An enhanced pre-frontier intelligence picture to safeguard the European borders

D2.2
Report on the legal, and security requirements for border security

Editor(s)	Rowan Dennis, Katie Bailey, Helen Gibson (CENTRIC)
Lead Beneficiary	CENTRIC
Status	☒ Draft ☒ Consortium reviewed ☒ Peer reviewed ☒ Management Support Team reviewed ☒ Project Coordinator accepted
Version	1.0
Due Date	31/03/2022
Delivery Date	08/04/2022
Dissemination Level	PU

NESTOR is a project co-funded by the European Commission under the Horizon 2020 Programme (H2020-SU-SEC-2018-2019-2020) under Grant Agreement No. 101021851

Project	NESTOR – 101021851
Work Package	WP2 - User requirements analysis and operational scenarios
Deliverable	D2.2 - Report on the legal, and security requirements for border security
Editor(s)	CENTRIC – Rowan Dennis, Katie Bailey, Helen Gibson
Contributor(s)	
Reviewer(s)	KEMEA – Georgia Melenikou MAGG – Sofoklis Efremidis
Ethics Assessment	☒ Passed ☐ Rejected Comments:
Security Assessment	☒ Passed ☐ Rejected Comments:

Abstract	The deliverable, D2.2 'Report on the legal, and security requirements for border security' provides an analysis of the relevant legal, ethical and security considerations for the NESTOR system as a whole and each specific technical component through the lens of the use of NESTOR as a potential future operational system. The aim of this deliverable is to be used as a reference guide by partners to ensure that they are designing and developing the technical components of the system in compliance with existing and envisaged legal, ethical and security obligations. While several considerations have been taken into account, it is important that all partners continue to assess the potential issues which may arise throughout the duration of the project.
Disclaimer	The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Communities. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. © Copyright in this document remains vested with the NESTOR Partners

Version	Date	Partner	Description
0.1	05/11/2021	CENTRIC	Table of Contents
0.2	29/11/2021	CENTRIC	Initial input of content
0.3	10/01/2022	CENTRIC	Sections 2 & 3 input
0.4	27/01/2022	CENTRIC	Section 4 input
0.5	21/02/2022	CENTRIC	Section 5 input
0.6	28/02/2022	CENTRIC	Section 6 input
0.7	11/03/2022	CENTRIC	Final draft
0.8	21/03/2022	CENTRIC	Internal review
0.9	04/04/2022	CENTRIC, KEMEA, MAG, EtAB, SAB	Peer and Ethics Review Forms were integrated, Ethics and Security assessment were filled in
1.0	08/04/2022	HP, KEMEA	Final Version – Ready to submit

Executive Summary

NESTOR aims to demonstrate a fully functional next generation holistic border surveillance system providing pre-frontier situational awareness beyond maritime and land border areas. The design and development of such a system should be safeguarded by various legal, ethical and security needs, restrictions and requirements which must be fully adhered to by partners during system design and development to ensure compliance with the relevant frameworks.

This deliverable provides an analysis of the relevant legal, ethical and security considerations for the NESTOR system and each specific technical component through the lens of its deployment as a future operational system. The aim of this deliverable is to be used as a reference guide by partners to ensure that the design and development of the technical components of the system respect all such fundamental rights, legal requirements and security best practices.

This document provides detail on the legal frameworks in the European Union (EU) which protect an individual's rights and the wider security of the EU, the GDPR is contextualised to the parameters of the NESTOR project to identify the relevant data protection principles that ensure the technologies developed in NESTOR keep fundamental rights at the forefront of design and development decisions. Further to this, the specific considerations for each pilot country and related scenarios are examined. This is to ensure that national legal, ethical and security considerations are accounted for prior to any piloting activities and with a view to future operational use.

This document also provides a perspective on the legal and ethical dimensions of each specific component of the NESTOR system. While many issues are common across multiple components, particularly relating to data privacy and the use of artificial intelligence, a number of other areas have been addressed which focus on the application and use of the individual technologies. The security requirements are discussed ensuring appropriate methods for assuring the security of the NESTOR system and the protection of data are incorporated into the system design.

Finally, it is prudent to note that, while several legal, ethical and security aspects have been considered and presented in this document, it is important that all partners continue to assess the potential issues which may arise throughout the duration of the project.

Table of Contents

List of Figures

Terms and Abbreviations

ACM	Association for Computing Machinery
AR	Augmented Reality
AI	Artificial Intelligence
CFR	Charter of Fundamental Rights
DPIA	Data Protection Impact Assessment
EASA	European Union Aviation Safety Agency
ECHR	European Convention on Human Rights
EEZ	Exclusive Economic Zone
EC	European Commission
EU	European Union
FRA	Fundamental Rights Agency
GDPR	General Data Protection Regulation
HCAA	Hellenic Civil Aviation Authority
IBM	Integrated Border Management
ISPS	International Security and Port Security Code
LEA	Law Enforcement Agency
ML	Machine Learning
MR	Mixed Reality
MS	Member State
PUC	Pilot Use Case
RF	Radio Frequency
SAR	Search and Rescue
SOLAS	Safety of Life at Sea
SSA	Ship Security Assessments
SSP	Ship Security Plan
TCN	Third Country Nationals
TEU	Treaty of the European Union
TFEU	Treaty on the Functioning of the European Union
UAS	Unmanned Aircraft System
UN	United Nations
UNCLOS	United Nations Conventions on the Laws of the Sea
UxVs	Unmanned Vehicles

1. INTRODUCTION

NESTOR aims to demonstrate a fully functional next generation holistic border surveillance system providing pre-frontier situational awareness beyond maritime and land border areas. It is crucial that any technology developed and deployed as part of the NESTOR system has considered the legal, ethical and security implications associated with this field. This deliverable will define the legal, ethical and security needs, restrictions and requirements which all partners must consider throughout the development of the NESTOR project through to its potential operational deployment. The report will provide the framework to enable the technologies developed within NESTOR to comply with current data privacy and security legislation. The deliverable is structured into the following sections.

Section 2 describes the key themes throughout the deliverable; specifically, ethics, artificial intelligence, and data. This will provide the context for the cross-cutting issues aligned to the underlying technologies to be developed within NESTOR.

Section 3 will detail the major European legal frameworks, explaining how these pieces of law relate to the activities conducted within NESTOR and how they protect the rights of individuals. This section will also examine relevant legal aspects specific to the NESTOR domains, including both maritime and aviation laws. Section 4 provides a deeper treatment of the key principles of the General Data Protection Regulation (GDPR), and their application within NESTOR, including how the development of NESTOR can align with the GDPR.

Section 5 reviews the legal, ethical and security considerations and implications of the proposed NESTOR technology and the NESTOR system as a whole. This section will provide specific detail specific considerations necessary for compliance with the prevailing legislative frameworks. It will then detail the security requirements which are proposed to be included within the NESTOR system to ensure the privacy rights of individuals are considered.

In Section 6, specific considerations are discussed in relation to the pilot locations and scenarios. These include maritime and aviation laws local to each pilot country, along with the legal considerations relating to the specific issue the pilot scenario intends to address. The deliverable concludes in Section 7.

2. CONCEPTS AND DEFINITIONS

2.1 SUMMARY AND LEGAL CONTEXT OF THE NESTOR PROJECT

The goal of the NESTOR project is to protect and safeguard the land and maritime borders of the European Union (EU) through the development of border surveillance system, based on the concept of European integrated border management. NESTOR engages border agencies to demonstrate how they can take advantage of state-of-the-art technologies to enhance situational awareness at the external borders of the EU.

Specifically, NESTOR will bring together data from a range of sensing technologies (including radar, radio frequency (RF), and UxV (unmanned vehicle)-mounted cameras (image and thermal)) alongside online and existing data feeds into a visual analytics and situational awareness component that will enhance decision-making in command-and-control (C2) and operationally in the field through mixed reality (MR) for border security agencies (as shown in the high-level view in Figure 1: High-level view of the NESTOR concept

).

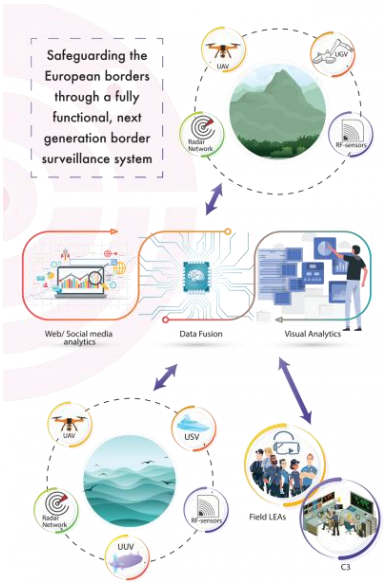

Figure 1: High-level view of the NESTOR concept

The development of NESTOR technologies will apply to both land and maritime borders at the 'pre-frontier' of the EU's external borders and testing will take place in three large-scale trials focused on different types of land and maritime border operations: trafficking of illegal goods, human trafficking and irregular migration, and search and rescue operations.

As a concept, European integrated border management was first established in Regulation (EU) 2016/1624 1 (subsequently repealed and replaced by Regulation (EU) 2019/1896 2.) The

overarching stated purpose of the Regulation can be extracted as follows (from recital (1), emphasis ours):

> *"The objective of Union policy in the field of external border management is to develop and implement **European integrated border management** at national and Union level, which is a necessary corollary to the **free movement of persons** within the Union and is a fundamental component of an area of **freedom, security and justice**. European integrated border management is central to **improving migration management**. The aim is to manage the crossing of the external borders efficiently and **address migratory challenges** and potential **future threats** at those borders, thereby contributing to **addressing serious crime** with a cross-border dimension and **ensuring a high level of internal security** within the Union. At the same time, it is necessary to act in **full respect for fundamental rights** and in a manner that **safeguards the free movement** of persons within the Union."*

To achieve the above, Article (3) provides the twelve main components of European integrated border management:

1. Border control (including border crossings, prevention and detection of cross-border crime).
2. Search and rescue operations.
3. Analysis of risks and threats for internal security.
4. Information exchange and cooperation between EU Member States (MS) and the European Border and Coast Guard Agency (Frontex)
5. Interagency cooperation between the border/coast guard authorities of the MS
6. Cooperation with relevant EU institutions, bodies, offices and agencies (such as European External Action Service, Europol, EU Agency for Asylum, Fundamental Rights Agency, EU Agency for Criminal Justice Cooperation, etc. – the full list can be found in Article 68).
7. Cooperation with third countries.
8. Technical and organisational measures within the Schengen area for border control.
9. Return of third country nationals (TCNs).
10. Use of state-of-the-art technologies including large scale information systems.
11. Quality and vulnerability control to ensure the implementation of EU law.
12. Solidarity mechanisms in particular EU funding instruments.

All of the above, also embed the overarching components of fundamental rights, education, training, and research and innovation. NESTOR addresses or contributes to the improvement and implementation of several of those objectives, specifically (1), (2), (3), (5), (8) and (10).

As mentioned above, NESTOR explicitly focuses on 'pre-frontier' situational awareness. The Regulation described applies the following definition, *"'pre-frontier area' means the geographical area beyond the external borders which is relevant for managing the external borders through risk analysis and situational awareness".* Consequently, the core focus for NESTOR is detecting the movement of goods and people, and the cooperation of EU and third country agencies around the EU external borders. Therefore, the discussion of the legal, ethical and security aspects of border security within the NESTOR project will be analysed within the context of the border security environment, the technology to be developed, and the proposed trialling activities.

2.2 ETHICS

It is difficult to define ethics as one particular notion, as it is often explained in ways relevant to the type of ethics being addressed. The aim of this deliverable is to define the requirements for how the NESTOR system should be implemented in an operational environment in an ethically-aware and compliant manner. Therefore, an important element is to examine the ethics surrounding the development and use of the various technologies by LEAs, border agencies and other relevant stakeholders in the context of the integrated border management environment (IBM) and in relation to the use cases defined for the trialling activities.

The wider view of ethics in the IBM context and the corresponding development of technology to support the delivery of IBM within NESTOR means that professional ethics in the domain of technology development, such as the Association for Computer Machinery (ACM) Code of Ethics and Professional Conduct 3, is essential. The ACM code has seven overarching principles: (i) contribute to society and to human well-being, acknowledging that all people are stakeholders in computing; (ii) avoid harm; (iii) be honest and trustworthy; (iv) be fair and take action not to discriminate; (v) respect the work required to produce new ideas, inventions, creative works, and computing artifacts; (vi) respect privacy; and (vii) honour confidentiality. As computing professionals these principles should already be embodied in the development of NESTOR technologies.

Many of these principles are also aligned with the specific ethical guides for particular technologies (e.g., artificial intelligence (AI)). For example, the European Commission states that AI systems should improve individual and collective wellbeing, and subsequently sets out four ethical principles which should be adhered to when designing and developing AI systems, to ensure this is done in a trustworthy manner 4. These are: (i) Respect for human autonomy; (ii) Prevention of harm; (iii) Fairness; and (iv) Explicability. These principles are intertwined with the fundamental rights and show the importance of legal and ethical considerations in achieving trustworthy AI. AI is considered in its own right in Section 2.3 below.

On the operational side, Frontex (the European Border and Coast Guard Agency) has also produced a document on the 'Ethics of Border Security' 5 that provides a guide (mainly to border guards) on the ethical challenges they may face in their role. The issues presented consider both the principles relating to specific border guard activities as well as the use of technology with the border domain. In line with the goals and activities of NESTOR, the

sections on Border Surveillance (5 s2.3, p32), Surveillance of Borders [in the context of ethics and technology] (5 s3.3, p45) – including the use of Unmanned Aerial Vehicles (UAVs, Radar and various cameras) and the use of databases/data-mining approaches (5 s3.5, p52) are all relevant and highlight specific ethical issues that should be considered in the context of border security. Nonetheless, it is also worth noting that the guide was produced in 2011 (i.e., pre-GDPR and before the widespread use of AI) and therefore there are further aspects which should now also be considered.

2.3 DATA FUSION AND PROCESSING

Data underpins the whole NESTOR system and includes personal data, sensor readings, models, imagery, text, and computed values. The availability of vast amounts of data provides significant potential for IBM activities, the proper processing and management of data is necessary to comply with legislation related to data protection and ethics.

For example, information from online can be helpful to authorities looking to detect instances of criminality (for example, a forum post detailing an occurrence of human trafficking, leading to detection of the crime), there is a necessity for NESTOR partners to collect and process personal data in a GDPR compliant way to ensure the protection of data subjects' rights and especially that of potential victims. Where the NESTOR system processes personal data, this will be subject to the GDPR principles described in Section 4, such as the principles of data minimisation and storage limitation. Sections 3 and 4 will provide information on the general provisions which must be adhered to when processing personal data. Section 5 will the put forward specific considerations for each technological component.

2.4 ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI), along with other forms of automated processing such as machine learning (ML), are playing an ever-increasing role in all parts of society, including the policing and security sector 6. While AI and ML offer a wealth of opportunities to security stakeholders (including law enforcement agencies, border and coast guards), it is important that legal and ethical considerations are taken into account at all stages of design, development and implementation to ensure any issues are mitigated at the earliest possible stage. AI yields great potential to significantly enhance the effectiveness of security and operational activities at the borders and beyond 7, however as AI technologies continue to evolve the legal, ethical and security challenges faced need to be considered extensively.

To support a harmonised view on AI, European Commission have proposed the following definition in its Communication on AI 8:

"Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)."

NESTOR will use this definition as the overarching definition for AI within the project.

3. GENERAL APPLICABLE LEGAL FRAMEWORKS

NESTOR, as a project, falls in the domain of border security, specifically in the context of the European Union, it considers both land and maritime borders and the activities and required cooperation that happen across them. This ranges from criminal aspects such as the trafficking of goods (also weapons, drugs, etc.) and people; instances of irregular migration[1], but also search and rescue operations; and, in some cases the intersection of these activities. Within the EU each of these aspects are governed by specific legal frameworks. Furthermore, to prevent, detect and intervene in these instances usually requires access to additional, and often personal, data, the development and operation of advanced technologies and the integration of national law.

This section will review and discuss existing legal frameworks that coincide with proposed domain and activities of the NESTOR project and how they manifest specific requirements within the project. The first aspect is the consideration of Fundamental Rights as this key principle underpins Article 6 of the Treaty on European Union (TEU) 9, one of the two primary treaties of the European Union (the other being the Treaty on the Functioning of the European Union (TFEU)).

3.1 EU FUNDAMENTAL RIGHTS

In 1948 the United Nations (UN) consolidated the first formulation of a document stating the requirements of every country within the UN to provide fundamental rights to every citizen without discrimination. Shortly afterwards, in 1950, the European Convention on Human Rights (ECHR) enshrined these rights in international law through the Council of Europe. These were at the forefront of the protection of citizens globally until the EU proposed a bill to incorporate and acknowledge the "common principles of the national constitutions and the ECHR" 10 in 2000. The Charter Fundamental Rights of the European Union (CFR) became legally binding in 2009 after the passing of the Lisbon Treaty. The TEU as described in the section above links the ECHR and the CFR to the overarching treaties of the EU. This section will give a brief overview of the frameworks governing fundamental rights in the EU and how they relate and impact upon the goals of the NESTOR project.

Fundamental rights concern important factors regarding "dignity, fairness, respect and equality."11 The EU Fundamental Rights Agency (FRA) provides guidance and requirements to EU Countries and citizens on when and how the CFR applies compared to the EHCR; notably

[1] In the EU context, the definition of an irregular migrant is: "a third-country national present on the territory of a Schengen State who does not fulfil, or no longer fulfils, the conditions of entry as set out in the Regulation (EU) 2016/399 (Schengen Borders Code) or other conditions for entry, stay or residence in that EU Member State." https://ec.europa.eu/home-affairs/pages/glossary/irregular-migrant_en

that the CFR applied when a MS is implementing a union law whilst the ECHR can be applied more broadly 12.

The main elements of the Charter of the grouped into seven titles: Dignity, Freedoms, Equality, Solidarity, Citizens Rights, Justice and General Provisions"13. **Dignity** or Title I (Articles 1-5) refers to the quality and right to human life; Title II - **Freedoms** highlight the right to expressions and privacy of individuals within the EU; this includes but is not limited to the protection of personal data, respect to private and family life. **Equality** (Title III) describes how citizens, business and governments should not discriminate and always provide racial, gender and cultural equality. There are also separate articles of the rights for the elderly, children, and disabled persons within this section. Title IV - **Solidarity** – sets out the protection of an individual's core elements of life: the rights to a work, social and family life including the protection of workers, health care regimes including financial support and protection rights. Title V - **Rights of Citizens** – includes aspects such as the right to vote and to be a candidate, the right to freedom of movement and diplomatic and consular protection – an important set of factors when referring to border and maritime law. Title VI - **Justice** - offer citizens' rights in law, right to defence, principles of legality and rights in trial including the right to an effective remedy and fair trial. The final provision of the CFR details the scope, application, and level of protection and how rights can be abused, these articles provide an overview to all other articles. The TEU/TFEU recognises the CFR as having the same legal value as the treaties and the TEU accedes to the ECHR; therefore, fundamental rights are one of the principles on which the EU is founded and are enshrined in EU law. Ultimately, as NESTOR is developed to protect EU citizens is underpinned by the protection of fundamental rights for all.

Furthermore, to align with the NESTOR use cases the CFR (in Article 5) expressly prohibits human trafficking and is mirrored to a certain extent in the ECHR based on Article 4 that mentions the prohibition of slavery and the slave trade, which can be interpreted relating to human trafficking in the modern day 14. Similarly, as will be discussed in relation to the UN Convention on the Safety of Life at Sea (SOLAS) is borne out of the right to life (Article 2 of the ECHR).

Overall, the general provisions are the limitations on the usage of the CFR and the responsibilities of the EU. By definition, fundamental rights are orientated around the law and the protection of individuals. Recently, the protection of personal data and the illegitimate use of such data – therefore violating a person's rights - has become a particularly high-profile topic. The result of these concerns was the introduction of the General Data Protection Regulation (Regulation 2016/679) 15 - a universal approach to data protection across the European Union.

3.2 GENERAL DATA PROTECTION REGULATION (GDPR)

Regulation 2016/679 of the Council of the European Union more commonly known as "General Data Protection Regulation (GDPR)" is implemented in the national law of all EU MS. The GDPR applies to any business, organisation or individual in the EU and ensures that they

apply consistent data protection legislation in their MS. Should they fail to abide to the GDPR's requirements and constraints they are liable to be subjected to legal action based on MS law. The goal of this deliverable is to focus on the legal, ethical and security aspects of the envisaged operational NESTOR system, therefore, while the project itself also must conform to the GDPR, here we focus on GDPR's applicability in operational contexts.

Article 4 of the GDPR defines a set of specific terms that relate to the entities (e.g., business, organisation, individual) involved in the processing of information. Firstly, there are several important terms to define to ensure that the scope of what personal data and data processing means in the wider context and, as will be discussed in the Section 4, the context of personal data processing within NESTOR.

"*Personal Data"* is defined in Article 4 of the GDPR as:

> *"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."*

It is important to note that the list of factors is non-exhaustive, and that the *processor* (definition below) has responsibility to identify what is personal data in the scope of their processing activities. Therefore, further important definitions include "*Data Subject*" – as the individual whose data is collected ultimately what is meant by "*processing"* (of personal data). The GDPR sets this out as:

> *"[processing] means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*

Processing itself is governed by one or two types of entities: the data controller and the data processor. The *"Data Controller"*, which may be a person, organisation, public body or any other entity determines the purpose and meaning of any data processing activity while the "*Data Processer*" processes data on behalf on the controller and the scope of what and how is processed is fully determined by the data controller. If any violations occur, the processor has an obligation to inform the controller within two days of the incident where the appropriate remedy to the "*Data Subjects*" can be applied regarding a breach of their data.

How each of the specific articles within the GDPR are relevant to NESTOR are discussed in more detail in Section 4; however, the instances where personal data is likely to be collected include through video camera images, through online and social media monitoring, potentially through some of the attached metadata from RF signals and also the data of the operators of the NESTOR system.

Chapter 2 of the GDPR sets out the following Articles V-IX which hold a valuable role in the protection of personal data and determining the reasoning behind the processing of a subject's data.

1. **Article 5** – Principles relating to the processing of personal data – ensuring that personal data in NESTOR is processed in accordance with the six core principles of processing
2. **Article 6** – Lawfulness of Processing – determining the legal basis for processing personal data in the operational context of border surveillance
3. **Article 7** – Conditions for Consent – the necessary conditions if consent is relied upon as a legal basis for processing
4. **Article 8** - Conditions applicable to child's consent in relation to information society services – potentially limited scope in NESTOR; however, minors are also trafficked or are part of irregular migration and therefore may have personal data processed
5. **Article 9** - Processing of special categories of personal data – additional conditions required for processing data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The GDPR is a core legal framework within NESTOR and there are several instances where processing of personal data to support the border surveillance requirements of the system may occur including visual data including persons from cameras and sensors, online and social media data. Section 4 considers each of these principles and explain their meaning and applicability within NESTOR and any best practices for ensuring that technology development remains in compliance with the GDPR overall.

3.3 RELEVANT LEGISLATION TO NESTOR SCOPE

While the protection of fundamental rights and the protection of personal data are almost universally applicable, the scope of NESTOR is particularly focused on border surveillance as well as the use of technologies (e.g., unmanned or autonomous vehicles and artificial intelligence) which necessitates the analysis of further legislation.

Furthermore, NESTOR operates at the 'pre-frontier' of the European Union and consider various cross-border applications. Therefore, the legislative scope must reflect each of these potentially different jurisdictions. To introduce further complexity, NESTOR is designed to operate at both land and sea borders. These two aspects relate to multiple areas of the law. Firstly, one of the four freedoms of the EU is the free movement of individuals as set out in Article 45 of the "*Treaty on the Functioning of the European Union*" which offers rights to EU citizens enshrined in law. Specifically, this allows any EU citizen to enter another MS with the right to find work and enjoy equal treatment with nationals in access to employment, working conditions and all other social tax advantages. A MS cannot impede the movement of an EU

National, and the legislation that governs the entry into the Schengen areas is Regulation 2016/399 also known as the "Schengen Border Code." 16

Operations that involve a maritime component must also pay due attention to maritime law which is a complex patchwork of legislation that has evolved over hundreds of years beginning through to the modern regulations that include UNCLOS (United Nations Convention on the Laws of the Sea) and SOLAS (International Convention on the Safety of Life at Sea).

NESTOR will also make use of technology such as unmanned aerial vehicles and artificial intelligence applications and therefore must also to be comply with the aviation and drone specific laws including their application in cross-border situations. Meanwhile, the EU is also seeking to introduce specific legislation to govern the use of artificial intelligence, and while the legislative processes are not yet complete it is essential to ensure NESTOR development and technology is fully aware of the potential consequences of future AI legislation.

3.3.1 Schengen Borders Code and Integrated Border Management

The Schengen Borders Code is the overarching legislation for internal and external border control within the Schengen area. The Schengen area includes all countries marked in blue in Figure 2: Schengen Area (Blue) [*Countries highlighted in Yellow are working to implement this later]*

[2] below, while the EU MS of Bulgaria, Cyprus, Croatia and Romania are still working towards fully joining the Schengen area, they must already comply with the rules for external border

Figure 4: Schengen Area (Blue) [*Countries highlighted in Yellow are working to implement this later]*

[2] Image from https://commons.wikimedia.org/wiki/File:Schengen_Area.svg

crossing into the EU. Furthermore, the code also supports the implementation of the EU policy on integrated border management as was introduced above.

The current version of the code sets out the following important concepts relevant to NESTOR. Firstly, Article 2 provide several important definitions, most notably:

1. External borders – *"means the Member States' land borders, including river and lake borders, sea borders and their airports, river ports, sea ports and lake ports, provided that they are not internal borders"*.

2. Border Surveillance – *"means the surveillance of borders between border crossing points and the surveillance of border crossing points outside the fixed opening hours, in order to prevent persons from circumventing border checks.*

Article 3 sets out the scope of the code and its application to *"any person crossing internal or external borders without prejudice to:*

1. the rights of persons enjoying the right of free movement under Union law;
2. the rights of refugees and persons requesting international protection, in particular as regards non-refoulement".18

Meanwhile, Article 4 links the code back to the obligations of the CFR.

NESTOR considers the specific contravention of the code, in the sense that while EU nationals are free to enter the Schengen Area, third country nations (TCNs) must possess valid documentation (passport, visa), justifications for their visit and have time-limits on the duration they can stay.

Article 13 sets out the conditions on Border Surveillance stating that its purpose is to:
1. prevent unauthorised border crossings
2. counter cross-border criminality, and
3. take measures against persons who have cross the border illegally.

These aspects are fully aligned to the goals of NESTOR and the project should consider the other aspects of this article and consider the requirements for both stationary and mobile surveillance, regular updates to surveillance periods to increase the likelihood of illegal border crossing detection, and the need for the use of technical and electronic means for such detection.

It should also be noted that since the 2020 Pact on Migration and Asylum, the EC has been consulting on updates to the Schengen Borders Code. More in particular, in the proposed updates to the regulation 19 Article 13 includes an explicit mention of the uptake of technologies such as UAVs and mobile sensors to support border surveillance activities. Additional aspects relating to border control legislation of specific countries are also considered in Section 6 when assessing the PUC.

As discussed in Section 2.1, the EU's policy on integrated border management is also a cornerstone of their approach to border surveillance and the management of the EU's

external borders 20 and therefore must play a fundamental role at the forefront of NESTOR's development to ensure full alignment with this strategy.

Finally, NESTOR proposes integration with EUROSUR 21 (the European Border Surveillance system). EUROSUR provides a framework for the standardisation of the information exchange and cooperation between MS and Frontex to support situational awareness at the external borders (i.e., the pre-frontier) of the EU. The EC has an implementing regulation on EUROSUR 23. The potential future success of NESTOR is likely dependent on effective cooperation with EUROSUR. Similarly, links to CISE (Common Information Sharing Environment) may also be relevant; however, CISE is not part of any existing legal frameworks within the EU and considered a voluntary and collaborative process for enhancing and promoting relevant information exchange 24.

3.3.2 Maritime Law

Maritime law mostly emanates from historic treaties from the United Nations (UN) and are fundamental to the protection of countries with land-sea borders. The United Nations Convention on the Law of the Sea (UNCLOS) and the Safety of Life at Sea (SOLAS) are the prevailing legislation in to respond to activities and incidents that occur at sea within the jurisdiction of every country within the UN.

In the case of maritime law, the distance out to sea determines who has the jurisdiction to act. The UNCLOS enshrines the distance between the coast up to twelve nautical miles out to sea as the "territorial sea" of the country whose coast it is. In this area they have the power to impose their laws and restrictions. Under the UNCLOS, a country is not able to impede the movement of a vessel in its territorial waters unless the actions or request of the vessel cover the instances found in the Article 27(a-d) in the case of criminal activity:

1. *if the consequence of the crime extends to the coastal state;*
2. *if the crime is of a kind to disturb the peace of the country or the good order of the territorial sea;*
3. *if the assistance of the local authorities has been requested by the master of the ship or by a diplomatic agent or consular officer of the flag State; or*
4. *if such measures are necessary for the suppression of illicit traffic in narcotic drugs or psychotropic substances [22]*

If one of the above situations occurred after twelve nautical miles, then they could only continue to act only if the interactions began in their territorial state. For example, a vessel became a threat and then attempted to flee into the Contiguous Zone (after the Territorial Sea) the territorial state can continue to pursue until the International Waters (24 nautical miles from the country's baseline). Nonetheless, the scope of NESTOR focuses around the areas of the territorial sea and therefore, other aspects of maritime law are beyond the scope of this deliverable.

Maritime law also has a further convention that relate to the requirements of vessel while at sea operating in international waters. The International Convention for the Safety of Life at Sea or SOLAS was introduced in 1914 after the Titanic disaster. This convention gives to the

master of a ship at sea which can provide assistance, the "obligation to provide assistance applies regardless of the nationality or status of such persons or the circumstances in which they are found" [23] in the case of a search and rescue operation. The SOLAS convention is paramount to the protection of individuals while at sea, especially when focusing on the border crossing of migrants for example. It is a country's legal requirement to provide a service to anyone regardless of their "status" or "nationality" as stated in the SOLAS Convention. The introduction of the SOLAS agreement is critical convention designed to mitigate losses of life while operating out on International and Internal / Territorial waters.

Further safety procedures were introduced via the International Security and Port Security Code (ISPS) this was introduced post the events on September 11th, 2001, and as a response to providing more clarity and security procedures on an international scale. The ISPS was an addition to Chapter 11.2 of the SOLAS convention. The ISPS code introduced the Ship Security Assessments (SSA) and the Ship Security Plan (SSP) to ensure that there was a fundamental and direct approach to responding to international threats on board of a vessel.

The International Convention on Search and Rescue (also known as the SAR Convention) provides a framework for search and rescue operations globally that ensures *"no matter where an accident occurs, the rescue of persons in distress at sea will be co-ordinated by a SAR organization and, when necessary, by co-operation between neighbouring SAR organizations"* 25. Of particular relevance to NESTOR is Chapter 3 that sets out that SAR operations should be coordinated with those of neighbouring states (e.g., those that share a land or sea border) and that entry into the territorial sea of another state is permissible in the case of searching for or rescuing maritime casualties.

In addition to UNCLOS, SOLAS ad the SAR Convention, Regulation 656/2014 26 provides the European context for maritime border surveillance. The regulation sets out the necessary contexts for detection (of vessels smuggling migrants or otherwise avoiding border checks) (Article 5); interception within the territorial sea, high seas or contiguous zones (Articles 6, 7 and 8); and search and rescue situations (Article 9) which have relevance to NESTOR.

Maritime Law extends at length into each section of the Pilot Use Cases – Section 6 will discuss the specific countries' legislative framework in relation to maritime law in the scope of NESTOR.

3.3.3 Aviation (UAV/drone) law

NESTOR proposes the use of UxVs to increase the surveillance area with limited resources. As part of the UxV fleet this will include utilising drones to support aerial surveillance. The use of drones (or unmanned aerial vehicles (UAVs)) is covered under aviation legislation and depends on the area to be flown over and the category of drone. In Europe, the European Union Aviation Safety Agency (EASA) manage civil aviation operations include those relating to UAVs providing regulations on the weights of specific drones and the heights and locations that they are legally allowed to be piloted.

The core legislation surrounding the utilization of UAVs (referred to as Unmanned Aircraft Systems (UAS)) in Europe is the "*Regulation 2019/947 on the rules and procedures for the operation of unmanned aircraft*" 27 The UAVs in NESTOR may operate in the either the specific or open categories. It is the operator's responsibility to identify which category the UAV belongs to and the associated rules for flying. Further information is set out in the Commission Delegated Regulation (EU) 2019/945 28. The main difference between the open and specific categories is that the open category does not require operational authorisation prior to conducting a flight 29 - this would be advantageous to NESTOR as UAV operations may need to take place at short notice to respond to an alert of a border-related incident. Where an UAV falls into the specific category a risk assessment must take place to assure the safe operation of the flight. Regardless of UAV category, all UAV operators must register in their MS (based on residence or business operation) and any UAV pilots must have undergone appropriate training. Finally, many countries have no-fly zones for UAVs and so the aviation restrictions should be reviewed prior to any flight.

In the case of additional national legislation these will be addressed in Section 6.

3.3.4 Proposed Artificial Intelligence Act and AI ethics

Artificial intelligence (AI) is one of the key-enabling technologies set out by the European Commission that have the potential to be transformational 30. While the technological uptake of AI has been rapid, the need for ethical and ultimately legislative controls on the use of such technology has also become imperative. Furthermore, the use of AI must be strictly controlled in relation to the use of personal data as Article 22 of the GDPR 31 states that individuals "*shall have the right not to be subject to a decision based solely on automated processing … which produces legal effects concerning him or her or similarly significantly affects him or her.*" It is therefore important that the use of AI focuses on decision support and what is sometimes referred to as 'augmented analytics' speeding up processes that would take analysts significant time but leaving the final action to a human decision based on all available evidence.

The EC has proposed in recent years a 'European approach to artificial intelligence' 32 An important first step in this approach was establishing the parameters of what is meant by trustworthy AI. The first important strategy to this end was the European High-Level Expert Group's (HLEG) Ethics Guidelines for Trustworthy AI which suggested seven key requirements for the trustworthy and ethical use of AI (human agency and oversight; technical robustness and oversight; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; and accountability) 33.

The development of these guidelines was a forerunner to the Proposal for a Regulation on Artificial Intelligence 34 which will form a framework for the requirements and obligations for implementations of AI. The regulation defines different levels of risk for different AI systems (from unacceptable risk to minimal risk) with each level of requirements and scrutiny. Of particular relevance for NESTOR is the classification of systems relating migration, asylum and border control management as being high-risk and therefore, NESTOR, in the event of the implementation of the future AI regulation may need to be in compliance with these

requirements. Specific aspects include risk assessment and mitigation, quality of data input, logging for traceability, documentation, information provided to the user, human oversight, and robustness, security and accuracy.

The recent work of the AP4AI project[3] (amongst others) also sets out the key principles for accountability in the use of AI in the internal security domain. The twelve AP4AI principles of legality, universality, pluralism, transparency, independence, robustness of evidence, enforceability and redress, compellability, explainabilty, constructiveness, conduct, and learning organisation 35 alongside the practical considerations in the report provide specific factors that uniquely need to be incorporated into AI systems for internal security in the EU.

3.4 KEY CONSIDERATIONS

NESTOR must adhere and strive to protect the **fundamental rights** of all citizens in accordance with the ECHR and the CFR especially considering the aspects related to the protection of victims of human trafficking and the right to life in respect of maritime incidents.

The **protection of personal data** as set out in the general data protection regulation is paramount and all personal data processed must have a basis in law and comply with all requirements for processing (elaborated in Section 4).

NESTOR's scope is closely linked to the principle of **European Integrated Border Management** and must seek to implement the laws set out in the **Schengen Borders Code** by supporting its approach to border surveillance (unauthorised crossings, cross-border crime, and acting against illegal crossings) including the proposed future requirement for the use of technical means to support border surveillance activities.

To work to link and integrate with **EUROSUR** and **CISE** as important instruments to support a unified approach to border surveillance activities and assure the future compatibility of the system within the European border management environment.

UNCLOS and SOLAS provide the key frameworks for the implementation of maritime law, most NESTOR capabilities are proposed to take place within the distance of the territorial sea and therefore fall under the jurisdiction on the coastal state. NESTOR system may also be called upon to support the implementation of the **SAR convention** in the coordination of search and rescue operations while the EU's border regulation provides the necessary justifications for the application of NESTOR to the detection of vessels smuggling migrants, interception in the territorial sea and further guidance on SAR operations.

The use of UAVs is subject to compliance with the necessary **aviation regulations.** Therefore, operators must ensure that the obtain the appropriate **licence** and **authorisations**, that the UAV pilots have undergone the necessary **training**, and that they are aware of no-fly zones and flying restrictions in the case of populated areas.

[3] Ap4ai.eu

Artificial intelligence provides a significant opportunity to process, analyse and extract information from large volumes of data, the proposed **Artificial Intelligence Act** will have a significant impact on the use and application of AI in the EU.

The above considerations translate into the following requirements

LER-001	NESTOR system must be compatible with fundamental rights (from CFR and ECHR)
LER-002	Processing of personal data must be in compliance with the GDPR and any relevant national laws
LER-003	The system should support the implementation of the Schengen Borders Code
LER-004	The system should support the vision for European Integrated Border Management
LER-005	Information exchange should be compatible with EUROSUR for future interoperability
LER-006	The conventions set out in UNCLOS, SOLAS and SAR convention must be applied in the context of the territorial sea
LER-007	UAV flights must have the appropriate drone licence, aviation authorisation and pilot training.
LER-008	Responsible, trustworthy, and accountable AI development and deployment is essential. The legislative progress of the AI Act should be monitored.

4. DATA PROTECTION AND SECURITY CONSIDERATIONS

The protection of personal data is a fundamental aspect to the security and safety of subjects (staff and citizens) who will interact with NESTOR. While Section 3.2 discussed the emergency and overarching purpose of the GDPR this section will set out the main scope of the relevant articles within the GDPR that NESTOR must be in compliance with and propose which aspects of the system will likely process personal data and provide a bridge to more specific discussions in Section 5.

In NESTOR, the following components will likely process personal data: images/video from surveillance cameras, information collected from online sources such as social media and internet forums, and user accounts and authentication methods (back-office functionality). Furthermore, future integration with EUROSUR could result in additional processing of personal data depending on the information exchanged.

To reiterate from Section 3.2, processing is defined as,

"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"

Therefore, when considering data processing operations in the context of the GDPR, the collection of personal data, the transformational actions (pre-processing, extraction, analysis), storage, presentation/disclosure, and disposal/deletion of that data must all handled in compliance with the GDPR.

The following sections consider the main articles of the GDPR and how they relate to NESTOR.

4.1 ARTICLE 5 – PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

Article 5 is the foundation of the GDPR and sets out the core requirements to allow how the processing of personal data. The principles of Article 5 state that personal data shall be processed in manner that is:

1. *processed lawfully, fairly and in a transparent manner in relation to the data subject (‘**lawfulness, fairness and transparency**’);*
2. *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes […] (‘**purpose limitation**’);*
3. *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimisation**’);*
4. *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘**accuracy**’);*
5. *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed […] (‘**storage limitation**’);*
6. *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘**integrity and confidentiality**’).*

In the context of NESTOR’s operational system, compliance with the above principles is mandatory. The purpose of the collection of any personal data will solely be for the function of carrying out border surveillance operations and search and rescue operations as necessary. NESTOR will only collect data for this purpose and not retain this data for any further use. Furthermore, personal data contained in images or from online sites will be kept to a minimum and in the context of NESTOR the aim is not to identify a person but to provide intelligence to counteract illegal activities in the border region. If collected data is identified as being not relevant, then the system will not retain this information. Furthermore, as explained in Section 5.3 the appropriate security measures will be applied to ensure the integrity and confidentiality of data in the system.

4.2 ARTICLE 6 – LAWFULNESS OF PROCESSING

Any processing of personal data carried out under the GDPR must have a legal basis based on a set of conditions in the GDPR. These conditions are the following:

1. *the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;*
2. *processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
3. *processing is necessary for compliance with a **legal obligation** to which the controller is subject;*
4. *processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;*
5. *processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;*
6. ***processing is necessary for the purposes of the legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

In the case of the operational version of the NESTOR system, the processing could be considered in the public interest – protecting the borders of the EU, in the case of a search and rescue situation it could be to protect the vital interests of the data subject or depending on the authority vested in the border guard operation the processing may be necessary in order to comply with their statutory legal obligations their operation as a border guard.

For processing of data of employees, in the context of either back-office functionality (such as the management of user accounts) or in the case where the images of border guard officials are also captured on camera during area monitoring the basis for processing should be consent.

The specifics of providing consent and the ways in which it can be given are also set out in Article 7. The requirements are that the consent must be demonstratable, freely given and distinguishable from any other consent given, and the data subject must be free to withdraw their consent at any time.

4.3 ARTICLE 9 – PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

The processing of special categories of personal data is prohibited except for in specific cases. Article 9(1) defines special categories of personal data as

> *"… personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation ...."*

In the case of NESTOR there are no existing requirements for the processing of special categories of personal data; however, it is accepted that when processing data from online sources there is a limit to the extent that the processor can know what type of data will be processed. Therefore, it is essential to perform online and social media acquisition in a targeted manner that limits the opportunity for accessing such data and/or making use of pseudonymisation or anonymisation techniques to further safeguard any potential processing of such data.

Processing of special categories of data can only occur when specific criteria are met, these are set out in Article 9(2) and include (amongst others) (a) explicit consent; (c) protecting the data subjects or another person's vital interests; (e) the data are manifestly made public by the subject; (g) substantial public interest; (i) public interest in the context of public health including protection of cross-border threats; and (j) scientific research (amongst others). This final aspect is only relevant to NESTOR in the context as a project and not as an operational system.

The NESTOR platform must ensure that these categories are met during the PUCs and in real world application to ensure that no fundamental freedoms are infringed upon of the data subjects or individuals who are involved within the project. Furthermore, many MS have specific derogations in relation to Article 9 and so any additional restrictions due to national law must also be included.

4.4 SECURITY, STORAGE AND RETENTION OF DATA

The principle of 'storage limitation' is set out in Article 5(1)(e) which says that personal data must be:

> *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed…"*

Therefore, any data acquired by NESTOR must be stored only for the length of time that is necessary and must be protected by appropriate technical and organisational safeguards. Article 32 sets out the requirements for the security of processing to ensure the security of data including the implementation of pseudonymisation, encryption, resilience and backups of data and systems and organisational measures for testing the effectiveness of these aspects. Furthermore, Recital 39 notes that time limits for erasure or period review of data held should be established.

The development of NESTOR should also ensure that it complies with the requirements set out in Articles 15-17 of GDPR. These articles determine how the interaction between data

subject and data controller occurs – including the data subject's abilities protect their fundamental rights regarding their privacy. These include mechanisms for

1. Right of access (to their data) by the data subject (Article 15) and the purposes, categories of data, length of time stored and if it is part of any automated decision-making process

2. Right to rectification (Article 16) allows data subjects to control their data, by giving them the right to rectification of inaccurate personal data concerning him or her.

3. Right to Erasure ('Right to be Forgotten') (Article 17) - the legal right to have their data erased where it is no longer necessary in relations to the purposes for which they were collected or otherwise processed, consent is withdrawn, no overriding legitimate grounds for processing, or the processing was unlawful (amongst others).

Finally, and importantly in the case of NESTOR the GDPR sets out the need for a data protection impact assessment (DPIA) under Article 35 in the case of *"…a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons."* Given the application of NESTOR, in the domain of border security and surveillance it could be necessary to undertake a DPIA in the context of the system and individual components that acquire and process personal data; relevant component (such as online and social media monitoring should continuously evaluate their data acquisition strategies and conduct a DPIA if such processing becomes high-risk.

4.5 KEY CONSIDERATIONS

Firstly, it is important to note that data within NESTOR is only personal data if it relates to an identifiable person. Therefore, in all instances where it is not necessary to identify the person involved efforts to **anonymise** the data at source should be undertaken.

In all other cases, NESTOR must ensure that a **lawful basis for processing** has been established in advance of the processing activity and that this basis remains valid throughout system operation.

All considerations in relation to defining the **purpose** for processing, the requirement to collect the **minimum** amount of personal data as possible to satisfy the purpose and to ensure this data is both **accurate** and **stored** only for the period necessary, and that appropriate **technical and organisational measures** are put in place to ensure to security of all personal data.

If **special categories of personal data** are to be processed, there must be the appropriate justifications in place to allow such processing to happen lawfully and where NESTOR is making use of new technologies or systematically monitoring a publicly accessible area on a large scale the need for a **data protection impact assessment** must be evaluated and completed prior to operational deployment.

These can be translated into the following legal and ethical requirements

LER-009	Personal data should be anonymised where feasible and not required for intelligence
LER-010	A lawful basis for processing must be established for each and every type of personal data collected
LER-011	All six principles for the processing of personal data should be documented and applied
LER-012	Justifications and safeguards must be in place in the case of processing special categories of personal data
LER-013	A data protection impact assessment should be carried out where the use of new technologies for processing personal data is required

5. LEGAL, ETHICAL AND SECURITY CONSIDERATIONS FOR NESTOR TECHNOLOGIES

This deliverable has so far examined the broad legal parameters in which the NESTOR system will exist and that the partners will need to adhere to when designing, developing and implementing the NESTOR system. This section will build upon the previous sections, further exploring the legal, ethical and security considerations and implications of the individual technical components and how they link to the NESTOR system. As this deliverable is produced within the early stages of the project, it is possible that further needs for safeguards will arise as the technologies reach higher levels of maturity and that the prevailing legislation will continue to evolve. Partners should consider the need for further assessment of legal and ethical issues throughout the life span of the project, should this arise.

The high-level view of the NESTOR concept was presented in Figure 1: High-level view of the NESTOR concept

and demonstrates how NESTOR will bring together UxVs, sensors, RF and radar technology with online data, information fusion and visual analytics to support decision-making capabilities in both the command centre and for field agents such as LEAs and Border Guards. The purpose of Section 5.1 and Section 5.2 are to set out the legal and ethical considerations for the technology while Section 5.3 presents the overall security requirements for the system itself.

5.1 NESTOR ADVANCED DETECTION CAPABILITIES

The role of the advanced detection capabilities is to utilise state-of-the-art technology to enhance the detection of border-related events such as migrant smuggling, goods trafficking and potential incidents at sea that necessitate search and rescue (SAR). The advanced detection capabilities themselves link into European regulations on the need for border surveillance (as discussed in previous sections) but must also be mindful of potential concerns and the need for appropriate safeguards to ensure all aspects of monitoring are necessary and proportionate to the scope and scale of the threat and the possibility of collateral intrusion on law-abiding persons.

5.1.1 Use and application of object detection capabilities.

NESTOR will use several types of sensors to identify objects of interest within the territory under surveillance. The types of sensors will include video streams from visual and thermal cameras, both static and UxV-mounted, as well as 360^{o} cameras. Object detection usually applies computer vision, machine learning and artificial intelligence techniques such as deep learning to quickly and accurately detect salient objects in video and image data.

Object detection is a widely used tool across LEAs and border authorities. For example, one application is automatic number plate recognition (ANPR) used by police forces in the UK Europe. Ethical issues in what could be considered a relatively benign technology have previously been highlighted (such as profiling, transparency, and accountability) 36 and therefore it is important to consider a broad spectrum of potential impact of object detection

technologies and the methods by which the image data is obtained. In NESTOR, the key objects to be recognised are people, vehicles, aircraft such as drones, and water-based vessels through static and UxV-mounted cameras.

In the legal sense, the most important aspect is to consider data privacy when detecting people through automate means. NESTOR does not propose any facial detection or recognition capabilities; however, the capture of video streams and image could still contain identifiable persons. Therefore, appropriate safeguards for the capture, storage, processing, management and disposal of this data is necessary in accordance with the GDPR. The European Data Protection Supervisor (EDPS) has noted that "well-designed and selectively used video-surveillance systems are powerful tools for tackling data security issues; badly designed systems merely generate a false sense of security while also intruding on our individual privacy and infringing other fundamental rights."37 The EDPS has produced accompanying guideline[4] to support the design and installation of video surveillance systems that recommend use of encryption, masking technique to obscure identifiable persons who are not the data subject, using lower resolution images to make identification not possible, only monitoring set times, and considerations on the placement of cameras. Furthermore, the public must be informed about the video surveillance or if the surveillance is to be covert then it must be approved by the EDPS. It is also important to be aware of scope creep and monitor for potential expansion of the system into behaviour detection and note that use of thermal imaging requires a further impact assessment. Therefore, it is crucial that any video surveillance in NESTOR is robustly scrutinised and tested to ensure the proper respect for the principles of data protection.

The use of AI in the object detection also brings ethical considerations. While there are relatively few ethical concerns if a van is misclassified as a car or a motorcycle as a push bike, especially if there is a 'human-in-the-loop', when detecting the presence of people additional concerns must be addressed. It is well-known that the use of AI in computer vision activities potentially lead to discrimination based on protected characteristics such as race, ethnicity and gender as well as age,[5] therefore, appropriate mitigations must be put in place to ensure that training and testing data is representative and delivering high and consistent levels of accuracy across all characteristics. Furthermore, as the GDPR states that *"the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"* it is essential that the outputs of the object detection are not linked to automated decision-making.

While remote monitoring of border areas is necessary, and, as discussed in Section 3.3.1, the use of UAVs may even be legally recommended in future, for border surveillance, it is crucial

[4] EDPS (2010) The EDPS Video-Surveillance Guidelines. Available at: https://edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf

[5] Wang, Z., Qinami, K., Karakozis, I. C., Genova, K., Nair, P., Hata, K., & Russakovsky, O. (2020). Towards fairness in visual recognition: Effective strategies for bias mitigation. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 8919-8928).

that these privacy considerations are taken into account when developing and deploying UxVs. The EC has previously published a report on the ethical and privacy concerns, focusing specifically on aircraft 38, noting previous research that the privacy of location and space "encompasses the right of individuals to move in their "home" and other public or semi-public places without being identified, tracked or monitored."39

Further stages of object recognition may extend into various forms of activity recognition that, based on the fusion of data output from multiple sensors, highlight suspicious or unusual behaviour. Potential ethical concerns would be linked to how the system can distinguish between an object carrying out a legitimate task, and one which is acting suspiciously. This furthers need for having a human involved in the decision-making process and ensuring that automated alerts are based on specific activities: these are changes in speed, direction, being stationary or entering/heading towards pre-defined restricted zones. The system should only notify an operation of such behaviour and not automatically undertake any actions based on such activity.

5.1.2 Detection of unknown RF signals

NESTOR will utilise radio frequency (RF) sensors to detect RF devices in the border locale that may be an indicator of unusual border activity. The sensors will aim to provide metadata about the devices emitting the signals and any additional information such a location. Combined with the data provided by other sensors, this information could support the identification of smugglers/traffickers when supported by human analysis.

One of the key considerations for the detection of RF signals relates to the potential for collateral intrusion, and the privacy of individuals who are not the intended subject of the interception. Under Article 8 of the ECHR, any potential interference with an individual's right to respect for private and family life must only be done where absolutely necessary and proportionate. It is therefore important that the signals take all reasonable steps to ensure that individuals carrying out legitimate activities are not targeted by the RF sensors, for example, only extracting further information from an RF signal after it has been identified as coming from a suspicious activity. It is also crucial that any detected suspicious signals which consequently have data stored within the NESTOR system are subject to the GDPR principles, as outlined in Section 4, particularly surrounding data minimisation and storage limitation.

Legally, detecting RF signals could fall under the Directive on privacy and electronic communications 40 supported by the European Electronic Communications Code 41. Therefore, it will be important to consider scoping of the detection and the type of data collected remains within lawful activity.

5.1.3 Threat identification using radar scanning

NESTOR will apply radar scanning to conduct high-performance coastal surveillance to automatically detect sea, ground and low-flying air targets. The outputs of the scanning will be fused with other sensor data to support border surveillance activities.

As with a number of the other technological components of NESTOR, the main ethical considerations are surrounding the privacy of data that could be collected and processed by

radar scanning. While the radar system itself does not capture personally identifiable information, this information may then be combined with other types of data within the NESTOR system to lead to identification. For this reason, it is important that the system operates a privacy-by-design/default approach (to be discussed in Section 5.3), as well as implementing a proper data security architecture and data management system. It is critical that measures are put in place to avoid leakage or misuse of data 44. Partners must be aware that non-personal data can easily become personal data when combined with other information.

Further considerations specific to the use of radars include the potential for the radars to detect objects as 'illegitimate' and flag them as such to the authorities, when the objects actually have a legitimate reason for being in that space. This again highlights the importance of having a human-in-the-loop and restrictions on automated decision-making (ADM) within the system as well as clear parameters for what is detected and how that information is interpreted within the NESTOR system.

In an operational capacity users should be aware when conducting search and rescue missions of the European Convention on Human Rights (ECHR) 45 right to life under Article 2. This places an obligation on those who may see a person who appears to be in distress to detect and rescue them where possible. Should a radar detect such an instance, capabilities should be in place to alert the relevant authorities in order to rescue the person(s).

5.1.4 Online information monitoring

NESTOR will use online information monitoring to identify content related to illegal border activities, including suspicious posts online about the sale of illegal goods, potential trafficking routes, and any potentially relevant information posted by bystanders. Information sources may include social media, forums, specific surface and deep web sites relating to the issues faced in border security, as well as those sites on the dark web.

The issues surrounding the legality and ethics of data collection from the web are still a grey area 46. The most prevalent legal consideration is the presence of personal data in the extracted information. Section 4 details the conditions imposed by the GDPR when it comes to collecting and processing personal data in the EU. While it is always preferable to get consent from the data subject when collecting personal data, in most cases relating to NESTOR's acquisition of data, this would be either unfeasible due to the vast amount of data to be collected or would alert the data subject who may pose a threat to border security. As with any data collection of this type online, there is a possibility of collateral intrusion; however, collection processes should strive to implement anonymisation or pseudonymisation procedures to limit personal data processing. To ensure that risks are identified and mitigated throughout the data acquisition process, a data protection impact assessment (DPIA) should be conducted prior to any data collection activities.[6] The DPIA

[6] See Article 35, GDPR for requirements of a DPIA.

should ensure the minimum amount of data necessary should be collected and any data which is not required is deleted in line with the GDPR storage limitation principle in Article 5.

Alongside this is the potential legal concern of scraping information which is copyrighted. Much of the information found on websites is subject to copyright restrictions and by downloading such information this may result in the infringement of copyright, depending on how this information is subsequently used. In 2019, the EU enacted the Copyright Directive (Directive (EU) 2019/790) 47 which sets out the EU's commitment to modernising the rules on copyright online. Of relevance to NESTOR is Article 3 that provides an exception for research organisations to carry out, for the purposes of scientific research, text and data mining of works or other subject matter to which they have lawful access. This, however, would only be applicable, for the online data acquisition throughout the lifetime of the NESTOR project and not for operational use.

A further legal consideration for the use of web and social media monitoring under NESTOR is the need to adhere to the website terms of service. Most websites and social media platforms require users to sign up in order to access the data, which may impose restrictions on who can use the data and for what purpose, and the amount of data which can be retrieved. Therefore, when acquiring data, it is important that the terms of service are fully understood.

While there are extensive legal frameworks in place for addressing the legal concerns with web crawling, the ethical issues have historically received more limited attention 50. The main ethical concern, which links closely with the legal considerations, is that of data privacy relating to the data subject. The need for compliance with the GDPR is detailed at length in Section 4, which sets out how partners must comply with the regulations to limit the intrusion to the data subject.

A further consideration that should be considered with this type of process is the potential for unexpectedly acquiring data from the dark web which is illegal 51. Should any illegal data be identified using the NESTOR systems, this should be reported as soon as possible using the appropriate legal channels. Care should also be taken to ensure the mental wellbeing of those viewing the illegal content and potentially the victims of the crime 3352.

5.1.5 Key Considerations

For NESTOR's advanced detection capabilities the following legal and ethical considerations have been identified and should be addressed within the development and testing phases prior to any future operational deployment.

1. Monitor for the capture of personal data in video and image streams especially from UAVs and limit the resolution to prevent persons being identified if this is not a required functionality.

2. Be aware of the potential for scope creep in the categories objects and types of threats detected especially with regard to the interpretation of legitimate vs. illegitimate activities and that the output does not feed into any automated decision-making processes.

3. Ensure the use of representative datasets for training data and put in place procedures to effectively monitor the accuracy of any AI models.

4. Beware of collateral intrusions for all aspects of data collection (image, RF, radar and online) and take all necessary steps to target data collection activities to a specific purpose.

5. Consider potential legal implications of detecting metadata and other content through RF signal detection and ensure the activity complies with all privacy and electronic communication legislation.

6. Ensure all online information monitoring and extraction is appropriately targeted based on existing intelligence.

7. Implement anonymisation or pseudonymisation procedures to limit the collection and processing of personal data related to online activity. The need for a DPIA may be necessary.

8. Consider the terms of service and the robots.txt instructions of the webpage or social media site and ensure all data extraction is in compliance and appropriately justified.

LER-013	Restrict the acquisition of facial data when processing image and video streams
LER-014	Train detection algorithms on representative datasets and ensure activity recognition detects factual activities
LER-015	Perform target online and social media monitoring and have safeguards to prevent collateral intrusion and respect terms of service

5.2 NESTOR SITUATIONAL AWARENESS

NESTOR brings together a range of technologies to support better situational awareness within the border surveillance environment. In particular, this involves the development of command-and-control functionalities that can be deployed in an operations centre as well as to field agents as necessary. Better situational awareness can also support further targeted information collection activities optimising the use of autonomous vehicles.

5.2.1 Use of mixed reality headsets for field and training operations

NESTOR will utilise augmented reality (AR) headsets for users to consume and visualise data and video streams in near-real time, improving the situational awareness and tactical assets during training and operations.

If the AR headsets are to use GPS, microphones and cameras, and record other input data from the user, then this data is likely to be subject to GDPR and consequently require strict regulations on capture, processing, storage and disposal. If personal data from the wearer is collected this should utilise informed consent as the legal basis for processing and if the headset is capable of monitoring biometric or other sensitive personal data from the wearer, then further obligations in line with Article 9 of the GDPR should also be adhered to.

There are also further ethical concerns to consider for the wearer of the headset. AR can induce a form of cybersickness on the user due to various factors including latency, restricted fields of view, as well as poor fitting. Similarly, wearing the headset for a prolonged period of time may also cause headaches and eyestrain 51. Therefore, it is not only the technical implementation that is an important consideration for the use of AR headsets but also the health and safety of the wearer must also be adequately accounted for.

As with other components of the NESTOR system, the data that is gathered from this may be combined with other pieces of personal data and pose a potential risk to the data subject. It can be particularly risky when an AR system is able to run simultaneously with other applications, or using specific user login details, meaning that the voice or camera input could be compromised and used in a malicious way 52. Partners should ensure that all GDPR principles are adhered to, and the transfer of personal data for display is limited to that is absolutely necessary and appropriate security protocols are in place.

5.2.2 Coordinated use of multiple UxVs

NESTOR will use an AI-support service to coordinate multiple UxVs to cooperatively cover large off-shore areas. The aim of this service is to define, calculate and provide a set of waypoint coordinates for the unmanned vehicles used in surveillance activities, in the context of missions with different objectives.

The key considerations surrounding the flight of unmanned vehicles are detailed in Section 5.1.1, therefore, this section only deals with the AI tool assisting mission planning of those vehicles. The main consideration when deploying any automated system is the procedures put in place for monitoring its effective operation. In NESTOR the automated decision is limited to optimising the routes of the UxVs to maximise the coverage of a predefined area. It is proposed that the NESTOR system provides interfaces for operator to oversee and authorise the missions.

5.2.3 Data fusion across multiple data streams

The main function of this component will be to process and fuse detection information the data streams discussed above to allow for various alerts that could be indicative of potential suspicious activities at the border crossing. Some of these alerting methods may rely on AI-based functionality to optimise the alerts and learn from historical data.

As with any development of AI-based technology, there are several legal and ethical areas to be considered to ensure the implementation of trustworthy AI and future compliance with the artificial intelligence act.

For an AI system to be deemed accountable, there needs to be a degree of transparency. The EU Ethics Guidelines for Trustworthy AI 4 states that processes need to be transparent, with the workings of the AI system being openly communicated and decisions being, as far as possible, explainable. This does not necessarily mean that this information should be public but that it should stand up to scrutiny if required by public bodies or institutions. This can be achieved by following the Ethics Guidelines for Trustworthy AI go into greater detail as to how systems can meet the transparency requirements for ethical AI, stating that *“the data sets and*

the processes that yield the AI system's decision, including those of data gathering and data labelling as well as the algorithms used, should be documented to the best possible standard to allow for traceability and an increase in transparency." Furthermore, human oversight should also be maintained to provide assurance that any AI system does not undermine human autonomy or cause other adverse effects, with the European Commission 53 stating that where less oversight is possible, more extensive testing and stricter governance is required.

5.2.4 Visual analytics and decision support

NESTOR will use a visual analytics dashboard as part of the command and control interface to provide a space represent the data in the system. This dashboard will include information from the different sensor inputs, alerts, and time-based geospatial visualisations of missions and other extracted data. The dashboard will support human-in-the-loop decision making across all aspects of the NESTOR system.

A key ethical consideration in the development of visual analytics and dashboard functionalities is to realise that the presentation of information is not objective in and of itself. Therefore, the design decisions made in terms of how information in presented, through which types of charts, maps and other visual mediums as well as the ease of access to different types of data within the system all impact on how the user interacts with the system and how they understand these data in context may all impact on the decisions they go on to make 54. Given this, the user experience and the visual presentation of information must be appropriately tested to ensure that information is being interpreted as intended by the designer and that important information is not being obscured from the user. This can, in part, be also achieved through user training as well as embedded information in the dashboard itself.

Another perspective is to also ensure that existing visual paradigms are respected and match with how they are presented in other systems so as to not lead to conflict. User acceptance testing can also support this activity to allow all feedback to be incorporated prior to the deployment stage.

5.2.5 Key considerations

The development of a holistic situational awareness picture is necessary to fully evaluate the border security situation and maintain effective situational awareness. The use of technology to achieve and present that information is essential. Within NESTOR the following legal and ethical considerations should be taken into account in support of situational awareness.

1. Monitor the use of augmented reality headsets including health and safety aspects for the wearer.
2. Ensure informed consent and details of processing are provided if personal data is captured from the headset wearer.

3. Restrict AI applications for UxV coordination to mission and route planning and provide appropriate interfaces to ensure human-in-the-loop monitoring of UxV activity during operation.

4. Conduct detailed impact assessments if further autonomous coordination between UxVs is to be developed considering both AI and data privacy aspects.

5. Ensure a balance between the neutral presentation of information and drawing attention to alerts needing attention by the dashboard users

6. Respect existing visual paradigms in the visualisation of information so that interpretation is consistent across systems.

These can be represented in the following legal and ethical requirements:

LER-016	Provide health and safety training and monitoring for wearers of AR headsets
LER-017	Provide neutral and accurate data representations through visual interfaces
LER-018	Ensure a human-in-the-loop approach is applied to all automated data processing activities

5.3 SECURITY REQUIREMENTS

As a potentially mission critical system and, ultimately a system that could be vulnerable to both data breaches and cyber-attacks, it is crucial that the overall security requirements of the system are incorporated into system design from the outset following security and privacy by design principles. This also includes the design and implementation of the technical measures (under Article 32 - Security of Processing, of the GDPR) required for the protection of personal data within the system.

5.3.1 User authorisation

Only authorised users of the NESTOR system should have access to the data and its various applications. Due to nature and sensitivity of the data within the system, there is the potential for a major security breach should an unauthorised individual gain access to the system. The key to ensuring only authorised access is granted is using multifactor authentication methods. This will create a double layer of security access for any potential unauthorised individuals to get through. It is also important that any individual who tries to access the system and is denied, is only given the minimum required information from rejected API requests. Furthermore, communication between components should also be authorised through appropriate means.

Alongside this, the implementation of an access control layer utilising role-based access control (RBAC) to limit access to individual parts of the system. This ensures that only those parts of the system which need to be accessed by an individual are open. This should be further backed up by administrative mechanisms, which are important to the management of privileges and roles within the system. Any individual who requires access to the system

should only be provided with access to those areas based on their role not individual requirements. This will mitigate any potential breaches of data from authorised users.

To add an extra layer of protection, and to make sure that access privileges are kept up to date, authorisation tokens used by the system should have an expiry data limiting the time that they can be used to access the system. Regular audits of access should also be conducted to further support this.

5.3.2 Utilisation of hashing and logging for auditability

While the creation of log files can do little to prevent a security incident they can support the flagging, investigation, resolution of an incident as if discovered. It is critical that log files are incorporated to enable full traceability and recording of actions and information that has been accessed by all users and components during the system's operation.

By ensuring a logging procedure is in place, it will help mitigate against the risk of unauthorised persons gaining access, but also the possibility of an authorised individual acting in a manner they should not. This may include attempting to access a part of the system they are not authorised to or downloading data from the system. The system should have mechanisms in monitor authorised users and provide flags or alerts if unusual patterns of access are attempted prevent security breaches and support the proper functioning of the system.

The hashing and signing of content can also support the traceability mechanisms verifying the data provenance and ensuring that data cannot be altered or tampered with without a clear record being included in the system. Activities within the system should always be linked to a user or a module to further support auditability.

5.3.3 Privacy-by-design and default

For NESTOR to adhere to all GDPR principles and ensure the privacy and security of collected personal or sensitive data, partners should implement a privacy-by-design/default approach when developing the technologies. By implementing privacy principles early within the design and development stages, this can support the delivery of responsible innovation 55. NESTOR partners should take the necessary steps to ensure the development of strong security to safeguard the confidentiality, integrity and availability of data within the system.

To enable the protection of personal or sensitive data, the system should implement mechanisms to protect the identity of those who own the data, and the information contained within. This may include encryption and anonymisation/pseudonymisation. An example of how data can be protected from unauthorised access, even from those who have limited access within the system, could be the blurring of text or images on the main screen, with additional authentication measures needed to access the full content.

The GDPR, through Article 25, mandates the application of 'data protection by design and by default. This is, in essence, the successor the privacy-by-design and sets out the requirements that data protection principles must be considered from the outset of any technology development that includes personal data. Specifically, it is important that the 'data minimisation' principle of GDPR (as outlined in Section 4.1) is fully adhered to, with measures

incorporated into the design and development of the system to ensure this is a core value of NESTOR. This may include mechanisms which flag up the inclusion of potentially unnecessary data. Alongside this, to protect any personal or sensitive data which is stored within the system, partners should adhere to the 'storage limitation' principle under the GDPR (as outlined in Section 4.1). This will ensure that any data is preserved for only the period of time which it is deemed necessary, with the system either automatically removing data which exceeds time limits or providing a notification to the data controller that such limits have been reached.

5.3.4 Protection of the NESTOR system

With the use of any system which processes data, there is the risk of it being subject to an attack, whether malicious or accidental. Examples of such risks include theft of the data by a person with authorised access, data being viewed by an unauthorised person, hackers targeting the system, or damage to the server which holds the data. While these risks all take different forms, the preventative mechanisms are predominately the same and should be considered by partners to prevent any security breaches occurring within the NESTOR system. A new threat is the use of adversarial AI whereby as understanding of the AI systems implemented grows the opportunity for bad actors to try to trick or circumvent AI also increase and therefore the design of AI systems should be robust to such attacks.

One of the key considerations, as mentioned in Section 5.3.3, is the need for encryption and anonymisation/pseudonymisation of data. The inclusion of this where personal or sensitive data may be present will mitigate the potential for a data subject to be identifiable, should the data be taken from the system somehow. It is also crucial that all data held within the system is backed up in the server/cloud server, which would ensure that should any loss of data occur, there is sufficient mechanisms in place to retrieve it.

Finally, secure-by-design principles 56 will be applied. They focus on the five main principles of establishing the context and fundamentals of the system being developed, making compromise difficult, making disruption difficult, making compromise detection easier and reducing the impact of compromise. As it can be seen, they clearly link into the efforts made to ensure privacy by design to increase the security of the whole system.

Specific security requirements are already set out in D2.1 and are summarised with the following considerations. Principles should as confidentiality, integrity and availability should always apply with regular and encrypted backups and system logs of user actions compatible with the storage limitation principle of GDPR and protected against cyberattacks. The system should only be accessible to registered users and user accounts should use role-based privileges utilising multifactor authentication methods.

6. PILOT SPECIFIC CONSIDERATIONS

The NESTOR project involves several European member states that will be involved within the Pilot Use Cases (PUCs) The PUCs are an opportunity to test how the NESTOR system may operate in a real-life scenario. As well as the technology, it is also important to consider the

specifics of these situations to understand how legal, ethical and security considerations may also need to be taken into account. The laws of each country will be similar due to the European Union law; however, sections can alter when regarding maritime considerations; and understanding the implications of the Schengen border control and respecting the Cypriot border specifically.

The NESTOR analysis of the PUCs also provides a test scenario to identify any further requirements that could evolve from these cases. The countries involved in the piloting are: Lithuania, Cyprus, Greece and Bulgaria; and the types of scenarios trafficking of illicit goods through maritime routes, a maritime search and rescue scenario, and a combined human trafficking and search and rescue scenario that incorporates both maritime and land border aspects. The benefit of carrying out this analysis is to demonstrate the additional aspects that would need to be considered if the system was to be deployed operationally.

6.1 LITHUANIA – LITHUANIAN MARITIME TRIAL

Lithuania has been a member of the European Union since the 1st of May 2004 which means that EU law has been transposed into the Lithuanian national law. The trial considers the maritime area near to the Russian border and focuses on the import of illicit goods via the maritime route into the country and ultimately into the EU.

The trial will utilise many of the proposed components within the NESTOR system including the sensors, RF-monitoring, use of UxVs (aerial and underwater) and the command-and-control centre. This PUC will be performed to find results regarding the protection of borders from illegally trafficked illicit goods. This section will detail the maritime law and aviation laws of the drones used within this specific maritime trial.

Maritime Considerations:

The location trial takes place at a main port in Lithuania. As discussed in Section 3.3.2 above, the applicable maritime law is UNCLOS, however, several further agreements have been made with neighbouring countries, namely Russia and Sweden, to set out the delineation of the baselines of Exclusive Economic Zone (EEZ) and the continental shelf 58. The 'Republic of Lithuania Law on Maritime Safety 1897' last amended in 2000 59 provides country specific legislation on the applicable maritime law of the country including that for Lithuanian Flag carrying ships as well as enacting several EU laws on maritime safety. This trial is focused on the area within the territorial sea of Lithuania; therefore, international waters and airspace are out of scope of this scenario.

As an extension of the maritime considerations, due to the focus on the trafficking of illicit goods, other relevant national laws include those setting out the responsibilities of the state border guard 60 including limitations on vessels in the territorial sea and combatting illegal trade through the sea (and land) borders.

Aviation Considerations

The Lithuanian PUC will utilise UAVs and therefore must adhere to the airspace laws of Lithuania. Lithuania's UAV laws are set out by the Lithuanian Civil Aviation Administration 61 and European Union's *Regulation 2019/947 on the rules and procedures for the operation of unmanned aircraft* 27 (as discussed in Section 3.3.3 above). This therefore places them under the requirements of this regulation which determine the legislation relating to the usage and operation of UAVs. The EU regulation state that a UAV must follow the following rules and therefore NESTOR must also apply these rules to be compatible and compliant with the prevailing legislation.

NESTOR will utilise small commercial UAVs and any UAV operator must acquire the appropriate licenses including a National Drone Pilot Certificate. Specific guidance in Lithuania requires that

> "*Drones must be kept a minimum of 50 meters (164 feet) from all vehicles, buildings, people, crowds, and places of worship.*"62

Therefore, this should be directly factors into any testing and ultimately deployment of the system.

Data Protection

The GDPR is transposed into Lithuanian national law through the Law on Legal Protection of Personal Data No. XIII-1426 63. There are few derogations in the national law that would affect data processing within NESTOR; however, it should be noted that if video data is captured and processed in the workplace employees must be notified. In NESTOR, this could be applicable if border guards (for example) are captured on video during the daily activities from the cameras used in the system or through the use of the Augmented Reality (AR) headsets 64.

Ethical Considerations

Ethical considerations in this use case mainly relate to factors relevant to illicit goods trafficking and management of the discovery of such consignments. In particular, organised crime groups may exploit those who a bringing goods across the border, therefore, if persons are identified it is possible that they are victims rather than criminals.

6.2 CYPRUS – SEARCH AND RESCUE OPERATIONS

The country of Cyprus is a member of the European Union EU Law as of the 1st of May 2004 in the same accession as Lithuania, however, is 'suspended in areas where the Cypriot government does not exercise effective control' 65. NESTOR's focus is the areas of Republic of Cyprus on the southern side of the island in the case of a Search and Rescue (SAR) operation. The application of NESTOR for SAR operations will make use of the cameras, sensors and autonomous vehicles for data collection and ingest and analyse them within the NESTOR system to provide decision support.

Maritime Considerations

Cyprus has been a member of the European Union since 2004, therefore, we can refer to the appropriate considerations that are detailed within the UNCLOS. Maritime law in Cyprus developed from the British Empire rule from 1878 until 1960 when the country declared independence – the laws created after the declaration of Independence within Cyprus are inherited from this previous rule. Cyprus has amended the British Merchant Act 1894 to ensure compliancy with their new legislative background *Merchant Shipping (Masters and Seamen) Laws 1963-2002* and *the Merchant Shipping (Fees and Taxing Provisions) Law of 2010* are alterations of this act plus the Cypriot edit of the UK Companies Act 1948; Cyprus utilizes Chapter 113 of the Statute Laws of Cyprus. This statute determines how shipping law interacts with Cyprus after being under British Empire Rule 66.

The set area for the PUC is within the territorial sea of Cyprus; and must remain within the waters of Cyprus to avoid entering international waters. Furthermore, operators should be aware of the disputes regarding the recognition of Cyprus' territorial sea67 . Consequently, Cyprus is yet to join the Schengen area due to these disputes68 .

Aviation Considerations

The aviation considerations 69 in Cyprus also make use of European UAV laws as highlighted in Section 3.3.3 UAVs cannot be flown within the vicinity of infrastructure or historical sites. Figure 3 highlights the restrictive areas upon which UAVs are unable to fly as per the European Union Aviation Safety Agency (EASA) due to airport restrictions. Specifically, UAVs must remain at least 8km away from any airport 70 at all times.

Figure 5 - Areas of no-drone flight within Cyprus

Cyprus set out specific requirements for professional drone operations based on national legislation including the Civil Aviation Act 71 and national decrees. Cyprus has also set up a specific guidance website for the operation of UAVs 72 but specific considerations for professional drone operations include abiding by the previously described laws, registration of the UAV and acquisition of a permit to fly, possess 3rd party liability insurance and have a drone pilot certificate. Further requirements may apply if the drone weighs over 25kg 73.

Data Protection

Cyprus implements the GDPR through transposition into its own national law 74. Cyprus does not implement significant derogations that are directly relevant to NESTOR; however, the use of video surveillance in the workplace is mentioned (similar to Lithuania) which could be applicable to NESTOR depending on the capture of border guards from cameras as part of the border surveillance capabilities 75.

6.3 GREECE - BULGARIA – WIDE AREA MONITORING FOR HUMAN TRAFFICKING AND IRREGULAR MIGRATION

The final pilot use case focuses on the use of Greece and Bulgaria as potential trafficking and irregular migrations routes into Europe by those coming from non-EU countries. The geography of this border means that there is significant land and sea areas to cover. Furthermore, the scenario extends to consider search and rescue applications due to the unfortunate possibility that boats bringing people into Europe by sea are not safe and the persons aboard may require rescue.

Greece and Bulgaria are both members of the European Union, Greece joined the EU in 1981 76 – with Bulgaria joining in 2007 77. Both countries have therefore transposed EU regulations into national law – such as for data protection and civil aviation. However, Bulgaria is yet to join the Schengen area although surrounding Schengen border countries allow a 'bilateral agreement that allow a free-visa travel.' 78

Maritime Considerations

The Maritime Law of Greece and Bulgaria is controlled by the UNCLOS and the proposed use of the NESTOR system applies within the territorial sea of Greece; therefore, this does extend to international waters that surround Greece. The Maritime Law within Greece is controlled by country convention which has been enacted within Greece; these are the following:

1. the Convention for the Unification of Certain Rules of Law with respect to Collisions between Vessels 1910 (the Collision Convention 1910);
2. the Protocol to amend the International Convention for the Unification of Certain Rules of Law Relating to Bills of Lading 1968 (the Hague-Visby Rules);
3. the International Convention on Salvage 1989 (the 1989 Salvage Convention);
4. the International Convention Relating to the Arrest of Sea-Going Ships 1952 (the arrest Convention 1952);
5. the Athens Convention on the Carriage of Passengers and their Luggage by Sea 1974(the Athens Convention); and
6. the Convention on Limitation of Liability for Maritime Claims 1976 (the LLMC Convention 1976) (including the Protocol to amend the LLMC Convention 1996(the LLMC Protocol 1996))) 79

Each piece of convention enacted with Greece has a specific power and ability to limit or control the shipping industry. The requirements of the NESTOR project should understand the powers presented within these acts and the "Code of Public Maritime Law" 80 and the "Code of Private Maritime Law" 81 can constitute the actions of vessels unless superseded in articles a-f 82 which are the ratified conventions. The coastal area of Bulgaria is not part of this PUC.

The NESTOR project will ensure that the requirements of international conventions and Greek Law will not be violated or infringed upon in any manner. The NESTOR project aims to respect all laws that are set by the country that the pilot use case takes place within.

Aviation Considerations

Aviation Considerations within this PUC will be required to adhere to both the Hellenic requirements of Drone utilization and the Bulgarian regulations. Regulations 2019/945 and Regulations 2019/947 will still hold grounds within both countries due to the European Union Membership, therefore, the specific legislation of the country for registration and licensing is the more prominent consideration for the NESTOR consortium.

The Hellenic Civil Aviation Authority (HCAA) determines the rules of UAS within Greece; there is a requirement for:

1. "Remote Pilot certificate of competency
2. UAS operator/owner registration.
    1. Unless a drone:
        1. Weighs less than 250g and has no camera or other sensor able to detect personal data; or
        2. Even with a camera or other sensor, weighs less than 250g, but is a toy (this means that its documentation shows that it complies with 'toy' (Directive 2009/48/EC);
3. Insurance
    1. Professional Use: All Drones
    2. Recreational: Drones with a Minimal Take-off Mass (MTOM) or greater than 4kg" 82

The NESTOR project will ensure the compliancy of these requirements of the HCAA plus prior approval to the deployment of such technology within the area of operations. Information regarding the requirements of drones through the European Union can be found within Section 3.3.3; these are requirements that are required for the functionates within Greece and the rest of the European Union.

Bulgarian UAV Law has similar requirements of Greece, the Directorate General of Civil Aviation Administration (DGCAA) are the organization that are responsible for enforcing the regulations that are produced by the European Union. Due this specific PUC involving a cross border operation; Greece and Bulgaria, it is the requirement of "the UAS operator shall provide the DG CAA with an application" 83 with regards to Article 12 of Regulation 2019/947. Upon the approval of this application the NESTOR project; with respect to the EU Laws and functions that are stated in statute, has the right to proceed with this trial on an Aviation Level.

7. CONCLUSIONS

In this deliverable we have reviewed the main EU legal frameworks that will apply to the development and operation of the NESTOR system, alongside the specific legislation which will be applicable to the individual pilot countries and scenarios. The intention is for this document to act as a guideline for the partners who are developing the NESTOR system, and those who intend to use it, to ensure adherence with the relevant laws. Also set out, are the legal and ethical considerations which may arise for each individual technical component of the system. While all efforts have been made to address the main issues, partners may find that as the project reaches a higher level of maturity there are further concerns which need to be addressed. Should this occur, guidance should be sought from the relevant legal and ethical partners to ensure the system remains in line with the legal standards. The security requirements which should be implemented within the NESTOR system have also been addressed, to ensure that the system keeps security and data privacy at the forefront of the project landscape.

The present report is closely related to D2.1 *Use cases and requirements for the innovative technologies*. The legal and security requirements constitute part of the NESTOR end-user requirements as they have been described and classified in D2.1. Due to their nature (stipulated by law), they are labelled as “Must-have” requirements. To ensure that the NESTOR system will operate in compliance with the legal and security requirements included herein, the content of this deliverable will be presented to the Consortium and relevant discussion with the technical partners and the end users will take place during the 2nd Project Meeting in May 2022.

8. REFERENCES

1. Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC. Available at: http://data.europa.eu/eli/reg/2016/1624/oj
2. Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624. Available at: http://data.europa.eu/eli/reg/2019/1896/oj
3. Gotterbarn, D. W., Brinkman, B., Flick, C., Kirkpatrick, M. S., Miller, K., Vazansky, K., & Wolf, M. J. (2018). ACM code of ethics and professional conduct. Available at: https://www.acm.org/code-of-ethics
4. High-Level Expert Group on Artificial Intelligence, (2019). 'Ethics Guidelines for Trustworthy AI'. European Commission. Available at: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1
5. Frontex (2011), Ethics of Border Security, Centre for Global Ethics of the University of Birmingham (UK), Frontex/64/2010, 29 April 2011. Available at: https://frontex.europa.eu/assets/Publications/Research/Ethics_of_Border_Security_Report.pdf
6. E. E. Joh (2017) Artificial intelligence and policing: First questions. Seattle UL Rev., vol. 41, pp. 1139-1144.
7. Frontex. (2021). Artificial Intelligence-Based Capabilities for the European Border and Coast Guard: Final Report. RAND Europe. https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf
8. European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe, Brussels, COM(2018) 237 final, 2018.
9. Consolidated version of the Treaty on European Union. Official Journal C 326, 26/10/2012 P. 0001 – 0390. Available at: http://data.europa.eu/eli/treaty/teu_2012/oj
10. European Union (1984) Draft Treaty of the Establishment of the European Union available at: https://www.europarl.europa.eu/RegData/etudes/fiches_techniques/2013/010106/04A_FT(2013)010106_EN.html
11. European Union Agency for Fundamental Rights (2021) "What are Fundamental Rights" retrieved from https://fra.europa.eu/en/about-fundamental-rights
12. EUFRA (2020) Handbook: Applying the Charter of Fundamental Rights of the European Union in law and policy making at a national level. European Union Agency

for Fundamental Rights. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-charter-guidance_en.pdf

13. European Union (2021) "The European Union Charter on Fundamental Rights" retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf
14. ECHR (2022) Factsheet on Human Trafficking. European Court of Human Rights (ECHR). Available at: https://www.echr.coe.int/Documents/FS_Trafficking_ENG.pdf
15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/E (General Data Protection Regulation)
16. Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code). Available at: http://data.europa.eu/eli/reg/2016/399/oj
17. Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code). Available at: http://data.europa.eu/eli/reg/2016/399/oj
18. Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code). Available at: http://data.europa.eu/eli/reg/2016/399/oj
19. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 on a Union Code on the rules governing the movement of persons across borders (COM/2021/891 final). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0891&from=EN
20. European Commission (n. d.) Effective management of external borders. Migration and Home Affairs. Available at: https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/effective-management-external-borders_en
21. European Commission (n. d.) EUROSUR. Migration and Home Affairs. Available at: https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/border-crossing/eurosur_en
22. UN General Assembly (1982) Convention on the Law of the Sea (UNCLOS). Available at: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
23. Commission Implementing Regulation (EU) 2021/581 of 9 April 2021 on the situational pictures of the European Border Surveillance System (EUROSUR). Available at: http://data.europa.eu/eli/reg_impl/2021/581/oj
24. European Maritime Safety Agency (2022) Common Information Sharing Environment (CISE). Available at: http://www.emsa.europa.eu/cise.html

25. IMO (1985) International Convention on Maritime Search and Rescue (SAR). International Maritime Organisation. Available at: https://www.imo.org/en/About/Conventions/Pages/International-Convention-on-Maritime-Search-and-Rescue-(SAR).aspx
26. Regulation (EU) No 656/2014 of the European Parliament and of the Council of 15 May 2014 establishing rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. Available at: http://data.europa.eu/eli/reg/2014/656/oj
27. European Union (2020) Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance). Available at: http://data.europa.eu/eli/reg_impl/2019/947/oj
28. Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. Available at: http://data.europa.eu/eli/reg_del/2019/945/oj
29. European Aviation Safety Agency (n. d.) Civil drones (unmanned aircraft). Available at: https://www.easa.europa.eu/domains/civil-drones
30. European Commission (n. d.) Key enabling technologies. Available at: https://ec.europa.eu/info/research-and-innovation/research-area/industrial-research-and-innovation/key-enabling-technologies_en
31. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Official Journal L119 4 May 2016. Available at: http://data.europa.eu/eli/reg/2016/679/oj
32. European Commission (2022) A European approach to artificial intelligence. Available at: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
33. High-level expert group on Artificial Intelligence (2019) Ethics guidelines for trustworthy AI. European Commission. Archived version available at: https://wayback.archive-it.org/12090/20201227221227/https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
34. Proposal for a Regulation of The European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
35. Akhgar, B. et al. (2022) AP4AI Framework Blueprint. Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain. Available at: https://ap4ai.eu/sites/default/files/2022-03/AP4AI_Framework_Blueprint_22Feb2022.pdf
36. Adams, D. (2019). Driving Ethics Forward: The Importance of Considering the Ethics of Automatic Number Plate Recognition (ANPR) - Surveillance Camera

Commissioner's Office. Available at: https://videosurveillance.blog.gov.uk/2019/02/15/driving-ethics-forward-the-importance-of-considering-the-ethics-of-automatic-number-plate-recognition-anpr/

37. European Data Protection Supervisor (n.d) Video-surveillance https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en
38. EDPS (2010) The EDPS Video-Surveillance Guidelines. Available at: https://edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf
39. Wang, Z., Qinami, K., Karakozis, I. C., Genova, K., Nair, P., Hata, K., & Russakovsky, O. (2020). Towards fairness in visual recognition: Effective strategies for bias mitigation. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 8919-8928).
40. European Commission, Directorate-General for Enterprise and Industry, Wright, D., Finn, R., De Hert, P., et al. (2015) Study on privacy, data protection and ethical risks in civil remotely piloted aircraft : final report, Publications Office. Available at: https://op.europa.eu/en/publication-detail/-/publication/6b277634-4af3-48a7-b3e9-0ca31f7480ce
41. Finn, Rachel L., David Wright, and Michael Friedewald, "Seven types of Privacy", in Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (Eds.), European Data Protection: Coming of Age, Springer, Dordrecht, 2013, pp. 4-5
42. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Available at: http://data.europa.eu/eli/dir/2002/58/oj
43. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance. Available at: http://data.europa.eu/eli/dir/2018/1972/oj
44. Karagiannidis, L. et al. (2019). RANGER: radars and early warning technologies for long distance maritime surveillance. 1st Maritime Situational Awareness Workshop. NATO.
45. Council of Europe (1953) Details of Treaty No.005 Convention for the Protection of Human Rights and Fundamental Freedoms. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005
46. Snell, J., & Menaldo, N. (2016). Web scraping in an era of big data 2.0. Bloomberg Law News. Available at: https://news.bloomberglaw.com/tech-and-telecom-law/web-scraping-in-an-era-of-big-data-20
47. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market (the "Copyright Directive") Available at: https://eur-lex.europa.eu/eli/dir/2019/790/oj
48. Krotov, V. and Silva, L. (2018). Legality and ethics of web scraping. Twenty-fourth Americas Conference on Information Systems. New Orleans.

49. Gercke, M. (2021). Ethical and Societal Issues of Automated Dark Web Investigation: Part 4. In Dark Web Investigation (pp. 169-187). Springer, Cham
50. Bosco, F., Vermeersch, E., Luda, V., Vacigago, U.G., and Lyle, A. (2016). 'Non-discrimination and Protection of Fundamental Rights in Cybercrime and Cyberterrorism Research.' In: Akhgar, B., and Brewster, B. (eds). Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities. London: Springer. pp. 97-115.
51. Hughes, C. L., Fidopiastis, C., Stanney, K. M., Bailey, P. S., & Ruiz, E. (2020). The psychometrics of cybersickness in augmented reality. Frontiers in Virtual Reality, 1, 34.
52. McFarlane, G (2017) Virtual and augmented reality: what are the legal issues? Eversheds Sutherland. Available at: https://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/tmt/Virtual_and_augmented_reality_what_are_the_legal_issues
53. European Commission, (2019). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Building trust in human-centric artificial intelligence. Available at: https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence
54. Correll, M. (2019). Ethical dimensions of visualization research. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-13).
55. Cavoukian, A. and Jonas, J. (2012). Privacy and Design in the Age of Big Data. Colorado: Information and Privacy Commissioner.
56. National Cyber Security Centre (2019) Secure by Design Principles. Available at: https://www.ncsc.gov.uk/collection/cyber-security-design-principles
57. UN General Assembley (1982) Convention on the Law of the Sea (UNCLOS). Available at: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
58. United Nations (2021) Lithuania -Laws of the Sea – Legislation and Treaties. Available at: https://www.un.org/depts/los/LEGISLATIONANDTREATIES/STATEFILES/LTU.htm
59. Republic of Lithuania Law amending the Law on Maritime Safety. 29 August 2000. Available at: https://e-seimas.lrs.lt/rs/legalact/TAD/TAIS.275300/
60. Republic of Lithuania Law on the State Border and the Guard Thereof. 23 November 2010. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/7b13b1228c7111e6a0f68fd135e6f40c?jfwid=
61. Transport Competency Agency (2021) Civil Aircraft of the Republic of Lithuaniam available at: https://tka.lt/oro-transportas/
62. DroneRules (2022) Regulations: Lithuania (LT) Available at: https://dronerules.eu/assets/covers/National-Regulation_LIT.pdf; https://dronerules.eu/en/professional/regulations/lithuania
63. Law on the Legal Protection of Personal Data of the Republic of Lithuania. 11 June 1996 No. 1374 Vilnius. Available at (in Lithuanian):https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/asr

64. Kirklytė, I. and Sidas Sokolovas, S. (2021) GDPR Derogations: Lithuania. Thomson Reuters Practical Law. Available at: https://uk.practicallaw.thomsonreuters.com/w-023-6239
65. European Union (n. d.) Greece. Country Profiles. Available at: https://european-union.europa.eu/principles-countries-history/country-profiles/cyprus_en
66. http://www.vasslaw.com/wp-content/uploads/2015/01/guide-to-shipping2013.pdf
67. Yiallourides, C. (2021). Maritime Boundary Delimitation in the Eastern Mediterranean Sea: Progress and Outstanding Legal Issues. Eastern Mediterranean Affairs, (2).
68. European Union (2021) Country Profiles, 'Cyprus' available at: https://european-union.europa.eu/principles-countries-history/country-profiles/cyprus_en
69. Republic of Cyprus: Department of Civil Aviation (2021) Civil Aviation Act (N213(I)/2002/2015) available at: http://www.mcw.gov.cy/mcw/dca/dca.nsf/All/87834DE09CBCA7C4C22582E20038A843?OpenDocument
70. Statutory Instrument 402/2015 (27.11.2015) - Civil Aviation Decree (Conditions for the Operation of Unmanned Aerial Vehicles in the Republic of Cyprus) 2015 as amended. Available at: http://www.mcw.gov.cy/mcw/dca/dca.nsf/All/BF026F4CECA35180C2257DB30030A750/$file/UAVS%20Decree%20402-2015-english%20tanslation%20last%20revision%20jan%202016%20(3).pdf
71. Statutory Instrument 403/2015 (27.11.2015) – Civil Aviation, (Exemption of Unmanned Aerial Vehicles from Obligatory Registration) Decision 2015. Available at: http://www.mcw.gov.cy/mcw/dca/dca.nsf/All/BF026F4CECA35180C2257DB30030A750/$file/UAVs-Decision%20403-2015-english%20translation.pdf
72. Department of Civil Aviation (2022) Unmanned Aircraft Systems. Available at: https://drones.gov.cy/
73. DroneRules (2022) Regulations: Cyprus (CY) Available at: https://dronerules.eu/en/professional/regulations/cyprus
74. Law Providing for the Protection of Natural Persons with Regard to the Processing of Personal Data and for the Free Movement of Such Data of 2018 (Law No.125(1)/2018). Available at: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf
75. Georgiades, A and Sapidou, C. I (2022) GDPR Derogations: Cyprus. Thomson Reuters Practical Law. Available at: https://uk.practicallaw.thomsonreuters.com/w-023-5063
76. European Union (n. d.) Greece. Country Profiles. Available at: https://european-union.europa.eu/principles-countries-history/country-profiles/greece_en
77. European Union (n. d.) Bulgaria. Country Profiles. Available at: https://european-union.europa.eu/principles-countries-history/country-profiles/bulgaria_en
78. etias.info (n.d) Bulgaria and the Schengen Area: Will Bulgaria join soon? Available at: https://www.etias.info/bulgaria-schengen-area-member/
79. Eddings, G., Chamberlain, A, and Colaço (2020) The Shipping Law Review. Seventh Edition. Law Business Research Ltd. Available At: https://www.hfw.com/downloads/SLR-7_Greece.pdf

80. Code of Public Maritime Law 1973
81. Code of Private Maritime Law 1958
82. Ministry for Infrastructure and Transport, Hellenic Civil Aviation Authority (2021) Information to visitors concerning UAS (drones) flights in Greece. Hellenic Republic. Available at: http://www.ypa.gr/en/HCAA_UAS_FLT_request_editable.pdf
83. Civil Aviation Administration (n. d.) Unmanned Aircraft Systems . Ministry of Transport and Communications. Bulgaria. Available at: https://www.caa.bg/en/category/633/16502

Appendix A: Deliverable Ethics Review

Ethical and Legal Issues	Yes/No by Partner & EtAB comments (if needed)
General	
This deliverable includes the opinion/input of a DPO, Legal or Ethics Advisor.	**Yes** **EtAB comments: Due to its nature, this deliverable has been drafted by Legal/Ethics Experts from CENTRIC.**
Human Participation in research activities (questionnaires, workshops, pilots or other research activities)	
This deliverable is based on research activities (questionnaires, workshops, pilots or other tasks) that involve human participants.	**No** **EtAB comments:**
This deliverable is based on research activities (either during pilots or during the execution of other tasks) that may involve children or adults unable to give informed consent or vulnerable individuals/groups.	**No** **EtAB comments:**
Informed Consent Forms for the participation of humans in research have been/will be signed.	**No** **EtAB comments:**
Measures for the protection of vulnerable individuals/groups have been/will be implemented.	**No** **EtAB comments:**
Incidental findings, i.e. findings that are outside the research's scope, may be detected as part of the research activities described in this deliverable (criminal activity or personal data of non-volunteers during trials).	**No** **EtAB comments:**
Data Protection	
This deliverable is based on research activities that involve processing of personal data.	**No** **EtAB comments:**
This deliverable is based on research activities that involve processing of special categories of personal data according to Article 9 GDPR. Special categories of personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation).	**No** **EtAB comments:**
This deliverable is based on research activities that involve further processing of previously collected personal data or publicly available personal data.	**No** **EtAB comments:**
Informed Consent Forms for the personal data processing have been/will be signed and data subjects have been duly informed about their rights.	**No** **EtAB comments:**
The conditions for consent cannot be fulfilled. Another legal basis exists.	**No** **EtAB comments:**
This deliverable is based on research activities that involve transfer of personal data from/to non-EU/EEA countries (non-EU/EEA partners or advisory board members from non-EU/EEA countries) or processing of personal data during the use of platforms regulated by non-EU/EEA law.	**No** **EtAB comments:**
This deliverable implements appropriate technical measures that constitute safeguards (encryption or anonymisation or pseudonymisation).	**No** **EtAB comments:**

This deliverable implements other security measures for the prevention of unauthorized access to, unauthorized transfer of, loss or erasure of personal data.	**No** **EtAB comments:**
This deliverable is based on research activities that involve profiling of data subjects. 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.	**No** **EtAB comments:**
Health and Safety procedures (for the staff and the participants in the pilots or other research activities)	
This deliverable refers to activities that may raise health and safety concerns (e.g. from the use of UAVs or from other risks during the pilots).	**No** **EtAB comments:**
This deliverable integrates the measures and mitigation actions presented in D8.5 EPQ-Requirement No.5.	**No** **EtAB comments:**
Dual use	
This deliverable refers to research activities that involve dual-use items in the sense of Regulation (EC) 428/2009, or other items for which an authorization is required.	**No** **EtAB comments:**
Potential misuse of the research findings	
This deliverable includes methodology, knowledge or references to tools and technologies that could be misused if they ended up to the wrong hands or could lead to discrimination and stigmatization of humans.	**No** **EtAB comments:**
This deliverable integrates the mitigation actions presented in D8.7 M-Requirement No.7.	**No** **EtAB comments:**

Appendix B: Deliverable Quality Review Report

NESTOR Consortium uses this Quality Review Report process internally in order to assure the required and desired quality assurance for all project's deliverables and consequently the consistency and high standard for documented project results.

The Quality Review Report is used individually by each deliverable's peer reviewers with allocated time for the review to be 7 calendar days. The author of the document has the final responsibility to reply on the comments and suggestions of the peer reviewers and decide what changes are needed to the document and what actions have to be further undertaken.

8.1 Reviewers

Project Coordinator	HP – Giannoula Xalvatzi
Management Support Team Member	KEMEA – Mirela Rosgova
Internal Peer Reviewer(s)	MAG - Sofoklis Efremidis, KEMEA – Georgia Melenikou

8.2 Overall Peer Review Result

The Deliverable is:

☐ Fully accepted

☒ Accepted with minor corrections, as suggested by the reviewers

☐ Rejected unless major corrections are applied, as suggested by the reviewers

8.3 Consolidated Comments of Quality Reviewers

General Comments	
Deliverable contents thoroughness	Reviewers' comment: Thorough coverage of the legal and security requirements addressed Author's reply:
Innovation level	Reviewers' comment: No innovation is expected Author's reply:
Correspondence to project and programme objectives	Reviewers' comment: Fully aligned with the project objectives Author's reply:
Specific Comments	
Relevance with the objectives of the deliverable	☒ Yes ☐ No ☐ Partially ☐ Not applicable Reviewers' comment: Author's reply:
Completeness of the document according to the its objectives	☒ Yes ☐ No ☐ Partially ☐ Not applicable Reviewers' comment: Author's reply:
Methodological framework soundness	☒ Yes ☐ No

	☐ Partially ☐ Not applicable Reviewers' comment: Author's reply:
Quality of the results achieved	☒ Yes ☐ No ☐ Partially ☐ Not applicable Reviewers' comment: At points the content is too broad, for example reference to the UN declaration for human rights for introducing Author's reply:
Structure of the deliverable with clear objectives, methodology, implementation, results and conclusions	☐ Yes ☐ No ☒ Partially ☐ Not applicable Reviewers' comment: Lots of legislation or conventions are listed in the document but in cases they it is not apparent their impact to NESTOR. See the comment on ECHR and CFR Author's reply:
Clarity and quality of presentation, language and format	☐ Yes ☐ No ☒ Partially ☐ Not applicable Reviewers' comment: The language must be improved throughout the document. Author's reply:

Detailed Comments (please add rows if needed)		
No.	**Reference**	**Remark(s)**
1		Please check comments inside the document
2		All security and legal requirements that relate to the NESTOR system/platform must be clearly expressed, placed in frames and numbered.
3		