic, racial, gender, religious, national, political origin. Response is provided solely on the basis of the medical needs of the patient and the available resources at the best discretion of the FR on the MCI scene, following training and applicable protocols.

Humanitarian contexts exist in peacetime, emergencies and in armed conflict. Humanitarian considerations such as humanitarian access, immunity of medical staff (MDA, ICRC, National Red Cross) to treat the wounded are accepted by belligerents even in the most extreme situations, at least in the vast majority of cases and are binding by law. Principles for the protection of civilians in armed conflict may also apply.

Taking into consideration the nature of a MCI where individuals (casualties) most often cannot provide consent to the use of their private data, several UN resolutions and guidelines in humanitarian (disaster) contexts include a humanitarian clause calling for particular care and flexibility when applying data protection principles in the humanitarian sector. In other words, seeing the overall objective in collecting data in a humanitarian context, there is flexibility in the ability to collect data (including sensitive data such as patient data) allowing saving lives. Nevertheless, the personnel collecting the data has to exercise extra care when doing so in view of the individual's inability to provide consent and in view of the sensitive nature of data processed (collected etc.- see definitions in supra). These considerations are in line with the due diligence approach adopted in this Handbook.

## 4.2 Societal considerations:

Integrating advanced technology to MCIs within the NIGHTINGALE project framework will enhance the capacity and efficiency of FR. The Nightingale project has the unique feature of combining both tech partners and users (FRs) along with other experts and advisors.

Notwithstanding this fact, the project partners should take into account societal considerations that if not addressed may hinder success and integrating rates of the Nightingale toolkit, limit the freedom of action of partners and wrongly influence political decision-makers. Public consensus and democratisation of the process is of importance. Outreach programs presenting the project, its objectives, methodology, process and outcomes should be made as ensured by the communication partners of the Nightingale Consortium and as described in the GA.

Concerns about advanced technology exist. Regardless of whether these concerns are well-based, trust-building is necessary between different social actors, beginning with tech partners and user partners but also with broader society and communities. Similar to any other modern development affecting society, education is needed in view of ensuring a better understanding of technologies, their objectives, design and use in life-saving situations such as MCIs and Disasters.

Case studies involving advanced technology and their misuse are not difficult to find. A few examples are set out below for illustration purposes:[5]

+ The 'Cambridge Analytica' scandal where facebook data was compromised possibly affecting elections during *the* Brexit referendum and the Trump elections in the US;

+ Pegasus and *NSO* scandal where spy software was used to spy on political opponents (allegedly);

+ double-use of drones and the 'bad reputation' of drones e.g. in 'targeted killings'- noteworthy: despite the *fact* in regular law enforcement paradigm this is clear violation of human rights (extrajudicial killings); in armed conflict, the use of drones may be the least harmful means preventing further loss of life and destruction with a land war and armored tanks as the alternative- therefore being the more lawful means to apply.

+ cases of facial recognition technology in the hands of repressive regimes: the example of China and the genocide *of* the Uhygur minority (genocide recognised by several countries).

+ Covid19 context where tracking and tracing technology was used to track individuals who were required to be in isolation or quarantine and high number of mistakes in the technology, unnecessarily limiting freedom to circulate.

Despite these challenges, all of the case studies relate either to the misuse of technology or to mistakes in the algorithms and unintended effects limiting fundamental rights.

MCIs present a context to which there is general public consensus of the need to act swiftly and efficiently in order to save lives, preserve human dignity and integrity of the person. The application (including training and disseminating among FRs staff and volunteers) of each FR's deontology rules, codes of conduct and protocols should arguably allow to ensure avoiding misuse or double use and ensuring the use of integrated advanced technology only for the purposes of saving lives, preserving human dignity and individual integrity.

One research on the societal acceptance of using drones in MCIs concluded: "Research to date suggests that use of drones in emergency medicine is feasible, will be accepted by the public, is cost-effective, and has broad application." Nevertheless, the field requires further research in order to reach conclusive results.

Nightingale partners and associated entities are cognisant of the humanitarian context and the societal considerations and commit to act in due diligence as described above in the Handbook and by abiding by the checklist provided by Annex I Human Rights Due Diligence.

[5] For a very recent study examining case studies of untrustworthy Artificial Intelligence, systematic biases and discrimination and novel systematic issues affecting human rights, see The Law Commission of Ontario Report, "Accountable AI", released 17 June 2022, available at: https://www.lco-cdo.org/wp-content/uploads/2022/06/LCO-Accountable_AI_Final_Report.pdf

# 5 Mitigating risks

The Nightingale partners and any associated entities, including volunteers will apply a due diligence approach based on 'obligation of means', whereby partners will assess risk, act to mitigate them and in case of need seek advise on how to mitigate risks and report to the SAB, namely the LHSM on compliance.

In terms of the question 'who is responsible man or machine' different jurisdictions apply different standards and each partner shall be aware of the national legal obligations he/she must comply with. Generally speaking, when applying AI technology, the responsibility is joint, and each actor is liable to the extent of his/her responsibility. In other words, the designer is liable for flaws in design, the user is liable for using technology without following the manufacturer's instructions. Neither entity can replace the other. In other words, the FR on the MCI scene has at all times the discretion of how to implement the relevant protocol depending on the circumstances on the ground and in good faith. All in all, the standard is of the 'reasonable' FR, similar to the acts of the 'reasonable' individual before civil law courts or the 'reasonable' military commander under the laws of armed conflict: no clear definitions apply, however, as long as the intent, acts and omissions were in view of complying with the humanitarian objectives of first response in an MCI or disaster, complied with duties and obligations than the actor is free from wrongful acts and liability. In this regard, the due diligence framework proposed, applying both binding legal standards and 'soft law' best practices and guidelines, provides optimal (although not perfect) protection from abuse. This in turn will arguably offer optimal legal certainty to the FR in MCIs as well as to the tech partners designing the technology and their DPOs monitoring use.

Reflecting on information in the Handbook, partners and associated entities should act diligently before, during and after an MCI (see Section 1) and namely in:

## 5.1 Early preparedness and monitoring of the legal and ethical obligations

The process of early preparedness and monitoring of the legal and ethical obligations is based on a collaborative approach and on working closely with the partnership. This methodology focuses on an early warning system in order to identify problems as early as possible, minimize the impact they can produce and recommend appropriate solutions. The monitoring activity is carried out through various channels:

a) a questionnaire to be filled out for Partners which helps to identify potential problems, useful tool for activating the first alarms;

b) review of the deliverables considered most critical.

In the specific field of AI, the document "Ethics By Design and Ethics of Use Approaches for Artificial Intelligence"[6] specifies that there are six general ethical principles[7] that any AI system must preserve and protect based on fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (EU Charter), and in relevant international human rights law:

1. **Respect for Human Agency**: human beings must be respected to make their own decisions and carry out their own actions. Respect for human agency encapsulates three more specific principles, which define fundamental human rights: autonomy, dignity and freedom.

2. **Privacy and Data governance**: people have the right to privacy and data protection, and these should be respected at all times;

3. **Fairness**: people should be given equal rights and opportunities and should not be advantaged or disadvantaged undeservedly;

4. **Individual, Social and Environmental Well-being**: AI systems should contribute to, and not harm, individual, social and environmental wellbeing;

5. **Transparency**: the purpose, inputs and operations of AI programs should be knowable and understandable to its stakeholders as far as possible- cognisant that in this field there exist limitations.

6. **Accountability and Oversight:** humans should be able to understand, supervise and control the design and operation of AI based systems, and the actors involved in their development or operation should take responsibility for the way that these applications function and for the resulting consequences.

To incorporate these six ethical principles into their design, proposed AI systems should comply with the general ethical requirements listed above.

The aim of Ethics by Design is to make people think about and address potential ethics concerns, while they are developing a system. An assessment of the potential ethics risks must be made in the very early development phases of design of a product and solutions must be foreseen and discussed with developers and ethics experts. The implementation can be represented by the proactive transposition of identified ethics principles in the system requirements. Different methods, or protocols we might say, have been studied in the past years where there has been a growing sensitivity for ethics by design. In the document *Ethics By Design and Ethics of Use Approaches for Artificial Intelligence* authors Brandt DAINOW and Philip BREY suggest a scheme made up by

[6] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf

[7] The ethical principles described in this document are informed by the work of the Independent High-Level Expert Group on AI (AI-HLEG) set up by the European Commission. They are also based on value frameworks proposed by the European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems, 2018, the Institute of Electrical and Electronics Engineers (IEEE), the Organisation for Economic Co-operation and Development (OECD) and UNESCO.

phases: 1) assessment of ethics principles, 2) transposition of principles in ethics requirements, 3) ethics by design guidelines to provide a roadmap for the process, 4) matching requirements into the different methodological steps and sequences, 5) tools and methods within the development process to assess the ethics by design concept.

The ethics by design represents an additional economic value: any issue, as a general rule, is much less costly if foreseen and fixed before it becomes an issue. It also represents an added value because of the growing sensitivity of the user communities towards ethics and fairness.

## 5.2 Outreach in view of mitigating societal challenges and building trust: engage with civil society, communication

Alongside the societal concerns described above (section 4.2.) in view of based or unbased concerns regarding risks when integrating advanced technology to first response in MCIs and disasters, there exists the need to build trust.

Building trust can only be done through theoretical informative and reliable education alongside constructive experience.

Outreach programs presenting the project, its objectives, methodology, process and outcomes are included in the overall objectives of the Nightingale project, ensured mainly by the communication partners of the Nightingale Consortium (see the GA) and by the Consortium partners.

Trust-building can be done by information (words) followed by acts: in other words, compliance with human rights due diligence standards, ethics by design, training for good use, do no harm, abiding by humanitarian concerns will increase societal acceptance needed for the chances of success rates for the integration and future of the Nightingale toolkit.

Concerns about advanced technology exist. Regardless of whether these concerns are well-based, trust-building is necessary between different social actors, beginning with tech partners and user partners but also with broader society and communities. Similar to any other modern development affecting society, education is needed in view of ensuring a better understanding of technologies, their objectives, design and use in life-saving situations such as MCIs and Disasters.

Education should be interactive, reach younger and older audiences, focus on target audiences as well as broader public. It should combine in-person training, remote and digital education and ensure presence in social media, and be accompanied by recognized symbols (logos of partners, consortium and EU) so as to avoid misinformation and ensure constructive, reliable and engaging information. The Consortium will use its own resources and partners will equally use their respective sources to engage with their respective audiences, under the guidance of communication partners.

Wherever possible, outreach programs exceeding the lifespan of the Nightingale project will be envisaged in view of creating a sustainable environment for the Nightingale toolkit.

## 5.3 Be loyal to humanitarian principles in MCIs

As expressed in section 4.1. above and throughout the Handbook, the mission of FRs in MCIs and Disasters is first and foremost of a humanitarian nature. Technical partners engaged with the Nightingale project committed to the humanitarian objectives of FRs in view of enhancing their ability in MCIs and Disasters by integrating advanced technology.

Therefore, in all intent, actions and omissions partners, and any associated entities (UAB, volunteers, etc.) are equally committed to loyalty to the over-riding humanitarian principles in MCIs and Disasters, namely: preserving, respecting and protecting human life, human dignity and the mental and bodily integrity of the individual. All relevant actors are loyal to the do no harm principle when engaging with the Nightingale project.

As mentioned in the societal concerns and needed outreach programs, complying with humanitarian principles will help ensure societal acceptance needed for the success of acceptance rates of the Nightingale toolkit.

© NIGHTINGALE Consortium, 2022. All rights reserved.

# 6 Conclusions

The Legal, Societal and Humanitarian Handbook provides the landscape of first response in MCIs and Disasters. It addresses a few inherent challenges as well as underlines specific legal, societal and humanitarian concerns relating to integrating advanced technology into first response in MCIs.

Additionally, the LSHH provides a general 'means responsibility' approach translated into a Human Rights Due Diligence risk-based legal framework allowing actors (users and tech) to be cognisant of risks, legal obligations, and to be able to address them in advance in design, preparedness and use.

The LSHH aimed to make accessible the binding obligations on all partners but also the advisable and appropriate measures to ensure the Nightingale toolkit not only is lawful but is also appropriate and cognisant of societal concerns, risks of misuse and double-use and compliant with over-riding humanitarian concerns at the crux of this project.

The LSHH will be followed by periodic reports whereby partners make transparent their process and outcomes in view of legal, societal and humanitarian aspects of the project.

Annex I: Human Rights Due Diligence is a tool intended to assist partners in their task. The LSHM is readily available for any further information.

# References[8]

INTERNATIONAL TREATIES, RESOLUTIONS, GUIDELINES (UN Bodies)

[1] UN General Assembly Resolution 45/95 of 14 December 1990, A/RES/45/95 14 December 1990, http://www.un.org/documents/ga/res/45/a45r095.htm

[2] UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990, http://www.refworld.org/docid/3ddcafaac.html

[3] UN General Assembly Resolution 45/95 of 14 December 1995 adopting the Guidelines for the Regulation of Computerized Personal Data Files

[4] the International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution) adopted by the ICDPPC in Madrid in 2009

[5] UN 2012 Guiding Principles for Business and Human Rights

[6] 1996 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies

[7] International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, Amsterdam, Netherlands 2015, https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf

[8] WHO, Code of Conduct for Responsible Research 2021, https://www.who.int/docs/default-source/documents/ethics/code-of-conduct-for-responsible-research-pamphlet-en.pdf?sfvrsn=93f07bc9_2

[9] International Conference on Data Protection and Privacy Commissioners, International Standards on the Protection of Personal Data and Privacy, https://icdppc.org/wp-content/uploads/2015/02/The-MadridResolution.pdf

[10] Resolution on Data Protection and Major Natural Disasters adopted by the ICDPPC in Mexico City in 2011

[11] Resolution on Privacy and International Humanitarian Action adopted by the ICDPPC in Amsterdam in 2015

[12] The UNHCR Policy on the Protection of Personal Data of Persons of Concern to UNHCR (2015)

[13] The IOM Data Protection Manual (2010)

EUROPEAN, EU and OECD LAW (DIRECTIVES, REGULATIONS and GUIDELINES)

[14] The OECD Privacy Framework (2013), https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

[15] OECD, Artificial Intelligence in Society, 2019, https://doi.org/10.1787/eedfee77-en

[16] the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), including the Additional Protocol

[17] EU General Data Protection Regulation 2016/679 (GDPR)

[8] References are divided by the nature of their source e.g, International Treaties and Guidelines; EU LAW; Scholarship, etc.

[18] EU Recommendation 02/2020 on Essential Guarantees in Surveillance, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en

[19] The European Code of Conduct for Research Integrity, 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/european-code-of-conduct-for-research-integrity_horizon_en.pdf

[20] EUI, President Decision No. 10/2019 of 18 February 2019: Regarding Data Protection at the European University Institute, https://www.eui.eu/Documents/AboutEUI/Organization/DataProtection/PresDecision10-2019-DataProtection.pdf

[21] EU Grants: Potential misuse of research: V2.0 – 14.09.2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-potential-misuse-of-research-results_he_en.pdf

[22] European Commission, Proposal for a Regulation on a European approach for Artificial Intelligence, 2021/0106 (COD), See in particular: recital 27, 2021/0106 (COD), https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence

[23] European Parliament, Legislative Train, Artificial Intelligence Act, https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence

[24] EU Dual Use Research Guidance - Draft, 2021, https://trade.ec.europa.eu/consultations/documents/consul_183.pdf

[25] European Commission, Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, 2021, https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation

EUROPEAN COURT OF JUSTICE CASE LAW

[26] ECJ, ' Schrems I ' Judgement 2015, https://eur-lex.europa.eu/legal - content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=en

[27] ECJ, ' Schrems II ' Judgement 2020, https://eur-lex.europa.eu/legal - content/EN/TXT/?uri=CELEX%3A62018CJ0311

HANDBOOKS

[28] Marelli and Kuner , Handbook on Data Protection in Humanitarian Action, 2017, https://rm.coe.int/handbook-data-protection-and-humanitarian-action-low/168076662a

[29] Inter Agency Standing Committee (IASC) of the Operational Policy and Advocacy Group (OPAG), Operational Guidance: Data Responsibility in Humanitarian Action, 2021, https://interagencystandingcommittee.org/resources?og_group_ref_target_id=19568&sort_by=field_published_date_value&sort_order=DESC&og_subspaces_view_all=1&og_subspaces_view_parent=0&f%5B0%5D=resource_audience_label%3AOperational%20Response&f%5B1%5D=resources_authored_on%3A1995-05&f%5B2%5D=resources_authored_on%3A2000-09&f%5B3%5D=resources_authored_on%3A2008-10&f%5B4%5D=resources_authored_on%3A2011-09&f%5B5%5D=resources_authored_on%3A2013-07&f%5B6%5D=resources_authored_on%3A2015-03&f%5B7%5D=resources_authored_on%3A2016-06&f%5B8%5D=resources_authored_on%3A2020-10&f%5B9%5D=resources_authored_on%3A2021-02&s=

© NIGHTINGALE Consortium, 2022. All rights reserved.

[30] UN Office for the Coordination of Humanitarian Affairs (OCHA), Building data responsibility into humanitarian action, 2016, https://datacollaboratives.org/static/files/framework.pdf

[31] DSEG, A Framework for the ethical use of advanced data science methods, 2018, https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/dseg_ethical_framework_april_2020.pdf

[32] WHO, A Guidance Document For Medical Teams Responding To Health Emergencies In Armed Conflicts And Other Insecure Environments, 2021, https://apps.who.int/iris/bitstream/handle/10665/341858/9789240029354-eng.pdf?sequence=1

[33] OCHA, Guidance Note Series, Data Responsibility in Humanitarian Action, Note 4: Humanitarian Data Ethics,2020, https://reliefweb.int/sites/reliefweb.int/files/resources/guidance_note_ethics.pdf

[34] Sydney University, Research Code of Conduct 2013, https://www.sydney.edu.au/dam/corporate/documents/news-opinions/research_code_of_conduct_2013.pdf

[35] A Framework for the Ethical Use of Advanced Data Science Methods in the Humanitarian Sector, 2020, https://www.hum-dseg.org/dseg-ethical-framework

ICRC

[36] The ICRC Rules on Personal Data Protection (2015)

[37] the ICRC Professional Standards for Protection Work (2013)

[38] ICRC Humanitarian Charter and Minimum Standards in Disaster Response 2004, https://www.refworld.org/pdfid/3d64ad7b1.pdf,https://www.icrc.org/en/doc/resources/documents/misc/64zahh.htm

ONTARIO LAW COMMISSION

[39] The Law Commission of Ontario Report, "Accountable AI", released 17 June 2022, https://www.lco-cdo.org/wp-content/uploads/2022/06/LCO-Accountable_AI_Final_Report.pdf

SCHOLARSHIP- ACADEMIC PUBLICATIONS, ARTICLES, BLOGS, BOOK CHAPTERS

[40] Sarah Soliman, Tracking Refugees With Biometrics: More Questions Than Answers, War on the Rocks Blog, 9 March 2016, https://warontherocks.com/2016/03/tracking-refugees-with-biometrics-more-questionsthan-answers/

[41] Ethical Guidance for Disaster Response, Specifically Around Crisis Standard of Care: a systematic review. Am J. of Public Health. Leider J.P., De Bruin et al 2017; 107(9)

[42] Johnson AM, Cunningham CJ, Arnold E, Rosamond WD, Zègre-Hemsey JK. Impact of Using Drones in Emergency Medicine: What Does the Future Hold? Open Access Emerg Med. 2021;13:487-498, https://doi.org/10.2147/OAEM.S247020

[43] Cliem, N. and McKenzie, A-M., Digital Dignity in Practice: Existing digital dignity standards, pursuing digital dignity and current gaps in digital dignity, 2019, https://www.alnap.org/help-library/digital-dignity-in-practice-existing-digital-dignity-standards-pursuing-digital-dignity

[44] Repine, The Dynamics and Ethics of Triage: Rationing Care in Hard Times, 2005, https://mercyhighered.org/wp-content/uploads/2020/04/Dynamics-and-Ethics-of-Triage-Rationing-Care-in-Hard-Times.pdf

© NIGHTINGALE Consortium, 2022. All rights reserved.

[45] 'Chatham House Rules', UK Royal Institute of International Affairs, June 1927, Chatham House official website: https://www.chathamhouse.org/about-us/chatham-house-rule?gclid=Cj0KCQjwrs2XBhDjARIsAHVymmTWZ5V4CGbjTE4NBEWJpmmfChOH4JU-7BoBl5qA5ZWeVJHbw-66GsaAjKiEALw_wcB

[46] Koskimies et al, The informational privacy of patients in prehospital emergency care—Integrative literature review, 2020, https://onlinelibrary.wiley.com/doi/abs/10.1111/jocn.15481

[47] White, Lo, A Framework for Rationing Ventilators and Critical Care Beds During the COVID-19 Pandemic, 2020, https://jamanetwork.com/journals/jama/article-abstract/2763953

[48] Albahri et al, Systematic Review of Real-time Remote Health Monitoring System in Triage and Priority-Based Sensor Technology: Taxonomy, Open Challenges, Motivation and Recommendations, 2018, https://link.springer.com/article/10.1007/s10916-018-0943-4

[49] Stewart, Dwivedi, Artificial intelligence and machine learning in emergency medicine, 2018, https://onlinelibrary.wiley.com/doi/abs/10.1111/1742-6723.13145

[50] De Stefani, Using social media in natural disaster management: a human-rights based approach, 2017, http://phrg.padovauniversitypress.it/2017/2/3

[51] Burkle, Advanced Triage Management for Emergency Medical Teams, 2019, https://www.researchgate.net/profile/Frederick-Burkle/publication/338489109_Advanced_Triage_Management_for_Emergency_Medical_Teams/links/5e1b71e392851c8364c8d5e8/Advanced-Triage-Management-for-Emergency-Medical-Teams.pdf

[52] Winn et al, Medical Volunteers during Pandemics, Disasters, and Other Emergencies: Management Best Practices, 2021, https://heinonline.org/HOL/LandingPage?handle=hein.journals/sjel11&div=13&id=&page=

[53] Jaskula, Siuta, Simple Emergency Triage (SET) the new perspective on mass casualty incident triage, 2020, https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/263940/jaskula_siuta_simple_emergency_triage_set_2020.odt?sequence=2&isAllowed=y

[54] Nielsen, Utilitarian Triage in Disasters, 2021, https://heinonline.org/HOL/LandingPage?handle=hein.journals/byulr46&div=8&id=&page=

[55] Hodge et al, Volunteer health professionals and emergencies: assessing and transforming the legal environment, 2005, https://pubmed.ncbi.nlm.nih.gov/16181044/

[56] Perate et al, The Use of Simulation in Disaster Medicine Preparedness, 2020,https://www.semanticscholar.org/paper/The-Use-of-Simulation-in-Disaster-Medicine-Perate-Rodgers/762735daa8bce9b431c624f97414dcc59afe98ff

[57] Alvares-Garcia et al, development of the Aerial Remote Triage System using drones in mass casualty scenarios: A survey of international experts, 2020, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0242947

[58] Montano et al, ‘Mobile Triage Applications: A Systematic Review in Literature and Play Store,2021, https://link.springer.com/article/10.1007/s10916-021-01763-2

[59] Johnson et al, Impact of Using Drones in Emergency Medicine: What Does the Future Hold, 2021, https://www.dovepress.com/impact-of-using-drones-in-emergency-medicine-what-does-the-future-hold-peer-reviewed-fulltext-article-OAEM

[60] Merchant et al, Integrating social media into emergency-preparedness efforts, 2011, https://www.nejm.org/doi/full/10.1056/nejmp1103591

[61] Jayshree Pandya, The Dual-Use Dilemma of Artificial Intelligence, Forbes, 2019

[62] Hodge et al, The Pandemic and All-Hazards Preparedness Act, 2007, https://www.researchgate.net/publication/6388781_The_Pandemic_and_All-Hazards_Preparedness_Act_Improving_Public_Health_Emergency_Response

[63] Ebben et al, Adherence to guidelines and protocols in the prehospital and emergency care setting: a systematic review, 2013, https://pubmed.ncbi.nlm.nih.gov/23422062/

[64] Abelsson et al, Learning by Simulation in Pre-hospital Emergency Care, 2016, https://pubmed.ncbi.nlm.nih.gov/26333061/

[65] Nimmorlrat et al, Patient triage system for supporting the operation of dispatch centres and rescue teams, 2021, https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-021-01440-x

[66] Zhang et al, Evaluative research of technologies for prehospital communication and coordination, 2020, https://pubmed.ncbi.nlm.nih.gov/32246206/

[67] Zoltowska et al, Preparedness of Health Care Workers and Medical Students in University Hospital in Krakow for Covid-19 Pandemic within the CRACoV Project, 2021, https://www.mdpi.com/2077-0383/10/16/3487

[68] Hempel et al, Allocation of Scarce Resources in a Pandemic, 2021, https://pubmed.ncbi.nlm.nih.gov/34048911/

[69] Emerging Technologies in Emergency Situations, 2021, https://www.researchgate.net/publication/353738439_Emerging_Technologies_in_Emergency_Situations_Guest_Editorial

[70] Afzali et al, The impact of the emergency medical services automation system on patient care process and user workflow, 2021, https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-021-01658-9

[71] Blank and Jensen, LOAC and the Protection and Use of Digital Property in Armed Conflict, 2021

[72] Cahane, The Right not to Forget: Cloud Based Services Moratoriums in War Zones and Data Portability Rights, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3944667

[73] Cliem, N. and McKenzie, A-M., Digital Dignity in Practice: Existing digital dignity standards, pursuing digital dignity and current gaps in digital dignity, 2019, https://www.alnap.org/help-library/digital-dignity-in-practice-existing-digital-dignity-standards-pursuing-digital-dignity

[74] Cochrane, Data Subject Access Rights and Military Agencies: A Comparative Perspective, 2020, https://csrcl.huji.ac.il/blog/protecting-privacy-and-data-protection-times-armed-conflict

[75] Crawford, The Right to Privacy and the Protection of Data in Situations of Detention in Armed Conflict', 2020

[76] Davenport, The use of Camble Infrastructure for the Interception and Collection of Data During Armed Conflict: Are There Any Limits?, 2021

[77] Hellwig, Investigation of Grave International Crimes', 2021

[78] Housen-Curiel, Managing Data Privacy Rights in Multilateral Coalition Operations' Information Sharing Platforms: Towards a "by Design and by Default" Model, 2021

[79] Oconnell, Data Privacy Rights: The Same in War and Peace', 2021

[80] Rejali, Saman and Heiniger, Yannick, The Role of Digital Technologies in Humanitarian Law, Policy and Action: Chartering a Path Forward, 2021, https://international-review.icrc.org/articles/digital-technologies-humanitarian-law-policy-action-913

[81] Ronen, The Right to be Forgotten and International Crimes, 2021,

[82] Shany and Mimran, Integrating Privacy Concerns in the Development and Introduction of New Military or Dual Use Technologies, 2021, https://openscholar.huji.ac.il/csrcl/event/yuval-shany-tal-mimran-article-36-ap1-vehicle-integrating-privacy-concerns-development

[83] Shehabi, Digital Privacy Rights, Data Protection and the Law of Occupation, 2021

[84] Van De Velde, From Telegraphs to Terabytes: The Implications of the Law of Neutrality for Data Protection by "Third" States and the Corporations Within Them, 2021

[85] Watt, NATO CCDCOE 'Rights to Privacy and Data Protection in Armed Conflict' Research Project, 2021, https://ccdcoe.org/research/data-protection-and-privacy-in-armed-conflict/

[86] West, Facial Recognition Technology use in Armed Conflict: A Case Study of the Relationship between Privacy and Precaution, 2021

[87] Dorothy Leonard-Barton, William A. Fraus, Implementing New Technology, Harvard Business Review, https://hbr.org/1985/11/implementing-new-technology

[88] Katam Raju Gangarapu, Ethics of Facial Recognition: Key Issues and Solutions, January 25, 2022 (blog guest post), https://learn.g2.com/ethics-of-facial-recognition

[89] I. Raji and G. Fried, About Face: A Survey of Facial Recognition Evaluation, 2021, https://arxiv.org/pdf/2102.00813.pdf

[90] D. Leslie, Understanding bias in facial recognition technologies, The Alan Turing Institute, 2020, https://zenodo.org/record/4050457#.YH7RdTHivD4

[91] M. Wang and W. Deng, Deep Face Recognition: A Survey, 2020, https://arxiv.org/pdf/1804.06655.pdf

[92] Tambiama Madiega and Hendrik Mildebrath, Regulating facial recognition in the EU- in-depth analysis, European Parliamentary Research Service (EPRS), Members' Research Service PE 698.021 – September 2021, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

[93] B.Kind, Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics, Ada Lovelace Institute, 2021, https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/

[94] G. Malgieri and M. Ienca, The EU regulates AI but forgets to protect our mind, 7 July 2021, https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/

[95] N. Smuha and others, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act", August 2021

[96] Podcast: The Bigger Picture EP. 6 - PROF. DANNY HAMIEL: HOW TO BUILD RESILIENCE & MAKING PSYCHOLOGY SCALABLE, May 16 2021,

https://music.amazon.com/podcasts/0badf9ac-3713-4149-b682-ebffc9b73412/episodes/b3bbc9a6-45a1-4882-b37f-ef81f95e9fa4/the-bigger-picture-ep-6---prof-danny-hamiel-how-to-build-resilience-making-psychology-scalable

[97] Invited Talk - Dr. Daniel Hamiel, From Crisis to Growth: Resilience Training with Children and Adults to Prevent Psychopathology and Build Life Skills, Biofeedback Federation of Europe (BFE), 18th Annual Meeting, March 2015, Salesian Pontifical University, Rome Italy, http://bfe-meeting.blogspot.com/2015/02/invited-talk-dr-daniel-hamiel.html

[98] Leo Wolmer, Daniel Hamiel, Michelle Slone, Maya Faians, Mayrav Picker, Tal Adiv, Nathaniel Laor, Post-traumatic Reaction of Israeli Jewish and Arab Children Exposed to Rocket Attacks Before and After Teacher-Delivered Intervention, Isr J Psychiatry Relat Sci - Vol. 50 - No 2 (2013), https://cdn.doctorsonly.co.il/2014/02/04_Post-traumatic-Reaction.pdf

© NIGHTINGALE Consortium, 2022. All rights reserved.

# Appendices

## Annex 1: Human Rights Due Diligence checklist: including International Human Rights Law, namely, dignity, privacy, gender, non-discrimination

| Human dignity, right to life and right to the integrity of the person | | |
|---|---|---|
| | Y/N<br>NA (Not Applicable) | Comments (for internal use of the organization) |
| Does your organisation have a code of conduct recognizing and embracing principles of human dignity, right to life and right to the integrity of the person? | | |
| Does your organisation include human dignity, right to life and right to the integrity of the person when training personnel? | | |
| What risks to human dignity, life and the integrity of the person is relevant in the activities of your organisation? | | |
| Does your organisation apply any decision-making process based on algorithms? | | |
| If yes, can this application have any effect on human dignity, right to life or right to the integrity of the person? | | |
| Would your organisation benefit for a specific training within Nightingale on these universal principles and on how to implement them in relation to the activities of your organisation? | | |
| For any questions please contact the project LSHM | | |

© NIGHTINGALE Consortium, 2022. All rights reserved.

## Right to private and family life

| | | |
|---|---|---|
| | Y/N<br>NA<br>(NotApplicable) | Comments (for internal use of the organization) |
| Does your organisation have a right to private and family life policy? | | |
| How does your organisation implement the right to private and family life of its workers ?(staff or volunteers) | | |
| How does your organisation implement the right to private and family life of its patients ?(staff or volunteers) | | |
| How does your organisation implement the right to private and family life of its customers ?(staff or volunteers) | | |
| Does your organisation include content on the right to private and family life in training? | | |
| Does your organisation have an internal/or external and independent review mechanism in case of breach? | | |
| How do you ensure the independence of the mechanism? (free from internal pressure)? | | |
| Does your organisation have a focal point for complaints of breach ? | | |
| For any questions please contact the project LSHM | | |
| | | |
| | | |

## Right to protection of personal data

| | | |
|---|---|---|
| | Y/N | Comments (for internal use of the organization) |
| Does your organisation have a protection of personal data policy? | | |
| If not, have you adopted specific measures to implement the protection of personal data? | | |

© NIGHTINGALE Consortium, 2022. All rights reserved.

| | | |
|---|---|---|
| When training personnel do you include guidelines for the protection of personal data? | | |
| Does the training or documentation policy include identifying when and what personal data is processed? | | |
| Is there an awareness in your organisation of what personal data is and that it includes sensitive data (e.g. patient data)? | | |
| Does your protection of personal data policy include special measures for the processing of personal data? (anonymization, pseudonimisation, minimisation of data policy...) | | |
| Is access to personal data secured by passwords? Restricted to authorized personnel? Include regular refreshment of passwords and similar safeguards | | |
| Does your organisation have a Data Protection Officer (DPO)? | | |
| Does your organisation have an internal review mechanism and focal point to prevent breach and in a situation of breach? | | |
| Would your organization benefit from a specific training session in the Nightingale framework? | | |
| Further questions or doubts? Please share them with the LSHM | | |

## Gender equality and non-discrimination policy[9]

| | Y/N | Comments (for internal use of the organization) |
|---|---|---|
| Does your organization have an equal opportunities and non-discrimination policy? | | |
| If not, have you adopted specific measures to implement equal opportunities and non-discrimination? | | |

[9] Extracted from D7.4 Ethics Handbook.

© NIGHTINGALE Consortium, 2022. All rights reserved.

| | | |
|---|---|---|
| Does your organization promote equal opportunities and non-discrimination actively (e.g. through training and/or specific documentation)? | | |
| Specifically, in the framework of the Nightingale project, has your organization actively worked towards the inclusion of female researchers (both at a senior and junior level) | | |
| Does your organization, e.g. when collecting data requiring to declare if male or female, provide fields for Male, Female, Non Binary and Not Declared? | | |
| Would your organization benefit from a specific training session in the Nightingale framework? | | |
| Further questions or doubts? Please share them with nightingale@ethics-heldesk.eu | | |

## Anti- harassment and non- sexual or gender based violence or any other form of violence including bullying at work

| | Y/N | Comments (for internal use of the organization) |
|---|---|---|
| Does your organisation include an anti-harassment policy and a zero tolerance to any sexual/gender-based or other form of violence? | | |
| Do you include periodic training of this policy? | | |
| Is there a focal point for anti-harassment and zero tolerance to any form of violence (especially sexual-based violence) in your organisation? | | |
| Is there an internal review mechanism in case of breach? | | |
| Would your organisation be interested in training within the framing of Nightingale? | | |
| For any further information please contact the project LSHM | | |

© NIGHTINGALE Consortium, 2022. All rights reserved.

| | | |
|---|---|---|
| **Misuse and Double-use Risk Mitigation** | | |
| | | |
| | Y/N | Comments (for internal use of the organization) |
| Does your organisation handle any of the following : sensitive data, large-scale data processing, drones (UAVs), biometrics, tracking and tracing software, facial recognition, automated data processing, Artificial Intelligence? | | |
| If yes, is there a risk mitigation from misuse or double-use policy? | | |
| If not, are there any special measures implemented? | | |
| If any of your relevant personnel be asked at random what does misuse and double-use mean in the context of your activity- would he/she know to answer? | | |
| Does your staff (including management) follow specific and periodic training on mitigating risk of misuse/double-use? | | |
| Is there a focal point and internal review mechanism on risk mitigation of misuse and double-use? | | |
| Would you and your organisation be interested in training within Nightingale? | | |
| For any further information please contact the project LSHM | | |