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

D1.6
Ethics and societal issues management final report

Project	NESTOR – 101021851
Work Package	WP1–Project coordination and management
Deliverable	D1.6 - Ethics and societal issues management (final report)
Editor	KEMEA - [redacted]
Lead Beneficiary	KEMEA
Status	☒ Draft ☒ Consortium reviewed ☒ Peer reviewed ☒ Management Support Team reviewed ☒ Project Coordinator accepted
Version	1.0
Due Date	30/04/2023
Delivery Date	04/05/2023
Dissemination Level	CO

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

Deliverable	D1.6 - Ethics and societal issues management (final report)
Editor	KEMEA – [redacted]
Contributors	External Ethics Expert (VUB) – [redacted] CENTRIC – [redacted] CERTH – [redacted] MILTECH – [redacted]
Reviewers	CENTRIC – [redacted] CERTH – [redacted]
Ethics Assessment	☒ Passed ☐ Rejected Comments (if any):
Security Assessment	☒ Passed ☐ Rejected Comments (if any):

Abstract	D1.6 is the final report on providing analysis and assessment of ethical and societal aspects of the NESTOR project. This deliverable aims at identifying, mapping and advising on the ethics and societal issues related to the NESTOR research activities and the implementation of the NESTOR system by the interested stakeholders.
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 Commission. 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	20/03/2023	KEMEA	Initial Draft - TOC preparation
0.2	03/04/2023	KEMEA	1st Draft Version
0.3	10/04/2022	KEMEA	Ready for review and additions by the EtAB
0.4	19/04/2023	External Ethics Advisor	Contribution to Chapter 3
0.5	24/04/2023	CENTRIC	Contribution to Chapter 3
0.5	25/04/2023	KEMEA	Incorporation of input by CERTH, MILTECH, CENTRIC
0.6	27/04/2023	KEMEA	Ready for peer review
0.7	03/05/2023	KEMEA	Final modifications based on the reviewers' comments
0.8	04/05/2023	KEMEA, CERTH, CENTRIC	Peer and Ethics Review Forms were integrated, Ethics and Security assessment were filled in
1.0	04/05/2023	HP, KEMEA	Final version – Ready to submit

Executive Summary

According to the description in the NESTOR Grant Agreement, D1.6 is the final report on providing analysis and assessment of ethical and societal aspects of the NESTOR project. This deliverable aims at identifying, mapping and advising on the ethics and societal issues related to the research activities to be conducted under NESTOR. The ethics experts are constantly in close cooperation with the Project Management Team, to provide guidance and steering on ethical and societal issues of the proposed solutions and how to implement H2020 ethics requirements. All partners have contributed to this task to the extent that they shall provide ethics-related documentation and demonstrate their compliance with the H2020 ethics standards. Additionally, it is highlighted that there is a strong collaboration and policy alignment with the External Ethics Advisor who is consulted upon the arising of any ethics and societal-related questions. Further to the description in the Grant Agreement, D1.6 extends beyond the research period by describing the ethical and societal aspects of the NESTOR system during its deployment and implementation by the interested stakeholders.

Table of Contents

List of Tables

Terms and Abbreviations

AI	Artificial Intelligence
AIA	Artificial Intelligence Act
AR	Augmented Reality
BM	Border Management
CO	Consortium Only
D	Deliverable
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DU-Requirement	Dual Use - Requirement
EC	European Commission
EPQ-Requirement	Extended Project Qualification - Requirement
EtAB	Ethics Advisory Board
EU	European Union
GEN-Requirement	General - Requirement
H-Requirement	Humans - Requirement
JCA	Joint Controllership Arrangement
LEAs	Law Enforcement Agencies
M	Month
ML	Machine Learning
M-Requirement	Misuse - Requirement
PEO	Project Ethics Officer
POPD-Requirement	Protection of Personal Data - Requirement
PSO	Project Security Officer
RF	Radio Frequency
SAB	Security Advisory Board
T	Task
TOD	Thermal Object Detection
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
USV	Unmanned Surface Vehicle
UUV	Unmanned Underwater Vehicle
VOD	Visual Object Detection
WP	Work Package

1 INTRODUCTION

The aim of T1.5 'Ethics and societal issues management' is to identify and describe the ethical and societal aspects of the NESTOR project during the research period and during the implementation phase.

To this end, two reports are part of this task:

D1.5 *Ethics and societal issues management (initial report)* constituted the initial version and was focused on the research by providing guidance to the Consortium and explaining how the NESTOR Consortium has dealt with the identified ethical issues until the date of that deliverable's submission. It also included a preliminary assessment of the NESTOR societal aspects.

The present deliverable, D1.6 *Ethics and societal issues management (final report)* constitutes the updated version of D1.5 and is focused: (1) on the research activities that were conducted by the end of the NESTOR project assessing their compliance with the ethical standards and the applicable laws as well as on the NESTOR activities that were carried out to meet to the project's societal objectives and (2) on the post-project implementation, initially, by assessing the NESTOR system's ethical aspects and indicating the appropriate procedures that must be followed by the technology developers and the future end users to mitigate the assessed risks and ensure compliance of the NESTOR system with the ethical principles and the applicable legal framework and, finally, by describing the NESTOR system's societal aspects and impact.

The second chapter presents how the NESTOR Consortium has dealt with the ethics issues identified as part of WP8 'Ethics requirements' (section 2.1). In addition, special reference is made about the development of AI-enabled technologies during the project's lifecycle following an ethics-by-design approach (section 2.2). The actions taken by the Consortium in order to meet the project's objectives related to the societal impact are also enumerated (section 2.3).

The third chapter is dedicated to the post-project phase and describes the ethical aspects (section 3.1) as well as the societal aspects of the NESTOR system (section 3.2).

In the fourth chapter, the concluding remarks are presented.

In the Appendix can be found: (A) the declaration of compliance obtained by CERTH, (B) the updated DPIA conducted by CERTH for the data processing operations carried out as part of T3.4 'Web and social media monitoring services' (relevant ethics deliverable D8.3), (C) the ethics guidelines related to the Cypriot Maritime Trial, (D) the Joint Controllership Arrangement drafted for the data processing operations carried out as part of the Cypriot Maritime Trial, (E) the ethics guidelines related to the Greek-Bulgarian Land and Maritime Trial, (F) the Joint Controllership Arrangement drafted for the data processing operations carried out as part of the Greek-Bulgarian Land and Maritime Trial and (G) the questionnaire on 'Ethics by Design for AI' that was sent to the NESTOR AI-system designers.

2 MANAGEMENT OF THE ETHICS AND SOCIETAL ISSUES IN THE NESTOR RESEARCH

2.1 ETHICS MANAGEMENT

During the preparation of the NESTOR proposal, the internal ethics experts from KEMEA conducted an initial ethics self-assessment which is reflected under Section 5 Ethics and Societal Impact of the NESTOR Grant Agreement. Based on this assessment, the European Commission set out the ethics requirements that must be fulfilled and submitted as deliverables for the NESTOR research to be compliant with the H2020 ethics standards and the project-related applicable legal framework. The ethics requirements are listed under WP8 of the NESTOR Grant Agreement and cover a wide spectrum of ethical aspects related to human participation, protection of personal data, non-EU countries, health and safety, dual use and misuse.

During the NESTOR research, the aforementioned ethical issues were analysed and described in detail in the respective WP8 deliverables, as well as the mitigation measures to effectively counter the possible risks. The deliverables were prepared by the Project Ethics Officer (PEO) based on the input provided by all partners of the NESTOR Consortium and they were reviewed or co-drafted by the other Ethics Advisory Board (EtAB) members.

In combination with the deliverables of the WP8, 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 was provided in D2.2 'Report on the legal, and security requirements for border security', that aimed to constitute a reference guide for NESTOR partners to ensure that the design and development of the technical components of the system respect all fundamental rights, legal requirements and security best practices.

All WP8 ethics deliverables have already been completed and submitted (incl. the final report of the EtAB due in M18) as shown in the table below.

Table 1. Ethics requirements submitted as deliverables

Deliverable Number	Deliverable Title	Status
D8.1	H-Requirement No.1	Submitted
D8.2	H-Requirement No.2	Submitted
D8.3	POPD-Requirement No.3	Submitted
D8.4	NEC-Requirement No.4	Submitted
D8.5	EPQ-Requirement No.5	Submitted
D8.6	DU-Requirement No.6	Submitted
D8.7	M-Requirement No.7	Submitted
D8.8	GEN-Requirement No.8	Submitted
D8.9	GEN-Requirement No.9	Submitted

The NESTOR Consortium was aware of its responsibilities and committed to respecting the WP8 ethics requirements in practice.

- **Ethics Advisory Board:** An Ethics Advisory Board (EtAB) was set up with internal and external ethics experts and its main responsibility was to conduct ethics monitoring throughout the project's lifespan and early address potential risks as well as recommend mitigating actions. The EtAB was chaired by the Project Ethics Officer (PEO). More information about the structure, the role and the activities of the EtAB can be found in D8.8 and D8.9 which are the reports drafted by the EtAB members.
- **Deliverable Ethics Review:** The Ethics Review Form that is attached as an Appendix to all project's deliverables helped the deliverables' authors understand their ethical/legal responsibilities while it also helped the PEO and the EtAB effectively monitor the research activities described in the respective project's deliverables.
- **Communication with the Consortium:** The information included in the WP8 ethics deliverables (identified risks and recommended or required procedures and measures) was made available to the NESTOR Consortium through dedicated sessions during the project meetings. Furthermore, guidance and assistance were provided by the PEO, in collaboration with the EtAB, upon any relevant questions asked or clarifications requested by a NESTOR partner.
- **Informed consent:** Information Sheets and Informed Consent Forms were drafted, and the informed consent procedure was followed prior to all project's activities that involved humans (project meetings, survey on standardisation needs, training courses, workshop on 'Border Management Standardisation Roadmap', three NESTOR trials, NESTOR Demo Day and Final Workshop). The objectives were (a) to ensure the voluntary character of each research activity after having provided to the participants information about the specific characteristics and the purpose of each research activity, any identified health and safety risks and the respective measures implemented by the NESTOR Consortium for their mitigation, the participants' right to withdraw their consent at any time without consequences and the contact details of the lead researchers (b) to obtain the consent of the participants/data subjects prior to each data processing operation (consent as lawful basis according to Article 6 par.1(a) GDPR) after having provided the information required according to Article 13 GDPR.
- **Data Protection Impact Assessment:** Following the risk assessment conducted under D8.3 POPD-Requirement No.3, due to the identification of potentially high risks for the rights and freedoms of the data subjects involved in the T3.4 'Web and social media monitoring services' data processing operations, two different DPIAs of Article 35 GDPR were conducted by CENTRIC and CERTH in collaboration with their DPO. Given that the consent of the data subjects could not be obtained, different lawful bases were confirmed by each controller (CENTRIC: public interest of Article 6 par.1 (e) GDPR for the processing of personal data through a web crawler, CERTH: legitimate interests of Article 6 par.1 (f) GDPR for the processing of personal data through a social-media crawler). Technical and organisational measures were implemented by each controller

that minimised effectively the privacy risks. The data processing operations related to T3.4 were regularly reviewed by the EtAB concluding that CERTH's DPIA needed to be updated prior to the start of the Greek-Bulgarian Land and Maritime Trial (see below Appendix B).

- **Training courses:**
  - As mentioned above, the informed consent procedure was followed prior to the start of the training courses.
  - Ethics guidelines on health and safety and on misuse mitigation were drafted by the PEO, in collaboration with the NESTOR Consortium, and were circulated to the trainers and trainees as part of the T6.2 training courses (see Annex of D1.5).
  - The NESTOR Consortium respected the health and safety procedures and implemented the necessary measures; hence, any relevant risks were prevented during the training courses and the Consortium staff was well-trained and prepared for the pilot demonstrations.
- **Pilot demonstrations:**
  - As mentioned above, the informed consent procedure was followed prior to the start of each pilot demonstration. In the pilots' case, the Information Sheets included an Annex on health and safety in order to provide thorough information to the trial participants prior to the acquisition of their consent.
  - Specifically, as regards the Greek-Bulgarian Land and Maritime Trial, the Information Sheet and the Informed Consent Form also included a confidentiality clause for those participants of the VIP Day that were not members of the NESTOR Consortium (external guests) in order to ensure the confidentiality of the discussions and to prevent further use of the information for different non-project related purposes.
  - Ethics guidelines were drafted by the PEO, in collaboration with the NESTOR Consortium, and were circulated to the trial organiser SBGSLT as part of the Lithuanian Maritime Trial (see Annex of D1.5), to the trial organiser JRCC as part of the Cypriot Maritime Trial and to the trial organiser HP as part of the Greek-Bulgarian Land and Maritime Trial (see below Appendix C and Appendix E, respectively). The ethics guidelines covered all WP8 ethics requirements, i.e., the ones related to human participation, acquisition of ethics approvals or declarations of compliance, personal data protection, health and safety, involvement of non-EU countries and acquisition of the necessary export licenses, dual use and the acquisition of the necessary authorisations where applicable, prevention of misuse).
  - All necessary ethics approvals and authorisations (relevant ethics deliverables D8.2, D8.4, D8.6, Appendix A of the present deliverable) were obtained in a timely manner prior to the start of the research activities.
  - The NESTOR Consortium respected the health and safety procedures and implemented the necessary measures; hence, all relevant risks were prevented during the pilot demonstrations.

  - Prior to the start of each pilot demonstration, a Joint Controllership Arrangement was agreed and was in place (three in total) between the NESTOR partners that acted as Joint Controllers according to Article 26 GDPR regarding the data processing operations carried out during the Lithuanian Maritime Trial (see Annex of D1.5), during the Cypriot Maritime Trial and during the Greek-Bulgarian Land and Maritime Trial (see below Appendix D and Appendix F, respectively).
- **Involvement of children and vulnerable individuals/groups:** No children and no vulnerable individuals or groups were involved in the project's research activities.
- **Incidental findings:** An incidental findings policy was created for the project (relevant ethics deliverable D8.1), however, no incidental findings were detected during the project's lifecycle and the policy was not used.
- **Misuse mitigation:** The NESTOR Consortium respected the misuse mitigation strategy (relevant ethics deliverable D8.7) and the guidance provided by the EtAB and the PSO.
- **Artificial Intelligence:** Albeit not included in the WP8 ethics requirements, a questionnaire on 'Ethics by Design for AI' was completed by the NESTOR technical partners that designed and used AI systems during the NESTOR research (see below Appendix G). The results are described below in section 2.2 of the present deliverable.

Moreover, the partners of the NESTOR Consortium declared (see D8.2 H-Requirement No.2 and Appendix A below) that during the lifetime of the project they will:

- fully comply with H2020 Regulation (EU) 1291/2013, particularly with Article 19 of this Regulation 'Ethical Principles' which stipulates that the research must comply with "*ethical principles and relevant national, Union and the international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention of Human Rights and its Supplementary Protocols*";
- fully comply with the Universal Declaration of Human Rights (UDHR, 1948), the EU Charter on Fundamental Rights (CFREU, 2010), the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR, 1950) and with the Principles and Good Research Practices as stated in the European Code of Conduct for Research Integrity (ALLEA);
- follow the informed consent procedure for ensuring voluntary participation in the project's research activities;
- fully comply with and respect the applicable national, European and international legislation regarding the protection of personal data, particularly GDPR and with their national law on data protection; to this end, they will follow the informed consent procedure for ensuring compliance with Article 6(1)(a) GDPR or, in cases where the consent cannot be obtained, another legal basis will be sought, and appropriate safeguards will be implemented;
- fully comply with and respect the health and safety procedures as described in D8.5 EPQ-Requirement No.5 and
- take into consideration the opinions and guidance given by the Ethics Advisory Board.

In this spirit and considering all aforementioned actions taken, it can be confirmed that the NESTOR Consortium, as constantly assisted by the ethics experts:

- Respected human dignity and integrity
- Ensured honesty and transparency towards research subjects
- Respected individual autonomy and obtained free and informed consent
- Ensured the protection of personal data and confidentiality
- Ensured the health and the safety of the staff and the research participants
- Obtained export licenses and other required authorisations (where applicable)
- Promoted justice and inclusiveness
- Minimised harm and maximised benefit
- Demonstrated social responsibility
- Delivered high-quality scientific outputs

2.2 ETHICS-BY-DESIGN APPROACH FOR ARTIFICIAL INTELLIGENCE

According to Article 2(7) of the AI Act proposal (latest version of 25 November 2022), "this Regulation shall not apply to any research and development activity regarding AI systems". Hence, the relevant activities carried out in the context of the NESTOR scientific research project are out of the AIA's scope.

Considering the various changes that have been made so far as concerns the content of the AI Act proposal and the fact that no binding text has been issued until today, in order to assess the conformity of the NESTOR system with fundamental rights and consequently its trustworthiness and readiness to be put on the market, a questionnaire (see below Appendix G) was drafted based on Annex I of 'Ethics by Design and Ethics of Use Approaches for Artificial Intelligence' version 1.0 of 25 November 2021 issued by the European Commission and was sent to the NESTOR technical partners that developed AI/ML-based technologies during the NESTOR lifecycle. The results can be found below in the following sections based on the responses provided by each technical partner involved in AI development:

2.2.1 CERTH

Respect for human agency:

The objective of the service is the automation of the detection of objects in the video feed. The tool does use this information after that in any way. It does not perform any decision-

making and it does not suggest actions to the operators. Hence, it can be confirmed that the AI system does not autonomously make decisions about issues that are normally decided by humans by means of free personal choices or collective deliberations or similarly significantly affects individuals.

The operators have been trained on how to use the service and have been advised that the service's purpose is to enhance their capabilities to make informed decisions and not to replace their judgement or authority. The users have full control over the AI system outcomes. Hence, it can be confirmed that end users and others affected by the AI system are not deprived of abilities to make all decisions about their own lives / take autonomous decisions about their lives.

The service has been developed using a human-centered approach, developed in collaboration with end users prioritising their interests, requirements and needs. The end users have been trained to understand some of the key theoretical elements of the algorithms in order to make the tool transparent to the extent possible. Hence, it can be confirmed that end users and others affected by the AI system are not subordinated, coerced, deceived, manipulated, objectified or dehumanised, nor are attached or addicted to the system and its operations.

Resilience and security:

The AI system is enabled by state-of-the-art deep learning object detection models which were selected after thorough review of the literature based on their demonstrated robustness in laboratory conditions. The models were trained and rigorously evaluated with a large number of images from publicly available datasets and data provided by the end users in the course of the project in order to confirm its robustness to various scenarios and use cases. Hence, the AI system design and implementation ensure technical robustness and safety.

The development process as well as an experimental evaluation has been documented in detail in D3.1 promoting reproducibility and allowing validation by external parties. Hence, the AI system design and implementation ensure accuracy, reliability and reproducibility.

Privacy and data governance:

The AI service is fed with visual data from cameras that follow the regulations and guidelines for lawful acquisition in a transparent approach. Hence, the service respects these aspects set by the local and national legislation and processes data in line with the requirements for lawfulness, fairness and transparency set in the national and EU data protection legal framework and the reasonable expectations of the data subjects.

The AI service targets to detect and classify specific objects of interest without the need to collect and process personal data. There is no necessity for the developed AI service to collect and process personal data during any period of time.

The AI system is processing videos in order to detect vehicles, vessels and persons. Although the processing of private data related to the physical appearance of people cannot be avoided

the AI system does not take any action to identify the detected persons and a random artificial alphanumeric ID is generated in order to refer to a specific detection in the platform.

The AI system does not save files on local storage at its output. Instead, it directly communicates its output to the rest of the platform through the communication channel (message bus) that has been created for this purpose. Potential data breaches and leakages cannot be monitored, controlled or stopped by the AI system itself and their occurrence is subject to the security of the facility/network the system is installed in.

Fairness and non-discrimination:

There is no specific mechanism built into the AI system's architecture design or method of deployment that can insert model bias. The AI system was trained in a compilation of large-scale object detection datasets that are publicly available. We consider the trained model bias-free to the extent that the landscape of available large-scale datasets that exist on the present day have made possible.

The AI system is not self-aware of the biases it may create. Instead, the identification of such biases is completely up to the end users to identify and report through the ongoing monitoring and evaluation of the AI systems for potential bias in real-world deployment.

The AI system is designed so that it can be used by different types of end-users with different abilities. There are no restrictions on who can be a potential end user of the AI system provided that they have been trained to do so properly through the training program.

The AI system does not have negative social impacts on the affected groups of individuals, including impacts other than those resulting from algorithmic bias or lack of universal accessibility. The AI system has been developed by involving stakeholder engagement, ensuring transparency through documentation, and incorporating end user oversight in all the stages of development, deployment, and evaluation.

Individual, and social and environmental well-being:

The AI system takes the welfare of all stakeholders into account and does not unduly or unfairly reduce/undermine their well-being. The AI system was built with through a collaboration with stakeholders and end users prioritising their interests, requirements and needs.

Regarding the principle of environmental sustainability, this is not relevant with the said system, hence not applicable.

The AI system does not have the capacity to negatively impact the quality of communication, social interaction, information, democratic processes, and social relations.

The system does not reduce safety and integrity in the workplace and complies with the relevant health and safety and employment regulations.

Transparency:

The end-users are aware that they are interacting with an AI system. They have been trained to use the AI system in the correct contexts.

The purpose, capabilities, limitations, benefits and risks of the AI system and of the decisions conveyed are openly communicated to and understood by end-users and other stakeholders along with its possible consequences. The end users have been informed about how the AI system works, as well as its limitations and potential risks. In the visualisation layer that is displayed to the end users a metric is displayed that represents the confidence level of the algorithm for each detection that is made and provides additional insight when interpreting its outcomes.

The AI system provides detections of objects of interest from videos and does not have any capability or authority to take further actions. Full control remains in the end users' hands to utilise the information provided by the AI system and decide upon their appropriate actions. Hence, human intervention is ensured at all times.

The AI system enables traceability during its entire lifecycle, from initial design to post-deployment evaluation and audit. The development, integration, deployment, and evaluation activities have all been documented in the relevant project deliverables.

Finally, the system does not make any decisions, hence relevant records (data logs) are not kept.

Accountability and oversight:

The AI system allows for human oversight during its decision cycles and operation. The AI system was developed and evaluated through a collaboration effort of the technology provider and the end users keeping the users in the loop during the full project's lifespan.

The system does not provide details of how potential ethically and socially undesirable effects will be detected, stopped, and prevented from reoccurring. It is up to the end users who are the final decision-makers to take all relevant necessary actions.

2.2.2 MILTECH

The tool is designed for the detection and classification of tracks detected by a thermal camera.

Respect for human agency:

The AI system does not perform any decision-making and it does not suggest actions to the operators. It only provides indicative information. Hence, it can be confirmed that the AI

system does not autonomously make decisions about issues that are normally decided by humans by means of free personal choices or collective deliberations or similarly significantly affects individuals.

The AI system provides only indicative information, and the users have full control over its outcomes. Hence, it can be confirmed that end users and others affected by the AI system are not deprived of abilities to make all decisions about their own lives / take autonomous decisions about their lives.

The TOD has been developed using a human-centered approach, developed in collaboration with end users prioritising their interests, requirements and needs. The AI system provides only indicative information and assists users in visual interpretation. Hence, it can be confirmed that end users and others affected by the AI system are not subordinated, coerced, deceived, manipulated, objectified or dehumanised, nor are attached or addicted to the system and its operations.

Resilience and security:

The AI system was thoroughly tested under all possible working conditions. Hence, the AI system design and implementation ensure technical robustness and safety.

The development process as well as an experimental evaluation has been documented in detail in D3.1 promoting reproducibility and allowing validation by external parties. Hence, the AI system design and implementation ensure accuracy, reliability and reproducibility.

Privacy and data governance:

No personal data are processed through the AI system. The TOD aims to detect and classify specific objects of interest without the need to collect and process personal data. There is no necessity for the developed AI tool to collect and process personal data during any period of time.

Fairness and non-discrimination:

The identification of any biases is completely up to the end users to identify and report through the ongoing monitoring and evaluation of the AI systems for potential biases in real-world deployment.

The AI system is designed so that it can be used by different types of end-users with different abilities. There are no restrictions on who can be a potential end user of the AI system.

The AI system does not have negative social impacts on the affected groups of individuals, including impacts other than those resulting from algorithmic bias or lack of universal accessibility. The AI system has been developed by involving stakeholder engagement, ensuring transparency through documentation, and incorporating end user oversight in all the stages of development, deployment, and evaluation.

Individual, and social and environmental well-being:

The AI system takes the welfare of all stakeholders into account and does not unduly or unfairly reduce/undermine their well-being. The AI system was built with through a collaboration with stakeholders and end users prioritising their interests, requirements and needs.

Regarding the principle of environmental sustainability, this is not relevant with the said system, hence not applicable.

The AI system does not have the capacity to negatively impact the quality of communication, social interaction, information, democratic processes, and social relations.

The system does not reduce safety and integrity in the workplace and operates in compliance with the relevant health and safety and employment regulations.

Transparency:

The end-users are aware that they are interacting with an AI system. They are also aware that they can enable/disable it at all times.

The purpose, capabilities, limitations, benefits and risks of the AI system and of the decisions conveyed are openly communicated to and understood by end-users and other stakeholders along with its possible consequences. The end users have been informed about how the AI system works, as well as its limitations and potential risks. In the visualisation layer that is displayed to the end users a metric is displayed that represents the confidence level of the algorithm for each detection that is made and provides additional insight when interpreting its outcomes.

The AI system provides detections of objects of interest from videos and does not have any capability or authority to take further actions. Full control remains in the end users' hands to utilise the information provided by the AI system and decide upon their appropriate actions. As mentioned earlier, the end users can enable/disable it. Hence, human intervention is ensured at all times.

The AI system enables traceability during its entire lifecycle, from initial design to post-deployment evaluation and audit. The development, integration, deployment, and evaluation activities have all been documented in the relevant project deliverables.

Finally, records are kept in the form of log data (timestamp, type of target detected and probability of confidence).

Accountability and oversight:

The AI system allows for human oversight during its decision cycles and operation. The AI system was developed and evaluated through a collaboration effort of the technology provider and the end users keeping the users in the loop during the full project's lifespan.

The system does not provide details of how potential ethically and socially undesirable effects will be detected, stopped, and prevented from reoccurring. It is up to the end users who are the final decision-makers to take all relevant necessary actions.

2.2.3 CENTRIC

WP3, T3.4 'Web and social media monitoring services' - The Entity Extraction component automatically identifies named entities such as individuals' names, location names, organisation names. In the case of NESTOR, a document refers to data collected by the web and social media component. It is worth mentioning that this component has not been developed (yet only used) by CENTRIC during the NESTOR project. Nevertheless ethics-by-design has been examined for reasons of completeness.

Respect for human agency:

The component only extracts entities – names of individuals, organisations, locations and similar. Hence, it can be confirmed that the AI system does not autonomously make decisions about issues that are normally decided by humans by means of free personal choices or collective deliberations or similarly significantly affects individuals.

The component does not take any actions based on the output; the output is used to detect trends in content which are then presented to the dashboard operator (human). Hence, it can be confirmed that end users and others affected by the AI system are not deprived of abilities to make all decisions about their own lives / take autonomous decisions about their lives as well as they are not subordinated, coerced, deceived, manipulated, objectified or dehumanised, nor are attached or addicted to the system and its operations.

Resilience and security:

The system could fall back on rule-based models if current implementation could not continue. Hence, the AI system design and implementation ensure technical robustness and safety.

the AI system design and implementation ensure accuracy, reliability and reproducibility.

Privacy and data governance:

The module operates in line with the requirements for lawfulness, fairness and transparency set in the national and EU data protection legal framework and the reasonable expectations of the data subjects. The processing of data is in line with all GDPR requirements and is documented as part of CENTRIC's DPIA

The processed data are received from the Content Acquisition Tool and Social Media Crawler, both having undergone a DPIA. The data are used solely for generating trends on an aggregated level in accordance with the purpose limitation principle.

The data are not stored beyond the lifetime of a specific operation or use of the system. Aggregated data (i.e., the counts) may be maintained without keeping the raw input.

Technical and organisational measures (pseudonymisation techniques) are implemented to remove personal identifiers from the extracted entities.

Security measures are also implemented. Access to the components is strictly controlled through authentication and authorisation mechanisms.

Fairness and non-discrimination:

The system is designed to avoid algorithmic bias, in input data, modelling and algorithm design.

The Entity Extraction module extracts only the detected entities from the provided content. Entities are not collected based on protected characteristics or other areas of potential bias. The entities identified are free from discriminatory biases.

The data collected through the Entity Extraction module no longer accurately reflects the current reality and is not targeted towards a specific subgroup of the target population. Hence, it avoids historical and selection bias in data collection, representation and measurement bias in algorithmic training, aggregation and evaluation bias in modelling and automation bias in deployment.

No negative social impacts have been identified or can be anticipated.

Individual, and social and environmental well-being:

No impacts are expected on well-being, quality of communication, social interaction, information, democratic processes, social relations and on the safety of the individuals.

Regarding the principle of environmental sustainability, this is not relevant with the said system, hence not applicable.

Transparency:

The end-users are aware that they are interacting with an AI system. Users are aware that automated extraction of data is used to inform other (non-AI) components of the NESTOR system.

The purpose, capabilities, limitations, benefits and risks of the AI system and of the decisions conveyed are openly communicated to and understood by end-users and other stakeholders

along with its possible consequences. The end users have been informed about how the AI system works, as well as its limitations and potential risks. During the training, the users of the system were informed as to where the data they are viewing has been extracted from.
The Entity Extraction module is a helper module and is not exposed via a public interface.

The AI system enables traceability during its entire lifecycle, from initial design to post-deployment evaluation and audit. The integration, deployment, and evaluation activities have all been documented in the relevant project deliverables. Furthermore, the end users are informed using the visual analytics tool as to where the underlying data comes from.

Finally, the system does not make any decisions, however the outputs, i.e., the entities extracted, are available.

Accountability and oversight:

The Entity Extraction component was used in response to the NESTOR system requirements. Users can see the output of the extraction in the visual trends interface.

The system is a helper module that does not produce undesirable decisions. It is up to the end users who are the final decision-makers to take all relevant necessary actions.

2.3 SOCIETAL ASPECTS

Further to the relevant section of D1.5, until the official end of the project the NESTOR Consortium conducted research by taking into consideration the societal aspects in line with the project's objectives as they had been addressed during the preparation of the proposal. Complete information verifying the above can be found below:

- The NESTOR user requirements were defined through the active involvement of the end users in the context of WP2 - User requirements analysis and operational scenarios (T2.1 'Use cases and user requirements definition'). Through this, the end users had the opportunity to play a decisive role in the design of a solution that will benefit them and that will be based on their expectations and operational needs.
- A specific task was dedicated to the NESTOR solution's legal and security requirements (T2.2 'Legal and security requirements for border security') which provided for necessary requirements to be fulfilled and the relevant procedures to be followed in accordance with the applicable legal framework. The protection of fundamental rights, including privacy and data protection, is prioritised.
- The NESTOR system was tested during the three pilot demonstrations of WP6 'Demonstration pilots and assessment'. End users from the NESTOR Consortium organised and actively participated in the trials in order to perform scenario storylines in accordance with the project's objectives. After the end of each trial, a questionnaire was circulated to the trial participants aiming for the collection of feedback for the evaluation of the NESTOR system.

- A specific task was dedicated to the development of the NESTOR community (T7.1 'Development of stakeholder community'). The task involved all required activities to establish a stakeholders' network, entitled as NESTOR community, in order to disseminate the project's results and determine potential collaborations with relevant beneficiaries. The community consisted of the NESTOR end users and expanded its synthesis by exploiting all existing contacts and network that each NESTOR partner possessed. Such contacts involved project organisations, representatives of international agencies and other national or local stakeholders that were interested in the NESTOR project. As such, the NESTOR Consortium ensured to maximize the impact of the final prototype.
- The NESTOR project, in cooperation with nine other EU-funded projects, invited relevant stakeholders to join a survey that aimed to collect standardisation needs from Border Management (BM) professionals and stakeholders for a BM Standardisation Roadmap that the projects were planning.
- Following the aforementioned survey, the NESTOR project, in cooperation with nine other EU-funded projects, organised a workshop on 'Border Management Standardisation Roadmap' on February 17, 2023 in Brussels where the standardisation needs were further discussed and validated by the NESTOR partners, BM professionals and other interested stakeholders that attended the workshop.
- As a result of the survey and the workshop, the NESTOR Consortium aimed for the delivery of a roadmap to the relevant standardisation bodies as well as to the European & national authorities and policy makers responsible for Border Management. Through this, NESTOR is expected to provide a wide range of exploitation prospects and consequently impact society and economy. All relevant information can be found in D7.6 'Standardisation and collaboration with other projects'.

3 ETHICAL AND SOCIETAL ASPECTS OF THE NESTOR SYSTEM

3.1 ETHICAL ISSUES

The NESTOR system is primarily composed of two main elements: the advanced detection capabilities and the situational awareness and automated navigation functionalities. D2.2 'Report on legal and security requirements for border security' reviewed some of the main ethical considerations in relation to various software and hardware technologies developed to form the NESTOR system. The NESTOR system is designed to provide a pre-frontier intelligence picture at the European Union's external borders with regard to all forms of activity including trafficking (of people, drugs, weapons and similar) and relevant search and rescue operations by safeguarding and promoting fundamental human rights.

Personal data protection: In D2.2, the advanced detection capabilities discussed relied on the following technologies: use and application of object detection technologies, detection of unknown RF signals, threat identification using radar scanning and online information monitoring. This led to several recommendations around ethical requirements for the NESTOR system to consider during development. Specifically, these included mechanisms to limit the acquisition of personal data and refrain from carrying out any identification activities in the development of technologies for visual cognition. The development focused on detecting only the presence of people, vehicles, and vessels, at a considerable distance, and no identification of persons through facial recognition or other approaches were developed. Such an approach must remain under continual review to ensure all data are being managed and monitored appropriately.

It needs to be pointed out that during the NESTOR research processing of personal data was carried out in accordance with the GDPR for scientific research purposes. During the deployment phase, depending on who will be the controller and for what purposes the NESTOR system will be used, the applicable legislation needs to be re-examined. Given that the end users and the interested stakeholders belong to "competent authorities" as defined in the Law Enforcement Directive and that the purposes of the NESTOR system are "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" at the European borders, applicable are the Law Enforcement Directive and the national legislation transposing the LED in the national legal framework.

In case the use of cameras and sensors that form the NESTOR system extends beyond the detection of people, vehicles and vessels and aims to the identification of individuals, this could entail high risks to the rights and freedoms of the data subjects. A Data Protection Impact Assessment of Article 27 LED (Article 35 GDPR) must be conducted by the controller where all necessary information will be reported. Consultation by the Data Protection Officer appointed in the controller and by the national supervisory authority must be sought.

Technical and organisational measures must be implemented and information about the processing must be provided to the affected data subjects through the official website of the controller or through other adequate means in order to enable the data subjects to exercise their rights related to data protection.

In the case of joint controllership (more controllers determine the means and purposes of the data processing operations), a Joint Controllers Agreement must be signed. In the case of a controller-processor relationship, a data processing agreement must be signed between the controller and the processor acting on the controller's behalf.

Regarding the web and social media monitoring, the potential ethical considerations raised were focused on issues such as limiting collateral intrusion and ensuring due respect of the terms of service of any page identified for extraction. The web monitoring approach limits the level of depth-based crawling to restrict the amount of data accessed while any starting URLs are managed by the operator. During system implementation it would be appropriate to have strict organisational controls on the input and monitoring of the data acquired from both the web and social media. The approach also implemented pseudonymisation and encryption techniques to mask any personal data collected during the crawling activity. A full data protection impact assessment was conducted from both CERTH and CENTRIC with regards to this component to ensure proper monitoring and to reduce the identified risks.

Prior to the deployment of the NESTOR system, the DPIAs must be revised in order to include any changes to their current content. Given that a DPIA is a living document, its content must be reviewed regularly and updated whenever needed.

Artificial Intelligence: The NESTOR system is coordinated by an overall command-and-control interface that has several functionalities and responsibilities for providing situational awareness. This includes the development of technologies that utilise mixed reality for training and field operations, coordinating the use of multiple UxVs, fusing data together from newly developed and legacy systems, and providing visual analytics and decision support.

The recommendations in D2.2 also included ensuring that appropriate and representative datasets are used for testing and training of any artificial intelligence components. As this was mainly carried out under the visual cognition elements (for both visual and thermal cameras) the training datasets were fully documented within the relevant deliverable D3.1 'Visual cognition algorithms for optimal surveillance'.

Regarding the use of human-in-the-loop, all activities within NESTOR are coordinated through the command-and-control interface that ensures all running processes and activities have continuous monitoring and require human oversight as well as human intervention to initiate and have control over each action. The ethics-by-design approach was followed for all NESTOR AI-enabled components as explained in detail in section 2.2 above by taking into consideration the Ethics Guidelines for Trustworthy Artificial Intelligence issued by the High-Level Expert Group on AI and aiming to ensure compliance of the components with the key requirements for trustworthy AI stipulated therein.

During the deployment phase, the end users that are planning to make use of the NESTOR system must continue respecting the aforementioned Ethics Guidelines and keep up with the legislative developments on the matter given that the relevant proposed Regulation (Artificial Intelligence Act) is still in progress.

According to the current version of the AIA proposal, Annex III makes an explicit reference to the high-risk AI systems of Article 6(3) and provides clarifications per category. AI systems that are used by LEAs or on their behalf are classified as 'high-risk' AI systems.

In particular, as 'high-risk' are classified: "(a) AI systems intended to be used by law enforcement authorities or on their behalf to assess the risk of a natural person for offending or reoffending or the risk for a natural person to become a potential victim of criminal offences; (b) AI systems intended to be used by law enforcement authorities or on their behalf as polygraphs and similar tools or to detect the emotional state of a natural person; (c) [deleted] (d) AI systems intended to be used by law enforcement authorities or on their behalf to evaluate the reliability of evidence in the course of investigation or prosecution of criminal offences; (e) AI systems intended to be used by law enforcement authorities or on their behalf to predict the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups; (f) AI systems intended to be used by law enforcement authorities or on their behalf to profile natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences (g) [deleted]".

The reason behind this, is that, due to their nature and purpose, actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter of Fundamental Rights. The AI system must be trained with high-quality data and meet adequate requirements in terms of its accuracy or robustness as well as it must be properly designed and tested before being put on the market or otherwise put into service. Otherwise, it may single out people in a discriminatory or otherwise incorrect or unfair manner.

According to Recital 62 and Chapter 2 of the AIA proposal, high-risk AI systems will be subject to strict obligations before they can be put on the market or otherwise put into service. Such obligations include:

- the conducting of a conformity assessment,
- the establishment of a risk management system,
- appropriate testing procedures,
- high quality of the datasets feeding the system to mitigate risks and discriminatory outcomes,
- activity logging to ensure traceability of results,
- technical documentation, record-keeping ('logs'),
- transparency and provision of clear and adequate information to the user,

- appropriate human oversight,
- high level of robustness, security and accuracy.

Health and safety: Ethical considerations were addressed in D2.2 and in D8.5 related to health and safety. The importance of health and safety monitoring for the use of UxVs, radars and AR headsets was highlighted. Regarding the monitoring of UxV pilots, radar/RF system operators and AR users, all health and safety procedures were implemented before any testing took place and this should continue to be monitored going forward. Additional support could include a reminder to AR users as they start the headset and a warning after a period of continual usage. All visual implementations followed best practices for the development and visualisation of information as well as making use of standardised libraries that have built-in features for supporting development.

Finally, NESTOR continually strived to monitor and address any ethical considerations as they arose throughout the project. The trials were designed to replicate real-world scenarios insofar as possible and thus the system was developed to address ethical issues as they would arise in an operational system.

It is of course necessary to continue to monitor for potential ethical issues including underlying aspects (for example, the introduction of technology can have impacts such as complacency through too much trust in technology, while it can also cause people (e.g., border guards) to have increased fears over their job security). Similarly, the transparency is also an important ethical issue to consider for organisations adopting advanced technology, i.e., how much should the public be aware of the implementation of technology in the security sector, against the extent to which malicious actors may implement adversarial approaches to reduce the effectiveness of such technology. Nonetheless, full documentation of all components of any system and the functions should be recorded and securely stored within the end user's organisation. In addition, a system such as NESTOR may continue to increase its use of artificial intelligence technologies and thus appropriate safeguards to comply with the forthcoming AI Act as well as taking best practices from projects such as AP4AI[1] will also be of significant benefit to manage ethics issues related to AI in the future and to create a trustworthy AI system that will be ready to be put on the market.

3.2 SOCIETAL IMPACT

The project's principal underpinning is to address the coordination and improvement of potential responses to threats and incidents through enhancing border surveillance systems and information sharing with competent authorities. Specifically, NESTOR multiply responds to the utmost need to safeguard the right to life; this is achieved by minimising the death toll at sea and at land, via detecting and monitoring irregular border activity, such as smuggling, human trafficking, irregular migration, and illegal fishing. The initiative is framed under

[1] https://ap4ai.eu

European Union's Policy on land border and coastal surveillance, towards protecting the EU community and its citizens from external threats. The manner in which this is achieved entails direct implications for life and the safeguarding of European values and fundamental rights and freedoms as enshrined in the EU Charter.

NESTOR contributes towards the protection of human lives by providing technical tools and methods to detect and efficiently manage risks at land and coastal borders. The research addresses land and maritime border security threats, maritime accidents, and loss of life at sea, illicit trafficking of weapons, drugs and persons, smuggling, illegal, unreported, and unregulated fishing, irregular migration, intentional and unlawful damage to marine environment. The positive impact of such initiative is by-design of high value, for several stakeholders, including public organizations, and the public at large. However, chilling effects to rights and freedoms as well as unexplored grounds are documented, entailing negative risks of implementing such solution at large-scale in the future.

First, among the beneficiaries are directly involved stakeholders, such as public authorities (national, regional, European) responsible for border surveillance, domestic or European law enforcement agencies, intelligence agencies and security providers, as end users. Additionally, a number of sectors is positively affected: academia, for the purposes of further research, and knowledge transfer, valorisation and exploitation; industry and technology providers through matching requirements and capability gaps of users and promoting coordination and collaboration; other authorities, who aspire to assist individuals in need at sea or land borders, whenever a threat is detected against their life, and survivors of human trafficking.

Second, positive impacts are recognised, probably indirectly, to the public (including individuals and public interests). Developing and implementing an enhanced capability vis-a-vis prevention, detection, mitigation, and reaction to border threats certainly contributes to citizen protection via regulating and pre-empting cross-border criminal activities and saving lives at land and sea borders. The vulnerability of the European Member States, individually and not as a whole, is a major challenge which today's EU reality is confronted with. Enhancing European society's resilience and promoting life, liberty and European values are among NESTOR's primary objectives. To this end, the project's mission is to contribute to the protection of citizens via strengthening border security and reinforcing cooperation of the authorities at a national, regional, and transnational level, additionally leading a more territorially cohesive and sustainable society.

Third, NESTOR allows for considerable cost-savings, performance improvement and quick adoption of the solution by building the NESTOR system on existing state-of-the-art systems and infrastructures. The project enables and improves the surveillance areas' overall operational image and qualitatively expands detection capabilities for the EU maritime safety and security agencies, as end users, by using mixed reality technologies and by offering a wide coverage surveillance system. Finally, improvement is expected on the global maritime security under the implementation of the EU Global Strategy by complying with the EU Maritime Security Strategy Action Plan.

Under a more precautionary lens, the 'smart border package', combined with artificial intelligence capabilities may profoundly affect individuals and the EU society as a whole. Advancing technical border solutions and ensuring constant surveillance on an entry-exit system cannot but reveal a strong emphasis on the policing dimension of border management, on enduring control and on a persisting predominance of national actors. This is not necessarily an adverse effect, a repercussion, but the center of discussion. The principle of proportionality requires a careful balancing between the actual risk and benefits; an answer to the question whether the measures finally implemented are suitable, necessary, and proportionate in a democratic society, as well as to which extent interferences to individuals' fundamental rights and freedoms are justified, remain top priorities in the EU agenda.

Most importantly, the introduction of artificial intelligence in border control and border management stays as one of the most topical discussions, interconnecting policymaking actions on technology and sovereignty, both necessitating a rather sensitive approach. From a different perspective, the EU may be seen as increasingly turning to artificial intelligence technologies in an effort to strengthen its own border control and mitigate security risks stemming from cross-border terrorism, among others, for the sake of its citizens' protection and its effective control over its territory. Smart EU borders may include the development and interlinking of large-scale, centralised information systems; such systems have gradually been expanded and upgraded to cover ever more categories of persons and to process increasingly varied types of personal data (including processing of biometric data).

There are clear benefits to be reaped from a careful adoption of artificial intelligence technologies in the context of border control, such as increased capacity to detect fraud and abuses, better and timely access to relevant information for taking decisions, and enhanced protection of vulnerable people. However, these benefits need to be balanced against the significant risks posed by these technologies to fundamental rights. Areas where artificial intelligence is used to advance the work of competent border and law enforcement authorities are synchronous controls, such as and emotion detection and biometric identification, including face recognition, and anterior mechanisms, such as algorithmic risk assessment.

Individuals' fundamental rights and freedoms are highly valued in the EU. While these rights are not guaranteed risk-free, interferences may only be justified under a strict proportionality protocol. Enabling artificial intelligence solutions in border control entails a series of risks, in particular risks related to bias and discrimination, data protection and mass surveillance. Whereas great attention has been paid to the issue of bias and discrimination, it must be noted that even accurate and unbiased AI systems may pose significant other risks, including to data protection and privacy. What is more, migrants, asylum seekers and survivors of unpleasant experiences such as human trafficking all constitute vulnerable categories of individuals, with low involvement and knowledge on how to exercise rights in a border environment. Moreover, even when profiling is not based on biometric or personal data (such as in the case of NESTOR), other types of data or combinations thereof used for algorithmic profiling may lead to discrimination based on prohibited grounds. Greater transparency, accountability and contestability of automated decisions are gradually ensured in the EU legal order, with

legislation such as the GDPR, the AI Act and collateral instruments, which further promote the fundamental rights and freedoms enshrined in the Charter.

NESTOR has been carefully designed to not only respect but also promote fundamental rights, as further elaborated in earlier sections of this deliverable. While a few points of caution are traced with regards to possible extensive use of this technology in the future, there is no doubt that end users, currently, would be multiply benefitted and that the NESTOR system will constitute contribution to society. Nevertheless, the conducting of a Societal Impact Assessment is highly recommended prior to the deployment of the NESTOR system where all advantages and disadvantages will be analysed as well as the opinions (expectations and potential objections) of the end users and of society members will be stated.

4 CONCLUSION

The present deliverable is the final report on the ethical and societal issues of the NESTOR project and constitutes the updated version of D1.5. It focuses on the ethics and societal issues' management during the period of the NESTOR research (activities not covered until the submission of D1.5) and on the ethics and societal aspects of the NESTOR solution during the implementation phase. The ethical and societal aspects of the project are presented in chapter 2, while the ethical and societal aspects of the NESTOR solution are described in chapter 3.

As part of the ethics management of the project, D1.6 describes the work done in NESTOR from an ethical perspective starting from a short reference to the submitted WP8 deliverables as a result of constant and close collaboration between the project's ethics experts (PEO and EtAB) and the NESTOR Consortium.

To avoid an overlap to the content of WP8, D1.6 describes in section 2.1 the actions taken and the procedures followed by the NESTOR Consortium *further to* the submission of the relevant ethics deliverables. Therefore, this section explains how the NESTOR Consortium has managed to meet the ethics requirements during the research period, how it has dealt with the identified risks and what steps it has taken to mitigate them.

In section 2.2 the ethics-by-design approach that has been followed for the development and use of the AI-enabled components is presented. The involved technical partners (CERTH, MILTECH and CENTRIC) have responded to a relevant questionnaire and based on the provided feedback, it can be confirmed that the AI tools have been designed and used in a way that ensures their operation is in conformity with the key requirements stipulated in the Ethics Guidelines for Trustworthy AI.

As part of the societal management of the project, D1.6 describes in section 2.3 the actions taken and the procedures followed by the NESTOR Consortium in order to meet the societal objectives of the project.

D1.6 extends beyond the research period and describes the ethical and societal aspects of the NESTOR system related to its implementation by the interested stakeholders.

In section 3.1, the main potential ethics issues as raised originally in D2.2 are considered for the different NESTOR technologies, while the section concludes with an overview of the possible wider and future ethical impact and issues related to the development of NESTOR system and pre-frontier intelligence. Special emphasis is placed on data protection, artificial intelligence and health and safety, describing the respective requirements according to the current applicable legal framework. Specifically with respect to artificial intelligence, given that no binding regulation has been issued until the date of the submission of this deliverable, the obligations need to be reviewed in order for the NESTOR system to operate in conformity with the legislative developments before being put into service.

In section 3.2, the main societal impact is presented. This is expressed in function of expected positive and negative consequences for competent authorities implementing the NESTOR solution and for the involved stakeholders, such as technology providers, the general public and individuals interacting with the system at the border point. Among the main findings are the large-scale direction of border control tasks towards automation, as well certain risks of artificial intelligence to fundamental rights and freedoms of vulnerable individuals.

It is noteworthy that the NESTOR solution, as tested and validated in the pilot demonstrations, aims at contributing to society and to the safeguarding of fundamental human rights. The NESTOR Consortium is aware of the importance of ethics and has performed all research activities, including the development of the NESTOR system, in accordance with the applicable legal framework and ethical standards. Any limitations to fundamental rights must be in accordance with the principle of proportionality as stipulated in the Charter of Fundamental Rights and all necessary actions will be taken in this direction.

5 REFERENCES

- European Commission, (2019, February 4). Horizon 2020 Programme Guidance How to complete your ethics self-assessment, version 6.1, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf
- Grant Agreement No 101021851 – Annex A Description of the action
- Grant Agreement Amendment AMD-101021851-3
- Proposal 101021851 for the NESTOR project, Section 5. Ethics and Societal Impact

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 (General Data Protection Regulation)

- Directive (EU) 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive)
- European Commission, 'Ethics by Design and Ethics of Use Approaches for Artificial Intelligence' version 1.0 (25 November 2021)
- High-Level Expert Group on AI, Ethics Guidelines for Trustworthy Artificial Intelligence (8 April 2019)
- Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative act – General Approach (25 November 2022)
- Artificial intelligence at EU borders - Overview of applications and key issues

Appendix A: Declaration of Compliance (CERTH)

NESTOR

Declaration of Compliance for the NESTOR project (GA No. 101021851)

The undersigned certifies that, within the scope of the NESTOR project, the research activities that will be carried out by **ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (CERTH)** under WP3, T3.1 and T3.4 and involve humans:

- fully comply with the Horizon Europe Regulation (No 2021/695 EU)[1], and particularly with Article 19 "Ethics", which states that "*actions carried out under the Programme shall comply with ethical principles and relevant Union, national and international law, including the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Supplementary Protocols*";
- fully comply with the Universal Declaration of Human Rights (UDHR, 1948), the EU Charter on Fundamental Rights (CFREU, 2010), the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR, 1950) and with the Principles and Good Research Practices as stated in the European Code of Conduct for Research Integrity (ALLEA);
- will only involve adult human voluntary participants who will be appropriately informed before their participation through the respective Information Sheet, and they will freely and voluntarily consent to such participation by signing an appropriate informed consent form;
- fully comply with and respect the applicable national, European and international legislation regarding the protection of personal data, particularly Regulation (EU) 2016/679 (General Data Protection Regulation) and the national law on data protection (Greek Law 4624/2019); to this end, Information Sheet shall be distributed and Consent Form regarding the processing of personal data will be signed by each participant; where the consent cannot be obtained, the processing will be carried out under a different lawful basis and Article 14 (5)(b) GDPR shall apply; the data protection impact assessment conducted under Article 35 GDPR shall be regularly reviewed and updated if necessary;
- will be conducted by taking into consideration the opinions and guidance given by the Ethics Advisory Board and the Data Protection Officer of CERTH.

Project responsible:

Position in the organisation: Scientific Responsible for CERTH for NESTOR Project

[redacted]

[1] https://eur-lex.europa.eu/eli/reg/2021/695/oj

Appendix B: Updated DPIA (CERTH)

VERSION 2.0

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

according to art.35 GDPR

for the NESTOR Project (GA No. 101021851)

1. Who is in charge of the processed personal data and who decides how the data will be used (art.24 GDPR)? Who determines the purposes and the means of the processing operation(s)? Please indicate the full contact details of the data controller(s) or joint controllers (art.27 GDPR).

Answer: CERTH/ITI is in charge of processing personal data and determines the purposes and the means of the processing operations. A Joint Controllership Agreement with other NESTOR partners will be drafted in case this role expands. The DPIA will be updated accordingly.

The contact details of CERTH/ITI are:

CENTRE FOR RESEARCH AND TECHNOLOGY HELLAS (CERTH)/INFORMATION TECHNOLOGIES INSTITUTE (ITI), 6th Km Charilaou - Thermi Road, 57001, Thessaloniki, Greece.

CERTH/ITI's contact points are:

[redacted]

2. If applicable, who is the processor? Are the obligations of the processor(s) clearly identified and governed by a contract (art.28 GDPR)?

Note: If anonymisation or pseudonymisation of the data takes place by a different natural or legal person, this is a processor.

Answer: N/A – All processing operations are performed by CERTH/ITI.

3. What is the processing under consideration?

Describe:

(a) the platform/tool under consideration and its operation,

(b) the nature and the purposes of the processing (refer to the relevant task and deliverables and explain why it is necessary for the project's objectives),

(c) its benefits/stakes.

1

This DPIA is based on the CNIL methodology <https://www.cnil.fr/en/privacy-impact-assessment-pia>

VERSION 2.0

Answer:

NESTOR project aims to demonstrate a fully functional next-generation holistic border surveillance system providing pre-frontier situational awareness beyond maritime and land border areas following the concept of the European Integrated Border Management. All involved technologies will form an interoperable network to detect, assess and respond to hazardous situations in border surveillance missions in both land and maritime operations. For that reason, the main outcome of the project - NESTOR BC3i system - will fuse in real-time border surveillance data combined with web and social media information, creating, and sharing a pre-frontier intelligent picture to local, regional, and national command centres in AR environment being interoperable with CISE and EUROSUR. The envisaged platform addresses the problem of providing enhanced and integrated situation awareness to the operational personnel acting in-situ and in command centres by developing (i) mixed reality technologies for enriched representation for border security tools, (ii) AI-based decision-support services and tools for field and command centre operators, and (iii) the required communication infrastructure with high-speed transmission and increased bandwidth links.

The activities where CERTH participates, will enhance the identification and development of the required NESTOR enhanced functionalities for accurate detections and improved sensing, through social media monitoring as well as through the analysis of data collected by other sources such as visual detection activities through drones and CCTV.

4. What are the data processed?

(a) Set out a detailed list of the data processed, by category.

(b) Set out a detailed list of the personal data, i.e. data which relate to an identified or identifiable natural person.

(c) Mention whether the personal data belong to special categories according to art.9 (1) GDPR.

This DPIA is based on the CNIL methodology <https://www.cnil.fr/en/privacy-impact-assessment-pia>

VERSION 2.0

The content of the stored posts is limited only to text (and the relevant metadata) without any images and with no reference to personal data. However, due to the inherent nature of social media posts, the processing of personal data might happen accidentally. Such data might include names and surnames, birth dates, birth places, marital status, addresses, tax information, and phone numbers. Due to the nature of the social media posts of interest there is a very low probability to collect posts revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data related to genetic data, biometric data, data concerning health, sex life or sexual orientation. However, the project is not expected to contain personal data belonging to the special categories described in art. 9 (1) of the GDPR. In any case and in accordance with the data minimisation principle, only the parts of the social media posts that are deemed necessary for the project's objectives will be processed subject to a privacy-by-design technique, while the majority will be deleted immediately. These data will be required for the duration of the project: (i) for scientific research purposes, (ii) to facilitate the functionality of other modules of the project, and (iii) for demonstration purposes.

c. Finally, data will be collected from other sources which will also adhere to the Data Minimization Principle, with CERTH ensuring to process only the needed data for the project's scope. All the personal identifiers (if any) will be removed (e.g., Photos blurring etc.) before being further processed, so that access to raw data with further links to personal data will not be possible.

In the case of collection and processing of any other data except for the above mentioned, we will proceed with a new updated version of the present DPIA in order to add the further personal data that may be collected in the framework of the project.

For the data processing that will take place after the completion of the project in the framework of the project results in commercial exploitation, another DPIA will be conducted, adapted to the new requirements.

5. If the processing of personal data occurs, would you be able to estimate the amount of processed data, the number of data subjects involved, and the geographical area covered?

Note: A larger number of processed personal data and data subjects would mean higher severity of impact in case of a data breach. The same if a bigger geographical area is affected.

Answer:

The final number of the data related to social media platforms (along with the dedicated profiles) cannot be precisely estimated, nor their data subjects, as the final number will depend on the relevant outcomes and the user requirements. For social media, since the official APIs will be used, additional limitations regarding the social media posts collected might also exist. Finally, due to the global nature of the Internet, there is no specific geographical area that it can be determined, nor a specific number of data subjects affected by the processing.

As far as the data collected from other sources, they can be only deterministically estimated, as they will depend on the quality of the data that can be extracted as well as on their relevance with the scope of the project and within the scope of each trial executed at these locations. An approximate amount of 10 events per 5 months can be an initial estimation. The geographic area will cover the Greek-Turkish borders, but from the Greek side only, as well as a sea area in Cyprus.

6. If the processing of personal data occurs, how frequently will be the data collected?

Note: More frequent collection entails a larger number of data and higher severity of impact in case of a data breach.

Answer:

The frequency that the data will be collected depends on the source type, the user requirements and generally it is something that cannot be easily foreseen. The crawler can check for content changes between consecutive crawls of the same page and, if the content of the page remains the same, will reduce the monitoring frequency automatically. The gathering module allows the manual configuration of the monitoring frequency for each source.

7. Are the processing purposes specified, explicit and legitimate? Can you achieve the same purpose without the processing? Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Answer:

It is foreseen that through the processing of the collected data from various sources useful intelligence will be generated for achieving the purposes of the project, i.e. (i) for scientific

VERSION 2.0 NESTOR

research purposes, (ii) to facilitate the functionality of other modules of the project, and (iii) for demonstration purposes. In any case, these processing purposes are specified, explicit and legitimate according to data protection legislation. Due to the fact that generally the algorithms are considered to be data hungry; they need a great volume of to achieve the purpose they have been developed. Due to the evolving nature of the Internet, further processing might be needed to expand the NESTOR tools capabilities of extracting higher quality intelligence on the field, thus the whole process will be a rather dynamic one throughout the whole lifespan of the project (also, see answer no. 8, below).

8. Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization principle)?

Present a detailed list of the data processed, reduced to what is strictly necessary, alongside the justification of this need as well as any additional minimization controls.

Answer:

The collected data will be used for training and offline validation of the models' performance. This is a very challenging task and requires several data from various sources collected, analysed, correlated, and combined to extract useful intelligence for the successful delivery of some of the end-users' requirements and cover the project's objectives. Processing less data might negatively impact the results of the project as it will limit our capabilities of extracting higher quality outcomes.

The collected data will mostly include non-personal information In accordance with the data minimisation principle, only the parts of the social media posts that are deemed necessary for the project's objectives will be processed subject to a privacy-by-design technique, while the majority will be deleted immediately.

9. What is the storage duration of the data?

Set out in detail for each data type:

(a) the storage duration,

(b) the justification of the storage duration and

(c) the erasure mechanisms at the end of the storage (for sensitive data and high-risk data should be made use of secure erasure tools that make the data irretrievable).

Note: The data should be kept no longer than the period necessary for the purposes pursued.

Answer:

VERSION 2.0

All data will be stored in secure servers within the organization's premises, which are only accessible to authorized individuals with a unique set of usernames and passwords. A firewall will also be in place to allow only specific (whitelisted) IPs to access the server and to restrict the access of each whitelisted IP only to specific ports/services. Devices that will store a backup of the data will follow the same security procedures as the main server. For any remote interactions with the server (e.g., remote control or data transfer), secure protocols are used. Any processing of the data is performed on that server. In case processing will be needed on other machines, the same security measures of the server will be applied to the respective machine. The metadata of the social media and the webpages will be also stored in a local database that is secured (authentication mechanisms are enabled) and is also IP protected.

The storage of collected data is realised according to the EC's guidelines and is up to 5 years after the completion of the project for auditing purposes. Then, specific protocols are followed for the destruction of the aforementioned data. These data will be required for the duration of the project: (i) for scientific research purposes, (ii) to facilitate the functionality of other modules of the project, and (iii) for demonstration purposes.

10. What is the legal basis making the processing lawful? In case of further processing of previously collected data, also justify compatibility.

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purposes for which the personal data are initially collected, take into account *inter alia*:

- any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

- the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

- the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed;

- the possible consequences of the intended further processing for data subjects;

- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Answer:

VERSION 2.0

Lawful Basis:

a. Consent of Art.6(1)(a) GDPR, for the dedicated SN profiles

b. Legitimate Interest of Art 6(1)(f) GDPR, following the safeguards and limitations as described in Art. 5(1b), and Art. 89 GDPR for the social platforms crawling activities and data from other sources (e.g., CCTV), in the sense also of Recital 50 GDPR (scientific research purpose)

11. How are the data subjects informed about the processing?

Describe the controls intended to provide information to users alongside the justification of the arrangement for or the impossibility of implementing them.

Answer:

For the data retrieved by the social platforms as well as from other sources (CCTV, etc.) Information for Data Subjects section is envisioned to be added in the project's website for informing the individuals for the processing of personal data not obtained from them (art. 14GDPR) as an effort of enabling the data subjects to exercise their rights. There specific information will be provided concerning the aims and objectives of the NESTOR project, the categories of collected and processed data, the purpose of data processing, the contact details of the relevant project representatives, as well as the rights of the data subjects will be explicitly outlined. Please note that the information of the data subject may be restricted to some extent in the light of the GDPR (e.g., art. 14 (5) (b) GDPR) or other applicable data protection legislation.

For the data retrieved by the dedicated Social Networking profiles that will be created among Consortium partners only for the needs of the project, a dedicated informed consent and Information Sheet will be created, distributed, and signed by the participants, fully aligned with Art.6(1)(a) GDPR.

12. If applicable, how is the consent of the data subjects obtained?

Answer:

For the data retrieved by the dedicated Social Networking profiles that will be created among Consortium partners only for the needs of the project, a dedicated informed consent and Information Sheet will be created, distributed, and signed by the participants, fully aligned with Art.6(1)(a) GDPR.

13. How can the data subjects exercise their rights to access and to data portability?

Answer: The nature of the data (a and c case) as well as the way they are collected does not allow the option for the data subjects to exercise their right to access. This is in accordance

VERSION 2.0

with the limitation stipulated for scientific research purposes in art. 89 par. 2 GDPR and art. 30 par. 2 Greek Law 4624/2019. However, the information will be made publicly available via the project's website as an effort of enabling the data subjects to exercise their other rights.

In addition, the principle of data portability does not apply when the legal basis is not the consent of the data subject or the need of the performance of a contract to which the data subject is a party, hence, this is not applicable in this case.

As far as the b case is concerned, participants will be able to exercise their rights (including the right to access and the right to data portability) that have been presented to them via the respective information sheet (to be developed), as they will also be provided all the relevant contact information of the respective person(s) responsible for the data collection and processing

14. How can the data subjects exercise their rights to rectification and erasure?

Answer: The nature of the data as well as the way they are collected do not allow the option for the data subjects to exercise their rights to rectification and erasure. This is in accordance with the limitation stipulated for scientific research purposes in Art. 17(3)(d) GDPR, Art. 89 (2) GDPR and Art. 30 par. 2 Greek Law 4624/2019. However, the information will be made publicly available via the project's website as an effort of enabling the data subjects to exercise their other rights .

As far as the b case is concerned, participants will be able to exercise their rights that have been presented to them via the respective information sheet (to be developed), as they will be also provided all the relevant contact information of the respective person(s) responsible for the data collection and processing.

15. How can data subjects exercise their rights to restriction and to object?

Answer: The nature of the data as well as the way they are collected do not allow the option for the data subjects to exercise their rights to restriction and to object. This is in accordance with the limitation stipulated for scientific research purposes in art. 89 par. 2 GDPR and art. 30 par. 2 Greek Law 4624/2019.

However, the information will be made publicly available via the project's website as an effort of enabling the data subjects to exercise their other rights.

As far as the b case is concerned, participants will be able to exercise their rights that have been presented to then via the respective information sheet (to be developed), as they will be also provided all the relevant contact information of the respective person(s) responsible for the data collection and processing.

16. How do you document your processing operations? Who has access to this documentation and up to what extent?

VERSION 2.0 NESTOR

Answer: The processing operations will be included in deliverables D3.1 "Visual cognition algorithms for optimal surveillance", D3.4 "Web and social media monitoring services", D4.3 "data fusion models".

Additionally, CERTH/ITI maintains a record of processing activities under its responsibility in accordance with Article 30 (1) GDPR. The record is made available to CERTH'S Data Protection Officer and shall be also made available to the competent supervisory authority upon request or to the data subject requesting access. That record contains all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative, and the data protection officer.
(b) the purposes of the processing.
(c) a description of the categories of data subjects and of the categories of personal data.
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations.
(e) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards.
(f) where possible, the envisaged time limits for erasure of the different categories of data.
(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

17. Are there any recipients of the collected data?

Answer:

The collected pseudonymised data will be stored in CERTH/ITI's premises. Additionally, the collected pseudonymized data will be received and used by STWS for the realization of the relevant trials (EL-BG Trial). In that case, STWS acts as the data controller of this data processing.

18. In the case of data transfer outside the European Union, are the data adequately protected according to Chapter V of the GDPR?

Set out in detail the geographic storage location of the platform/tool, alongside justification of the choice of remote hosting (if any) and indication of the arrangements implemented (e.g. Adequacy Decision, standard contractual clauses etc. based on Chapter V GDPR) in order to ensure adequate protection of the data.

Answer:

N/A

VERSION 2.0 NESTOR

19. How do you demonstrate compliance with data protection law, including the measures that you take in order to ensure that the data processors also comply? Do you or/and the data processor(s) have appointed a DPO (art.37 GDPR)?

Answer:

A DPO has been appointed [redacted]

Additionally, the technical, organisational measures, and security measures that are implemented to ensure compliance with the GDPR provisions are:

[1] Adoption of certain technical measures to allow pseudonymisation (please check our reply above), thus ensuring data minimization.
[2] All crawling activities will adhere to the terms of the official APIs of the social media platforms.
[3] The server hosting all data is accessible only by authorised users through authentication (using passwords of high complexity). A firewall will also be in place to allow only specific (whitelisted) IPs to access the server and to restrict the access of each whitelisted IP only to specific ports/services.
[4] Different access privileges to the database will be available in order to ensure that the authorised users will only have access to the stored data on a need-to-know basis, i.e. that the authorised users will have access only to the stored data needed in order to fulfil their tasks.
[5] The server is located inside a locked room, accessible only by authorised personnel through authentication (using passwords of high complexity). A firewall will also be in place to allow only specific (whitelisted) IPs to access the server and restrict the access of each whitelisted IP only to specific ports/services.
[6] Devices that will store a backup of the data will follow the same security procedures as the main server.
[7] For any remote interactions with the server (e.g., remote control or data transfer), secure protocols [redacted] are used.
[8] Any processing of the data is performed on that server. In case processing will be needed on other machines, the same security measures of the server will be applied to the respective machine.
[9] If none of the collected personal data are deemed useful for the project, they will be immediately deleted or anonymized.

20. Are there standards applicable to the processing?

List the sector-specific standards applicable to your processing (e.g., code of conduct according to art.40 GDPR, a certification according to art.42 GDPR, a security policy).

VERSION 2.0 NESTOR

Answer: CERTH has an internal security policy.

21. Are the data accurate and kept up-to-date?

Set out in detail the data quality compliance controls, carried out on the device, as well as a justification of the arrangement for or impossibility of implementing them (e.g. regular checks, traceability of data amendments).

Answer:

The social media crawler will support the option to continuously monitor sources of interest and to update the local copies when discrepancies are found. However, this will be dependent on the user requirements as they have been extracted for the project.

22. What security measures do you implement in order to ensure data security and integrity (art. 32 GDPR)?

Answer: Please check answer 19 (Bullets 3-9)

23. If processing of personal data occurs, is the access to the personal data restricted? What are the rules of access (with special attention to its conditions, mode, and limits)?

The details of processing operations should be clarified and documented (via, e.g. logs, permissions).

Answer: Different access privileges to the data will be available in order to ensure that the authorised users will only have access to the stored data on a need-to-know basis, i.e., that the authorised users will have access only to the stored pseudonymised data needed in order to fulfil their tasks. Since the list of the types of data required by the other modules of the project is not finalised, the rules will be constantly updated based on the current needs of each module. This DPIA will be updated accordingly.

24. What is the nature of your relationship with the individuals whose personal data will be collected? Would they have a reasonable expectation that their data are used this way? Would they object if they knew?

Note: In order for some legal grounds to be applicable and the data subjects to be able to enforce their rights and freedoms fully, it is important that the data subjects have a reasonable expectation that their data are processed.

Answer:

For data collected from social media platforms and other sources, no direct communication is envisioned with the individuals, as they will be mainly social media users or online users. For transparency reasons, an Information for Data Subjects section is envisioned to be added

in the project's website for informing the individuals about the processing of personal data not obtained from them (art. 14 GDPR) as an effort of enabling the data subjects to exercise their rights.

For the data collected by the dedicated SN profiles, they will be personally and duly informed on the aims of the activity, the way their data will be used, the benefits and potential risks of their participation, their rights, any relevant data protection issues, they will be given contact details in case they would request more info and they will also sign a relevant consent form.

25. Have you adopted or will you adopt procedures for dealing with data breaches and notification of breaches to the national supervisory authority or to the affected individuals, if applicable (art.33-34 GDPR)?

Answer:

In case of data breach Art. 33 and 34 of GDPR are applicable. CERTH's procedure enshrines the following steps: 1. All the necessary actions to stop the breach 2. Filing of all the information regarding the data breach 3. Analysis of the causes and the consequences of the incident 4. Legal analysis of the incident 5. Organization of the responding system to requests for information by the data subjects.6. Notification of the data breach to the Hellenic Data Protection Authority and to the data subjects, when this is considered as necessary, according to GDPR. 7. Organization of a recovery plan.

VERSION 2.0

26. Describe the sources of potential risks and the nature of the potential impact on individuals. Evaluate the impact based on the figure below. If there are more than one risk, add more tables.

Severity of impact	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Answer:

Risk: Data processed on a large scale as part of systematic monitoring*
likelihood of harm: Reasonable Possibility
severity of impact: Some Impact
likelihood of occurrence of the risk: Medium Risk

* Due to the nature of the tool (crawler), it is possible that personal data will be processed on a large scale (however this is not final yet). However, not all data are deemed useful for the project, hence, they will be deleted. For those that are deemed useful, safeguards will be implemented.

Risk: Sensitive data or data of a highly personal nature*
likelihood of harm: Remote
severity of impact: Serious Harm
likelihood of occurrence of the risk: Low Risk

* Sensitive data or data of a highly personal nature, as due to the nature of social media posts they might include special categories of personal data of article 9 GDPR, such as political, religious views, racial or ethnic origin.

Risk: The processing itself prevents the data subject from exercising a right*
likelihood of harm: More likely than not
severity of impact: Minimal impact
likelihood of occurrence of the risk: Low Risk

*Due to its nature data processing through a crawler prevents the data subject from exercising the rights related to data protection. However, in the course of scientific research, the GDPR research privileges exclude certain rights for the data subject. Additionally, art. 14 (5) (b) applies. Appropriate safeguards are implemented

27. Identify envisaged measures to reduce or eliminate the risks depicted as medium or high in the previous question (e.g., privacy by design, encryption, pseudonymisation, anonymisation).

VERSION 2.0

Answer:

For the risks "data processed on a large scale as part of systematic monitoring" and "sensitive data or data of a highly personal nature:

In compliance with Art.89 (1) GDPR, rule-based pseudonymisation techniques will be utilised for the pseudonymisation of the data if deemed useful by the project or deletion of the data if otherwise (the latter is the most possible).

For the risk "the processing itself prevents the data subject from exercising a right":

In the context of personal data processing for scientific research purposes (as in NESTOR), limitations of data subjects' rights are stipulated by the GDPR and Greek data protection law. In compliance with the transparency requirements of the GDPR and in line with Art 14(5)(b) GDPR, an *Information for Data Subjects* section is envisioned to be added in the project's website for informing the individuals for the processing of personal data not obtained from them (art. 14(5)(b) GDPR) as an effort of enabling the data subjects to exercise their rights. There specific information will be provided concerning the aims and objectives of the NESTOR project, the categories of collected and processed data, the purpose of data processing, the contact details of the relevant project representatives, as well as the rights of the data subjects will be explicitly outlined.

28. Do the aforementioned measures reduce or eliminate the risks in practice? Specify.

Answer: We strongly believe that the aforementioned measures considerably reduce the risks depicted as medium in question 26. By immediately deleting or pseudonymising by design any personal data no high risks are expected to the rights and freedoms of the data subjects. The better the utilised pseudonymisation techniques are, the lower the risks will be.

Due to the nature of the processing activity, it is impossible to obtain the consent of the data subjects and it is impossible/would require disproportionate effort to inform the data subjects about the processing of their personal data. Therefore, apart from the implementation of the aforementioned measures, the information of art.14 GDPR will be made publicly available through the official website of the project, to enable the data subjects to exercise their rights.

The appointment of a Data Protection Officer within CERTH, the existence of an internal security policy and the keeping of records of processing activities constitute additional safeguards.

This DPIA is a living document, and it will be updated in case any information included herein changes within the lifetime of the NESTOR project (e.g., new risks, new mitigating measures, change of the controller, new recipients of data etc).

29. Opinion of the Data Protection Officer

Data processing has been reviewed for its compliance with the applicable data protection legislation by CERTH's DPO and this document was drafted under advice. DPO confirmed that the data processing can proceed. DPO advice was provided on 02/06/2022. A further review of the current updated DPIA (version 2.0) was conducted on 3/3/2023 by CERTH's DPO.

Appendix C: Ethics guidelines for the Cypriot trial

ETHICS GUIDELINES
for the NESTOR pilot demonstrations
Human Participation in research activities (questionnaires, workshops, pilots or other research activities)
When the research activities involve human participants (interviews, workshops, trainings, pilot demonstrations, other tests), the criteria and the procedures for the recruitment of these participants must be explicitly described.
The participants will be selected by the researcher based on (inclusion criteria): • Their age (only adults will be involved); • Their state of health (only physically and mentally healthy humans will be involved); • Their free will to participate (an informed consent procedure will be followed); • Their knowledge and experience on the field (e.g., certified UAV operators); • Their working position (relation to the end-users)
The NESTOR Consortium will not recruit (exclusion criteria): • Any person under the age of 18; • Participants that are considered vulnerable (patients, incompetent/incapacitated persons, refugees/asylum seekers, minors, unaccompanied minors, disabled people, elderly people, pregnant women, single parents with minor children, victims of trafficking in human beings, persons with serious illnesses, persons with mental disorders and persons who have been subjected to torture, rape or other serious forms of psychological, physical or sexual violence); • If the COVID-19 pandemic crisis remains until the carrying out of the pilots, any person not willing to follow the guidelines issued by the Government or the Ministry of Health at that time. • Any person that has not followed the informed consent procedure or has withdrawn their consent.
The voluntary character of the entire procedure must be clearly declared and fully respected by the researcher by following an informed consent procedure.
The informed consent procedure will be followed for all participants, irrespective of their position and role in the project, meaning the members of the NESTOR Consortium, external actors and the personnel of public authorities.
Consent of the participants must be clearly and freely given by them before their participation and only after they have been fully informed about the specific conditions and characteristics of the research activity through an Information Sheet.
Informed Consent Forms for the participation of humans in research will be signed by the participants.
The language of the Information Sheet and of the Informed Consent Form will be English, while with respect to the pilot demonstrations, the form will be translated to the native language of the participants, if needed.
A representative of the lead researcher present at the scene will be there to assist the participants and answer to their questions.
The participants can withdraw their consent at any time without consequences.

Volunteers acting in the scenarios will assume the various roles (both the roles involving criminal action as well as the roles involving counter criminal action) in such a way that those roles will refer to a variety of different social characteristics in a random manner (i.e., gender, race, religion, sexual orientation, political beliefs, ethnicity etc.)
The personal information on the Informed Consent Form will be processed in compliance with the GDPR and will be stored securely by the data controller(s) for 5 years after the completion of the project for accountability reasons and in accordance with Articles 18.1 and 22.1 of the NESTOR Grant Agreement.
Incidental findings, i.e., findings that are outside the research's scope, may be detected during the research activities (criminal activity or processing of personal data of non-volunteers).
The NESTOR Consortium is advised to notify the Project Ethics Officer (KEMEA) in case of incidental findings.
The NESTOR Consortium is advised to follow the "Law of the Land approach" – i.e., to maintain compliance with the applicable legislation in the country in which the research activity is carried out and personal data are collected.
Criminal activity witnessed or uncovered in the course of research must be reported to the responsible and appropriate authorities, even if this means overriding commitments to participants to maintain confidentiality and anonymity.
Personal Data Protection
When the research activities involve human participants, the processing of their personal data by the researcher (data controller) is based on their consent according to article 6(1)(a) GDPR.
The informed consent procedure will be followed for all participants (data subjects), irrespective of their position and role in the project, meaning the members of the NESTOR Consortium, external actors and the personnel of public authorities.
Consent of the data subjects must be clearly and freely given by them before their participation and only after they have been fully informed about the data processing operations through an Information Sheet.
The Information Sheet includes the information required to be provided to the data subjects according to article 13 GDPR (types of data, purposes of processing, lawful basis, storage period, data protection rights, etc.).
The data subjects will be given through the Information Sheet the contact details of the Data Protection Officer (DPO) appointed within the data controller in order to ask any questions and exercise their rights related to data protection. In the absence of a DPO, the data subjects will be given through the Information Sheet the contact details of the Project Ethics Officer (KEMEA) and of a contact person on behalf of the data controller.
Informed Consent Forms for the processing of personal data will be signed by the data subjects.
The language of the Information Sheet and of the Informed Consent Form will be English, while with respect to the pilot demonstrations, the form will be translated to the native language of the data subjects, if needed.
The data subjects can withdraw their consent at any time without consequences. The withdrawal does not affect the processing of personal data already carried out before their relevant request.

The personal information on the Informed Consent Form will be processed in compliance with the GDPR and will be stored by the data controller(s) securely for 5 years after the completion of the project for accountability reasons and in accordance with Articles 18.1 and 22.1 of the NESTOR Grant Agreement.
The data controller will seek consultation from the appointed DPO. In the absence of a DPO, the data controller will follow the NESTOR data protection policy included in D8.3 POPD-Requirement No.3.
The data controller will implement the security measures included in D8.3 POPD-Requirement No.3 to ensure appropriate security of the personal data processed during the research including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage of personal data.
Transfer of personal data outside the EU will be held in accordance with Chapter V of the GDPR. Any transfers of personal data: • to CENTRIC (UK) and DCD (Switzerland): in accordance with Article 45 GDPR, as the European Commission has adopted adequacy decisions for the United Kingdom and for Switzerland • to DBAM (Republic of North Macedonia): in accordance with Article 49 GDPR which stipulates derogations for specific situations. Derogations can occur in compliance with the GDPR provisions if the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards (Article 49 (1) (a)GDPR) and if the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request (Article 49 (1) (b) GDPR).
The data subjects will be informed by the data controller about a potential transfer of their personal data outside the EU through the Information Sheet and any transfer will occur based on their consent.
Any further processing of previously collected personal data will be carried out under a lawful basis and with the implementation of appropriate safeguards (technical and organisational measures). not applicable in the Cypriot Trial
In cases where the consent of the data subjects cannot be obtained or would require disproportionate effort, another lawful basis is sought and article 14 GDPR applies (implementation of technical and organisational measures, such as anonymisation/pseudonymisation, including making the information about the processing publicly available to the data subjects). not applicable in the Cypriot Trial
A Data Protection Impact Assessment (DPIA) of article 35 GDPR is conducted by the data controller in case the processing is likely to result in high risks to the rights and freedoms of the data subjects. The DPIA is a living document that must be updated in case of changes. not applicable in the Cypriot Trial
Health and Safety procedures
Requirements with respect to the "open category" of UAS operations (art.4 Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft):

- No prior authorisation is needed for this category. Operational risks in the 'open' category are considered low and, therefore, no operational authorisation is required before starting a flight.
- The operator will have direct visual contact with the unmanned aircraft, at a distance of not more than 500 meters and will rely on this visual contact to carry out any necessary operating actions, in order to monitor the flight path of the aircraft in relation to other aircraft, persons, animals, vehicles, buildings and structures for the purpose of avoiding collisions.
- No autonomous flights will take place. 'Autonomous operation' means an operation during which an unmanned aircraft operates without the remote pilot being able to intervene (art.2 (17) Regulation (EU) 2019/947). An autonomous operation should not be confused with an automatic operation, which refers to an operation following pre-programmed instructions that the UAS executes while the remote pilot is able to intervene at any time.
- The drones will be operated according to the safety rules which require good weather.
- The drones' take-off weight is less than 25kg.
- The drones will not fly above the altitude of 120m.
- The drones will not fly at night.
- The drones will not fly over assemblies of persons. 'Assemblies of people' means gatherings where persons are unable to move away due to the density of the people present (art.2 (3) Regulation (EU) 2019/947).

Additional safeguards/requirements:

- Only rational and healthy adults that will follow the informed consent procedure will participate in the pilot demonstrations.
- All project's research activities, including UAV flights, will be carried out in a controlled environment.
- The drones will be operated by experienced certified UAV pilots following all safety regulations and the instructions given in the User Manual.
- Highly qualified LEA officers from the NESTOR Consortium will be present at the pilot sites.
- The research activities that cannot be carried out remotely will involve a low number of participants (the minimum number needed for the operation of the tools and technologies and for the project's objectives to be successfully served).
- The drones will not fly in airport zone and over cultural heritage monuments.
- The drones will not carry dangerous goods that may result in high risk for third parties in case of accident. Only portable sensors will be onboard UAVs.
- The drones will not involve the transport of people.

Additional safeguards/requirements:

- Only rational and healthy adults that will follow the informed consent procedure will participate in the pilot demonstrations.
- All project's research activities, including UGV testing activities, will be carried out in a controlled environment.

- Only specialised operators from ROB and trained staff from the NESTOR Consortium will use the UGVs in accordance with the safety instructions of the User Manual.
- ROB personnel will be present ensuring that the safety instructions are followed during the operation of the UGV.
- Highly qualified LEA officers from the NESTOR Consortium will be present.
- The research activities that cannot be carried out remotely will involve a low number of participants (the minimum number needed for the operation of the tools and technologies and for the project's objectives to be successfully served).

Unmanned Underwater Vehicles (UUVs) and Unmanned Surface Vehicles (USVs)

Safety instructions for UUVs:

- In case a vehicle gets stuck under the water during operation, the following procedure is followed:
  1. Make sure the vehicle is static in its position. Diagnose the error and note down the location.
  2. Contact local authorities about this incident and request the intervention of a diving team.
  3. Communicate the coordinates of the vehicle, including its depth to the diving team.
  4. Make sure that the propeller will not be activated during the intervention.
  5. Instruct the diving team on how to handle the vehicle while under the water and how to bring the vehicle back to the surface.

- In case the operator loses contact with the UUV, the following procedure is followed:
  1. Make sure the vehicle is not on the surface (using GSM and Satellite communications)
  2. Execute the same path the vehicle should be doing with a vessel and stop every 500 meters to place hydrophone and acoustic modem in the water and try to locate the vehicle near this position.
  3. If the previous approaches fail to locate the UUV, warn the local authorities about the missing equipment. Also warn the insurance company about the incident.
  4. Keep repeating the search procedure above. Also using binoculars to search the ocean surface. The vehicle is more visible at night time (blinking led) than it is during the day. Make sure that a vessel and crew are available and are allowed to sail at night.

- In case there is a collision with surface traffic, the following procedure is followed:
  1. Make immediate contact with the vessel that collided with the UUV, as required by the insurance provider.
  2. Recover the UUV.
  3. Assess the damage on the UUV and surface vessel.
  4. Re-validate the vehicle readiness to operate before redeploying the vehicle to the water. Warn the insurance company about the incident, in case of any damage.

Additional safeguards/requirements:

- Only rational and healthy adults that will follow the informed consent procedure will participate in the pilot demonstrations.
- All project's research activities, including UUV/USV testing activities, will be carried out in a controlled environment.
- Only specialised operators from OMST and trained staff from the NESTOR Consortium will use the UUV/USV.

- OMST personnel will be present ensuring that the safety instructions and any recommendations of the local authorities are followed during the operation of the UUV/USV.
- Highly qualified LEA officers from the NESTOR Consortium will be present.
- The research activities that cannot be carried out remotely will involve a low number of participants (the minimum number needed for the operation of the tools and technologies and for the project's objectives to be successfully served).
- Authorisation will be obtained by the local maritime authorities.
- A navigational warning shall be placed by the authorities restricting the traffic in the area of operation or simply warning other traffic about the potential hazard.
- No humans will swim in the area of operation.

Additional safeguards/requirements:

- Only rational and healthy adults that will follow the informed consent procedure will participate in the pilot demonstrations.
- All project's research activities, including radar and RF system testing activities, will be carried out in a controlled environment.
- The devices will be operated by experienced and trained staff from HEN and NARDA and trained staff from the NESTOR Consortium following all safety regulations and the instructions given in the User Manuals.
- As underlined in Recital 11 of the Directive 2013/35/EU, the undesired effects on the human body depend on the frequency of the electromagnetic field or radiation to which it is exposed. No frequent exposure is planned during the NESTOR research activities and the required distances must be kept.
- Highly qualified LEA officers from the NESTOR Consortium will be present.
- The research activities that cannot be carried out remotely will involve a low number of participants (the minimum number needed for the operation of the tools and technologies and for the project's objectives to be successfully served).

Augmented Reality (AR) tools not applicable in the Cypriot Trial

- The participants will be informed that they must stop using AR devices as soon as symptoms such as nausea, dizziness, sweating, and pallor appear.
- The participants will be informed that they need to take a rest for one to two hours after using AR devices.
- These technologies should be avoided by people with epilepsy, or anyone identified as vulnerable, e.g., people suffering from motion sickness or balance problems, or susceptible to migraines, etc.

Additional safeguards/requirements:

- Only rational and healthy adults that will follow the informed consent procedure will participate in the pilot demonstrations and in all research activities.
- All project's research activities, including AR testing activities, will be carried out in a controlled environment.

COVID-19

The necessary health and safety measures will be implemented during the pilots in accordance with the current national laws and guidelines in the country of the pilot.

Dual use

Dual-use items in the sense of Regulation 2021/821 means items, including software and technology, which can be used for both civil and military purposes, and includes items which can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery, including all items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices.

In two cases, authorisations are required on a constant basis:

a) for the export of dual-use items listed in Annex I and

b) for the intra-Union transfers of dual-use items listed in Annex IV.

For the other cases, authorisations are required on a case-by-case basis, if the items are or may be intended for the uses referred to in Article 4 (1) of the Regulation 2021/821.

All NESTOR partners have identified whether the NESTOR research activities involve dual-use items for which an authorisation is required.

Involvement of Non-European Countries

No import of materials to non-EU countries will take place.

Potential misuse of the research findings

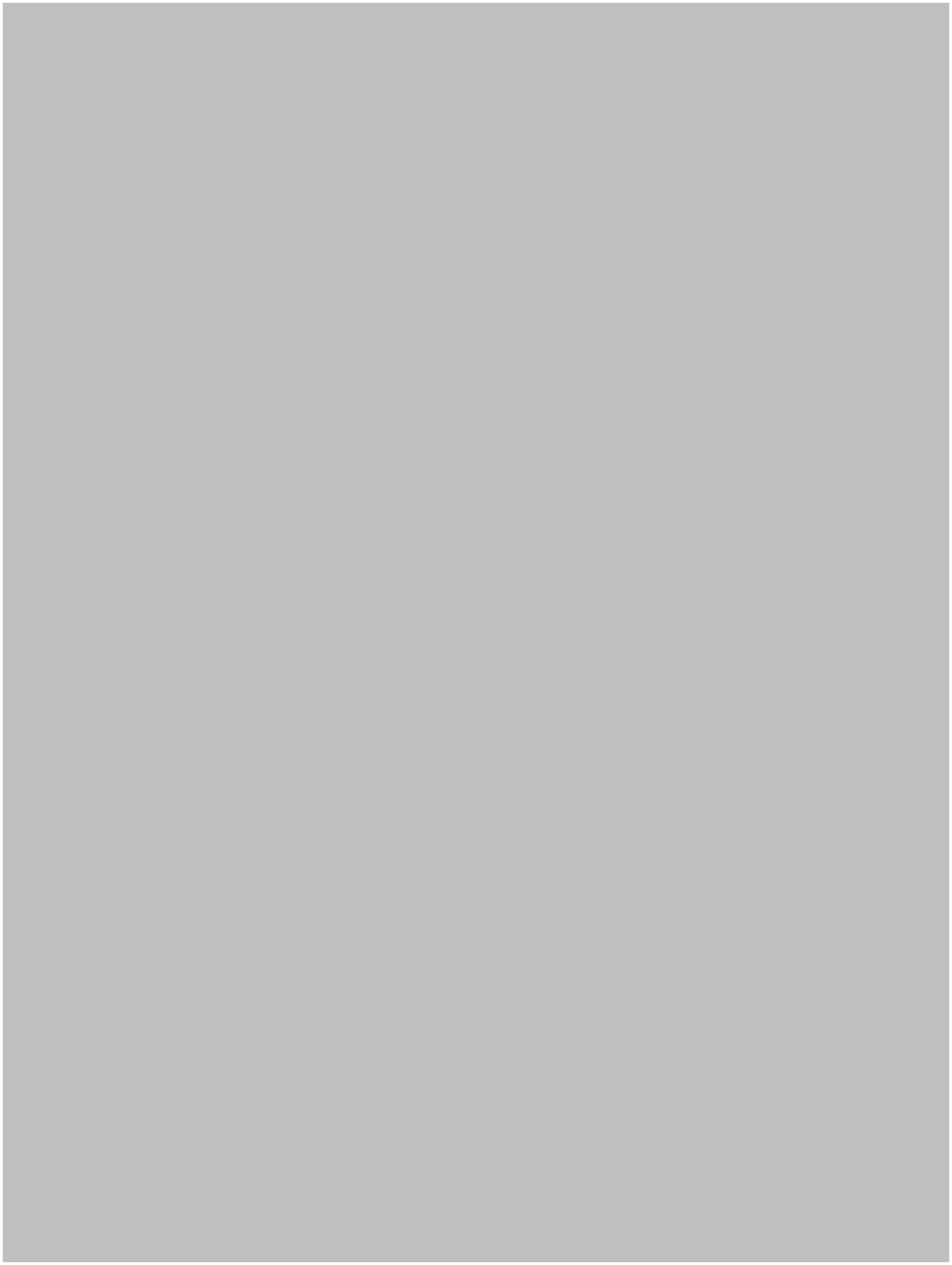
A misuse mitigation strategy has been created for the NESTOR project including ex-ante and ex-post protective mechanisms.

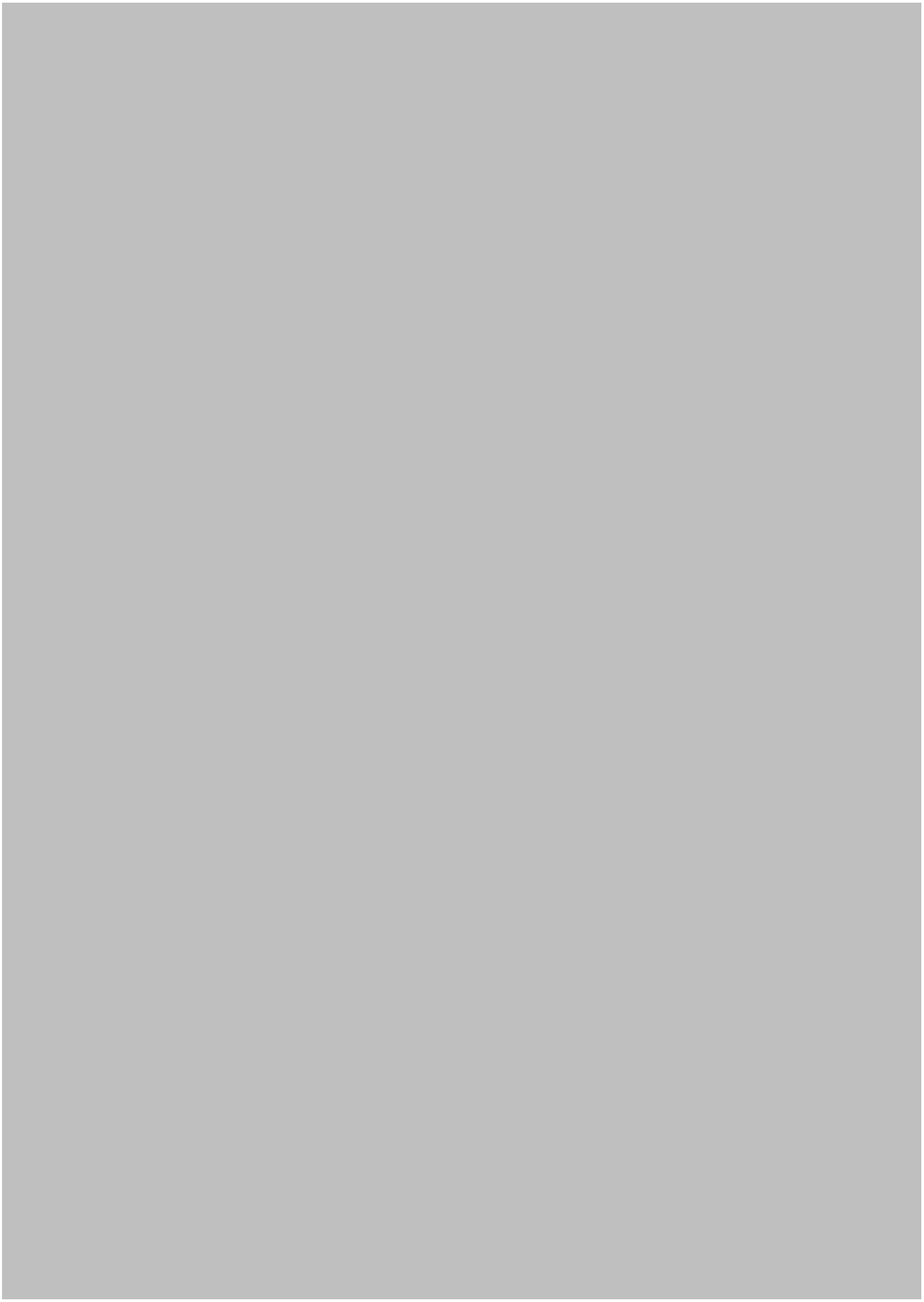
Ex-ante mechanisms:

1. Establishing an ongoing monitor and review process is one of the most critical factors affecting the effectiveness of a risk assessment. This process will be carried out by the ethics and security experts of the project as well as by the EC for the specified management action plans to remain relevant, accurate and updated. The NESTOR project has appointed a Project Ethics Officer (PEO), an Ethics Advisory Board (EtAB), a Project Security Officer (PSO) and a Security Advisory Board (SAB) that will closely monitor the research activities from an ethical, legal and security point of view and will work together against potential misuse of the research findings.
2. As part of the deliverable review process, an Ethics Review Form must be filled out by the author of each deliverable. This brings any ethical issues to the foreground during the preparation of each deliverable, serving as a reminder to the Consortium to adhere to best practices. The responses are reviewed by the EtAB.
3. Deliverables that include highly sensitive information which could be misused have been classified as EU RESTRICTED/RESTRAINT EU.
4. Deliverables that include sensitive information which could be misused are disseminated only amongst the Consortium and the EC (CO).
5. Confidentiality undertakings have been signed by parties that are external to the Consortium (External Ethics Advisor, EAB members). Disclosure of any information shared with external parties is prohibited with only few exemptions expressly and exhaustively stipulated in the undertaking.
6. Ethics opinions/approvals have been obtained by ethics committees and, in absence of such committees, declarations of compliance have been signed by the partners prior to the start of research activities with humans. Relevant documentation is included in D8.2 H-Requirement No.2.

Ex-post mechanisms:

1. Sensitive information that includes details on the technologies, methods, materials, knowledge that could be misused will be filtered prior to publications or dissemination events and will not be made available to the public.
2. Sensitive information involved or generated during a project's task will be available solely between the involved NESTOR partners and only to authorised personnel of these partners that have a need-to-know.
3. Encryption of databases that include sensitive information will be implemented during the execution of specific tasks and complex passwords will be utilized for enhanced security as well as constant local data backup or backup in a secondary Cloud ecosystem for the prevention of data loss or data theft due to a potential cyber-attack.
4. Specific technologies will operate in a secure encrypted network channel (VPN).
5. Anonymisation and pseudonymisation of personal data will be implemented in compliance with the GDPR requirements.





Appendix E: Ethics guidelines for the Greek-Bulgarian trial

ETHICS GUIDELINES
for the NESTOR pilot demonstrations (Greek-Bulgarian Trial)
Human Participation in research activities (questionnaires, workshops, pilots or other research activities)
When the research activities involve human participants (interviews, workshops, trainings, pilot demonstrations, other tests), the criteria and the procedures for the recruitment of these participants must be explicitly described.
The participants will be selected by the researcher based on (inclusion criteria): • Their age (only adults will be involved); • Their state of health (only physically and mentally healthy humans will be involved); • Their free will to participate (an informed consent procedure will be followed); • Their knowledge and experience on the field (e.g., certified UAV operators); • Their working position (relation to the end-users)
The NESTOR Consortium will not recruit (exclusion criteria): • Any person under the age of 18; • Participants that are considered vulnerable (patients, incompetent/incapacitated persons, refugees/asylum seekers, minors, unaccompanied minors, disabled people, elderly people, pregnant women, single parents with minor children, victims of trafficking in human beings, persons with serious illnesses, persons with mental disorders and persons who have been subjected to torture, rape or other serious forms of psychological, physical or sexual violence); • If the COVID-19 pandemic crisis remains until the carrying out of the pilots, any person not willing to follow the guidelines issued by the Government or the Ministry of Health at that time. • Any person that has not followed the informed consent procedure or has withdrawn their consent.
The voluntary character of the entire procedure must be clearly declared and fully respected by the researcher by following an informed consent procedure.
The informed consent procedure will be followed for all participants, irrespective of their position and role in the project, meaning the members of the NESTOR Consortium, external actors and the personnel of public authorities.
Consent of the participants must be clearly and freely given by them before their participation and only after they have been fully informed about the specific conditions and characteristics of the research activity through an Information Sheet.
Informed Consent Forms for the participation of humans in research will be signed by the participants.
The language of the Information Sheet and of the Informed Consent Form will be English, while with respect to the pilot demonstrations, the form will be translated to the native language of the participants, if needed.
A representative of the lead researcher present at the scene will be there to assist the participants and answer to their questions.
The participants can withdraw their consent at any time without consequences.

Volunteers acting in the scenarios will assume the various roles (both the roles involving criminal action as well as the roles involving counter criminal action) in such a way that those roles will refer to a variety of different social characteristics in a random manner (i.e., gender, race, religion, sexual orientation, political beliefs, ethnicity etc.)
The personal information on the Informed Consent Form will be processed in compliance with the GDPR and will be stored securely by the data controller(s) for 5 years after the completion of the project for accountability reasons and in accordance with Articles 18.1 and 22.1 of the NESTOR Grant Agreement.
Incidental findings, i.e., findings that are outside the research's scope, may be detected during the research activities (criminal activity or processing of personal data of non-volunteers).
The NESTOR Consortium is advised to notify the Project Ethics Officer (KEMEA) in case of incidental findings.
The NESTOR Consortium is advised to follow the "Law of the Land approach" – i.e., to maintain compliance with the applicable legislation in the country in which the research activity is carried out and personal data are collected.
Criminal activity witnessed or uncovered in the course of research must be reported to the responsible and appropriate authorities, even if this means overriding commitments to participants to maintain confidentiality and anonymity.
Personal Data Protection
When the research activities involve human participants, the processing of their personal data by the researcher (data controller) is based on their consent according to article 6(1)(a) GDPR.
The informed consent procedure will be followed for all participants (data subjects), irrespective of their position and role in the project, meaning the members of the NESTOR Consortium, external actors and the personnel of public authorities.
Consent of the data subjects must be clearly and freely given by them before their participation and only after they have been fully informed about the data processing operations through an Information Sheet.
The Information Sheet includes the information required to be provided to the data subjects according to article 13 GDPR (types of data, purposes of processing, lawful basis, storage period, data protection rights, etc.).
The data subjects will be given through the Information Sheet the contact details of the Data Protection Officer (DPO) appointed within the data controller in order to ask any questions and exercise their rights related to data protection. In the absence of a DPO, the data subjects will be given through the Information Sheet the contact details of the Project Ethics Officer (KEMEA) and of a contact person on behalf of the data controller.
Informed Consent Forms for the processing of personal data will be signed by the data subjects.
The language of the Information Sheet and of the Informed Consent Form will be English, while with respect to the pilot demonstrations, the form will be translated to the native language of the data subjects, if needed.
The data subjects can withdraw their consent at any time without consequences. The withdrawal does not affect the processing of personal data already carried out before their relevant request.

The personal information on the Informed Consent Form will be processed in compliance with the GDPR and will be stored by the data controller(s) securely for 5 years after the completion of the project for accountability reasons and in accordance with Articles 18.1 and 22.1 of the NESTOR Grant Agreement.
The data controller will seek consultation from the appointed DPO. In the absence of a DPO, the data controller will follow the NESTOR data protection policy included in D8.3 POPD-Requirement No.3.
The data controller will implement the security measures included in D8.3 POPD-Requirement No.3 to ensure appropriate security of the personal data processed during the research including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage of personal data.
Transfer of personal data outside the EU will be held in accordance with Chapter V of the GDPR. Any transfers of personal data: • to CENTRIC (UK) and DCD (Switzerland): in accordance with Article 45 GDPR, as the European Commission has adopted adequacy decisions for the United Kingdom and for Switzerland • to DBAM (Republic of North Macedonia): in accordance with Article 49 GDPR which stipulates derogations for specific situations. Derogations can occur in compliance with the GDPR provisions if the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards (Article 49 (1) (a)GDPR) and if the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request (Article 49 (1) (b) GDPR).
The data subjects will be informed by the data controller about a potential transfer of their personal data outside the EU through the Information Sheet and any transfer will occur based on their consent.
Any further processing of previously collected personal data will be carried out under a lawful basis and with the implementation of appropriate safeguards (technical and organisational measures).
In cases where the consent of the data subjects cannot be obtained or would require disproportionate effort, another lawful basis is sought and article 14 GDPR applies (implementation of technical and organisational measures, such as anonymisation/pseudonymisation, including making the information about the processing publicly available to the data subjects).
A Data Protection Impact Assessment (DPIA) of article 35 GDPR has been conducted by the data controllers CENTRIC and CERTH for processing operations that are likely to result in high risks to the rights and freedoms of the data subjects. The DPIA is a living document that must be updated in case of changes.
Health and Safety procedures
Requirements with respect to the "open category" of UAS operations (art.4 Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft):

- No prior authorisation is needed for this category. Operational risks in the 'open' category are considered low and, therefore, no operational authorisation is required before starting a flight.
- The operator will have direct visual contact with the unmanned aircraft, at a distance of not more than 500 meters and will rely on this visual contact to carry out any necessary operating actions, in order to monitor the flight path of the aircraft in relation to other aircraft, persons, animals, vehicles, buildings and structures for the purpose of avoiding collisions.
- No autonomous flights will take place. 'Autonomous operation' means an operation during which an unmanned aircraft operates without the remote pilot being able to intervene (art.2 (17) Regulation (EU) 2019/947). An autonomous operation should not be confused with an automatic operation, which refers to an operation following pre-programmed instructions that the UAS executes while the remote pilot is able to intervene at any time.
- The drones will be operated according to the safety rules which require good weather.
- The drones' take-off weight is less than 25kg.
- The drones will not fly above the altitude of 120m.
- The drones will not fly at night.
- The drones will not fly over assemblies of persons. 'Assemblies of people' means gatherings where persons are unable to move away due to the density of the people present (art.2 (3) Regulation (EU) 2019/947).

Additional safeguards/requirements:

- Only rational and healthy adults that will follow the informed consent procedure will participate in the pilot demonstrations.
- All project's research activities, including UAV flights, will be carried out in a controlled environment.
- The drones will be operated by experienced certified UAV pilots following all safety regulations and the instructions given in the User Manual.
- Highly qualified LEA officers from the NESTOR Consortium will be present at the pilot sites.
- The research activities that cannot be carried out remotely will involve a low number of participants (the minimum number needed for the operation of the tools and technologies and for the project's objectives to be successfully served).
- The drones will not fly in airport zone and over cultural heritage monuments.
- The drones will not carry dangerous goods that may result in high risk for third parties in case of accident. Only portable sensors will be onboard UAVs.
- The drones will not involve the transport of people.

Additional safeguards/requirements:

- Only rational and healthy adults that will follow the informed consent procedure will participate in the pilot demonstrations.
- All project's research activities, including UGV testing activities, will be carried out in a controlled environment.

- Only specialised operators from ROB and trained staff from the NESTOR Consortium will use the UGVs in accordance with the safety instructions of the User Manual.
- ROB personnel will be present ensuring that the safety instructions are followed during the operation of the UGV.
- Highly qualified LEA officers from the NESTOR Consortium will be present.
- The research activities that cannot be carried out remotely will involve a low number of participants (the minimum number needed for the operation of the tools and technologies and for the project's objectives to be successfully served).

Unmanned Underwater Vehicles (UUVs) and Unmanned Surface Vehicles (USVs)

Safety instructions for UUVs:

- In case a vehicle gets stuck under the water during operation, the following procedure is followed:
  6. Make sure the vehicle is static in its position. Diagnose the error and note down the location.
  7. Contact local authorities about this incident and request the intervention of a diving team.
  8. Communicate the coordinates of the vehicle, including its depth to the diving team.
  9. Make sure that the propeller will not be activated during the intervention.
  10. Instruct the diving team on how to handle the vehicle while under the water and how to bring the vehicle back to the surface.

- In case the operator loses contact with the UUV, the following procedure is followed:
  5. Make sure the vehicle is not on the surface (using GSM and Satellite communications)
  6. Execute the same path the vehicle should be doing with a vessel and stop every 500 meters to place hydrophone and acoustic modem in the water and try to locate the vehicle near this position.
  7. If the previous approaches fail to locate the UUV, warn the local authorities about the missing equipment. Also warn the insurance company about the incident.
  8. Keep repeating the search procedure above. Also using binoculars to search the ocean surface. The vehicle is more visible at night time (blinking led) than it is during the day. Make sure that a vessel and crew are available and are allowed to sail at night.

- In case there is a collision with surface traffic, the following procedure is followed:
  5. Make immediate contact with the vessel that collided with the UUV, as required by the insurance provider.
  6. Recover the UUV.
  7. Assess the damage on the UUV and surface vessel.
  8. Re-validate the vehicle readiness to operate before redeploying the vehicle to the water. Warn the insurance company about the incident, in case of any damage.

Additional safeguards/requirements:

- Only rational and healthy adults that will follow the informed consent procedure will participate in the pilot demonstrations.
- All project's research activities, including UUV/USV testing activities, will be carried out in a controlled environment.
- Only specialised operators from OMST and trained staff from the NESTOR Consortium will use the UUV/USV.

- OMST personnel will be present ensuring that the safety instructions and any recommendations of the local authorities are followed during the operation of the UUV/USV.
- Highly qualified LEA officers from the NESTOR Consortium will be present.
- The research activities that cannot be carried out remotely will involve a low number of participants (the minimum number needed for the operation of the tools and technologies and for the project's objectives to be successfully served).
- Authorisation will be obtained by the local maritime authorities.
- A navigational warning shall be placed by the authorities restricting the traffic in the area of operation or simply warning other traffic about the potential hazard.
- No humans will swim in the area of operation.

[redacted]

Additional safeguards/requirements:

- Only rational and healthy adults that will follow the informed consent procedure will participate in the pilot demonstrations.
- All project's research activities, including radar and RF system testing activities, will be carried out in a controlled environment.
- The devices will be operated by experienced and trained staff from HEN and NARDA and trained staff from the NESTOR Consortium following all safety regulations and the instructions given in the User Manuals.
- As underlined in Recital 11 of the Directive 2013/35/EU, the undesired effects on the human body depend on the frequency of the electromagnetic field or radiation to which it is exposed. No frequent exposure is planned during the NESTOR research activities and the required distances must be kept.
- Highly qualified LEA officers from the NESTOR Consortium will be present.
- The research activities that cannot be carried out remotely will involve a low number of participants (the minimum number needed for the operation of the tools and technologies and for the project's objectives to be successfully served).

Augmented Reality (AR) tools

[redacted]

In addition:

- The participants will be informed that they must stop using AR devices as soon as symptoms such as nausea, dizziness, sweating, and pallor appear.
- The participants will be informed that they need to take a rest for one to two hours after using AR devices.
- These technologies should be avoided by people with epilepsy, or anyone identified as vulnerable, e.g., people suffering from motion sickness or balance problems, or susceptible to migraines, etc.

Additional safeguards/requirements:

- Only rational and healthy adults that will follow the informed consent procedure will participate in the pilot demonstrations and in all research activities.
- All project's research activities, including AR testing activities, will be carried out in a controlled environment.

COVID-19

The necessary health and safety measures will be implemented during the pilots in accordance with the current national laws and guidelines in the country of the pilot.

Dual use

Dual-use items in the sense of Regulation 2021/821 means items, including software and technology, which can be used for both civil and military purposes, and includes items which can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery, including all items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices.

In two cases, authorisations are required on a constant basis:

a) for the export of dual-use items listed in Annex I and

b) for the intra-Union transfers of dual-use items listed in Annex IV.

For the other cases, authorisations are required on a case-by-case basis, if the items are or may be intended for the uses referred to in Article 4 (1) of the Regulation 2021/821.

All NESTOR partners have identified whether the NESTOR research activities involve dual-use items for which an authorisation is required.

Involvement of Non-European Countries

No import of materials to non-EU countries will take place.

Potential misuse of the research findings

A misuse mitigation strategy has been created for the NESTOR project including ex-ante and ex-post protective mechanisms.

Ex-ante mechanisms:

7. Establishing an ongoing monitor and review process is one of the most critical factors affecting the effectiveness of a risk assessment. This process will be carried out by the ethics and security experts of the project as well as by the EC for the specified management action plans to remain relevant, accurate and updated. The NESTOR project has appointed a Project Ethics Officer (PEO), an Ethics Advisory Board (EtAB), a Project Security Officer (PSO) and a Security Advisory Board (SAB) that will closely monitor the research activities from an ethical, legal and security point of view and will work together against potential misuse of the research findings.
8. As part of the deliverable review process, an Ethics Review Form must be filled out by the author of each deliverable. This brings any ethical issues to the foreground during the preparation of each deliverable, serving as a reminder to the Consortium to adhere to best practices. The responses are reviewed by the EtAB.
9. Deliverables that include highly sensitive information which could be misused have been classified as EU RESTRICTED/RESTRAINT EU.
10. Deliverables that include sensitive information which could be misused are disseminated only amongst the Consortium and the EC (CO).
11. Confidentiality undertakings have been signed by parties that are external to the Consortium (External Ethics Advisor, EAB members). Disclosure of any information shared with external parties is prohibited with only few exemptions expressly and exhaustively stipulated in the undertaking.
12. Ethics opinions/approvals have been obtained by ethics committees and, in absence of such committees, declarations of compliance have been signed by the partners prior to the start of research activities with humans. Relevant documentation is included in D8.2 H-Requirement No.2.

Ex-post mechanisms:

6. Sensitive information that includes details on the technologies, methods, materials, knowledge that could be misused will be filtered prior to publications or dissemination events and will not be made available to the public.
7. Sensitive information involved or generated during a project's task will be available solely between the involved NESTOR partners and only to authorised personnel of these partners that have a need-to-know.
8. Encryption of databases that include sensitive information will be implemented during the execution of specific tasks and complex passwords will be utilized for enhanced security as well as constant local data backup or backup in a secondary Cloud ecosystem for the prevention of data loss or data theft due to a potential cyber-attack.
9. Specific technologies will operate in a secure encrypted network channel (VPN).
10. Anonymisation and pseudonymisation of personal data will be implemented in compliance with the GDPR requirements.

Appendix G: Questionnaire on Ethics by Design for AI

QUESTIONNAIRE 'Ethics by Design for AI'

The objective of this questionnaire is to collect information from the NESTOR technical partners about the way in which AI-based tools and technologies that form the NESTOR system have been designed in order to follow an Ethics-by-Design approach. The results and relevant recommendations will be presented in D1.6 'Ethics and societal issues final report'.

Before you start answering the questions on the table below, check the definitions to understand the notion of "Artificial Intelligence" and decide whether your technology/tool is AI-based or not.

DEFINITIONS:

From the Ethics Guidelines for Trustworthy AI issued by the European Commission's High-Level Expert Group on AI (https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai):

Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimisation), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).

From the Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act), as it has been currently amended (https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf):

'artificial intelligence system' (AI system) means a system that is designed to operate with elements of autonomy and that, based on machine and/or human provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge-based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.

Name of the partner: .....

Work Package and Task: .....

Name and short description of the AI-based technology/tool, its technique and its purpose:

.....

.....

.....

1

Specification of Objectives against Ethical Requirements	YES (How?)	NO (How potential risks will be mitigated?)	Comments (If any)
Respect for Human Agency. **Human beings must be respected to make their own decisions and carry out their own actions. Respect for human agency encapsulates three more specific principles, which define fundamental human rights: autonomy, dignity and freedom**			
It can be confirmed that the AI system does not autonomously make decisions about issues that are normally decided by humans by means of free personal choices or collective deliberations or similarly significantly affects individuals.			
It can be confirmed that end-users and others affected by the AI system are not deprived of abilities to make all decisions about their own lives / take autonomous decisions about their lives.			
It can be confirmed that end-users and others affected by the AI system are not subordinated, coerced, deceived, manipulated, objectified or dehumanized, nor are attached or addicted to the system and its operations.			
Resilience and Security. **AI systems need to be safe, ensuring a fall-back plan in case something goes wrong, as well as being accurate, reliable and reproducible. That is the only way to ensure that also unintentional harm can be minimised and prevented.**			
AI system design and implementation ensure technical robustness and safety.			
AI system design and implementation ensure accuracy, reliability and reproducibility.			
Privacy & Data Governance. **People have the right to privacy and data protection, and these should be respected at all times.**			
The AI system processes data in line with the requirements for lawfulness, fairness and transparency set in the national and EU data protection legal framework and the reasonable expectations of the data subjects.			
The AI system processes personal data for a specific purpose(s) in accordance with the purpose limitation principle set in the national and EU data protection legal framework.			

2

Specification of Objectives against Ethical Requirements	YES (How?)	NO (How potential risks will be mitigated?)	Comments (If any)
The AI system processes personal data for a specific period of time that is needed to achieve the defined purpose(s) in accordance with the storage limitation principle set in the national and EU data protection legal framework.			
Technical and organisational measures are in place to safeguard the rights of data subjects (such as data minimisation, anonymisation, pseudonymisation, encryption, and aggregation).			
There are security measures in place to prevent data breaches and leakages (such as mechanisms for logging data access and data modification).			
Fairness. Non-discrimination. **People should be given equal rights and opportunities and should not be advantaged or disadvantaged undeservedly.**			
The AI system is designed to avoid algorithmic bias, in input data, modelling and algorithm design.			
The AI system is designed to avoid potential negative discrimination against people on the basis of any of the following grounds (non-exhaustively): sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.			
The AI system has put in place processes to address and rectify for potential discrimination (bias).			
The AI system is designed to avoid historical and selection bias in data collection, representation and measurement bias in algorithmic training, aggregation and evaluation bias in modelling and automation bias in deployment.			
The AI system is designed so that it can be used different types of end-users with different abilities.			
The AI system does not have negative social impacts on the affected groups of individuals, including impacts other than those resulting from algorithmic bias or lack of universal accessibility.			

3

Specification of Objectives against Ethical Requirements	YES (How?)	NO (How potential risks will be mitigated?)	Comments (If any)
Individual, and Social and Environmental Well-being. **AI systems should contribute to, and not harm, individual, social and environmental wellbeing**			
The AI system takes the welfare of all stakeholders into account and do not unduly or unfairly reduce/undermine their well-being.			
The AI system is mindful of principles of environmental sustainability, both regarding the system itself and the supply chain to which it connects (when relevant).			
It can be confirmed that the AI system does not have the potential to negatively impact the quality of communication, social interaction, information, democratic processes, and social relations.			
It can be confirmed that the system does not reduce safety and integrity in the workplace and complies with the relevant health and safety and employment regulations.			
Transparency. **The purpose, inputs and operations of AI programs should be knowable and understandable to its stakeholders.**			
The end-users are aware that they are interacting with an AI system.			
The purpose, capabilities, limitations, benefits and risks of the AI system and of the decisions conveyed are openly communicated to and understood by end-users and other stakeholders along with its possible consequences.			
People can audit, query, dispute, seek to change or object to AI or robotics activities (human intervention).			
The AI system enables traceability during its entire lifecycle, from initial design to post-deployment evaluation and audit.			
The system offers details about how decisions are taken and on which reasons these were based (when relevant and possible).			
The system keeps records of the decisions made.			

4

Specification of Objectives against Ethical Requirements	YES (How?)	NO (How potential risks will be mitigated?)	Comments (If any)
Accountability & Oversight **Humans should be able to understand, supervise and control the design and operation of AI-based systems, and the actors involved in their development or operation should take responsibility for the way that these applications function and for the resulting consequences.**			
The system provides details of how potential ethically and socially undesirable effects will be detected, stopped, and prevented from reoccurring.			
The AI system allows for human oversight during its decision cycles and operation.			

5

Appendix H: 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.

1.1 Reviewers

Project Coordinator	HP-
Management Team Member	KEMEA-
Internal Peer Reviewers	CENTRIC- CERTH- , External Ethics Advisor-

1.2 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

1.3 Consolidated Comments of Quality Reviewers

General Comments	
Deliverable contents thoroughness	Reviewers' comments: Yes Author's reply:
Innovation level	Reviewers' comment: N/A Author's reply:
Correspondence to project and programme objectives	Reviewers' comment: 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 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: Author's reply:
Structure of the deliverable with clear objectives, methodology, implementation, results and conclusions	☒ Yes ☐ No ☐ Partially ☐ Not applicable Reviewers' comment: Author's reply:
Clarity and quality of presentation, language and format	☒Yes ☐ No ☐ Partially ☐ Not applicable Reviewers' comment: Author's reply:

Detailed Comments (please add rows if needed)		
No.	**Reference**	**Remark(s)**
1		
2		
3		

Appendix I: 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 the deliverable is drafted by the PEO as well as it is reviewed and finalised by the other EtAB members.
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.	**Yes** **EtAB comments:** Questionnaire on Ethics by Design for Artificial Intelligence that aimed at helping the technical partners contribute to this deliverable.
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 partner sor 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 unauthorised access to, unauthorised 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 toanalyse 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 authorisation 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 stigmatisation of humans.	**No** **EtAB comments:**
This deliverable integrates the mitigation actions presented in D8.7 M-Requirement No.7.	**No** **EtAB comments:**