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

D8.7
M-Requirement No.7

Editor(s)	
Lead Beneficiary	KEMEA
Status	☒Draft ☒Peer reviewed ☒Management Support Team reviewed ☒Project Coordinator accepted
Version	1.0
Due Date	31/07/2022
Delivery Date	10/08/2022
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

Project	NESTOR – 101021851
Work Package	WP8 – Ethics Requirements
Deliverable	D8.7 M-Requirement No.7
Editor(s)	KEMEA –
Contributor(s)	All partners
Reviewer(s)	CENTRIC –
	External Ethics Expert – (VUB)
Ethics Assessment	☒Passed ☐ Rejected Comments (if any):
Security Assessment	☒Passed ☐Rejected Comments (if any):

Abstract	D8.7 M-Requirement No.7 is the seventh deliverable of WP8-Ethics Requirements that has been set out by the European Commission. This deliverable includes: Risk assessment and details on measures to prevent misuse of research findings.
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	20/05/2022	KEMEA	Skeleton
0.2	14/06/2021	KEMEA	First draft
0.3	20/06/2022	KEMEA	Incorporation of input by partners
0.4	29/06/2022	KEMEA	Incorporation of input by partners
0.5	11/07/2022	KEMEA	Incorporation of input by partners
0.6	21/07/2022	KEMEA	Incorporation of input by partners
0.7	25/07/2022	KEMEA	Incorporation of input by partners
0.8	26/07/2022	KEMEA	Ready for review
0.8.1	28/07/2022	EtAB	Review and suggestions
0.8.2	28/07/2022	EtAB	Review and suggestions
0.8.3	02/08/2022	KEMEA	Incorporation of EtAB's comments
0.9	02/08/2022	KEMEA	Sent for security review and approval by the Project Manager and the Project Coordinator
1.0	10/08/2022	KEMEA	Final version – Ready to submit

The NESTOR Consortium

No	Name	Short Name	Country
1	HELLENIC POLICE	HP	Greece
2	GLAVNA DIREKTSIA GRANICHNA POLITSIA	CDBP-MoI	Bulgaria
3	MINISTRY OF INTERIOR	DBAM	Republic of North Macedonia
4	MINISTRY OF TRANSPORT, COMMUNICATIONS AND WORK	JRCC	Cyprus
5	VALSTYBES SIENOS APSAUGOS TARNYBA PRIE VIDAUS REIKALU MINISTERIJOS	SBGSLT	Lithuania
6	MINISTERIO DEL INTERIOR	GUCI	Spain
7	WOITSCH CONSULTING OY	WCO	Finland
8	KENTRO MELETON ASFALEIAS	KEMEA	Greece
9	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	Greece
10	SATWAYS – PROIONTA KAI YPIRESIES TILEMATIKIS DIKTYAKON KAI TILEPIKINONIAKON EFARMOGON ETAIRIA PERIORISMENIS EFTHINIS EPE	STWS	Greece
11	DECODIO AG	DCD	Switzerland
12	NARDA SAFETY TEST SOLUTIONS GMBH	NARDA	Germany
13	MILTECH HELLAS BIOMICHANIA EMPORIO ANTIPROSOPEIES ILEKTRONIKON OPTIKON KAI MICHANOLOGIKON EIDON AE	MILTECH	Greece
14	MAGGIOLI SPA	MAG	Italy
15	ELISTAIR	ELI	France
16	OCEANSCAN – MARINE SYSTEMS & TECHNOLOGY LDA	OMST	Portugal
17	ROBOTNIK AUTOMATION SLL	ROB	Spain
18	OULUN YLIOPISTO	UOULU	Finland
19	SHEFFIELD HALLAM UNIVERSITY	CENTRIC	United Kingdom
20	HENSOLDT SENSORS GMBH	HEN	Germany
21	INGENIERIA DE SISTEMAS PARA LA DEFENSA DE ESPANA SA-SME MP	ISDEFE	Spain

Executive Summary

D8.7 M-Requirement No.7 is the seventh deliverable of WP8 'Ethics Requirements' and the seventh ethics requirement that must be fulfilled to identify technologies, materials, methods or knowledge either developed or used during the lifetime of the NESTOR project that could be misused and to ensure that the relevant risks will be mitigated with the implementation of appropriate measures.

In particular, D8.7 should include a risk assessment and details on measures to prevent misuse of research findings.

Table of Contents

List of Tables

Terms and Abbreviations

AR	Augmented Reality
ASV	Autonomous Surface Vehicle
AUV	Autonomous Underwater Vehicle
BC3i	Broad Control Category Cost Indicators
CISE	Common Information Sharing Environment
CO	Consortium Only
D	Deliverable
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
EPQ-Requirement	Extended Project Qualification - Requirement
EtAB	Ethics Advisory Board
EU	European Union
EUROSUR	European Border Surveillance System
H-Requirement	Humans - Requirement
KPIs	Key Performance Indicators
LEAs	Law Enforcement Agencies
M	Month
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
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
VPN	Virtual Private Network
WP	Work Package

1 INTRODUCTION

Although research activities are usually carried out with benign intentions, they have the potential to harm humans, animals or the environment. Given the severe consequences the potential misuse of research could have on the general public, the need to monitor research activities and to protect research findings must be taken into serious consideration by anyone engaged in the research field. The risk of misuse cannot be eliminated, but it can be minimized by recognizing risks in good time and taking the right precautions.

The European Commission through its Research Executive Agency plays a central role in safeguarding EU funded research against potential misuse by defining the framework and organising Ethics Screening, Review and Audit.

The NESTOR project has appointed an Ethics Advisory Board (EtAB) chaired by the Project Ethics Officer (PEO) and a Security Advisory Board (SAB) chaired by the Project Security Officer (PSO) that closely monitor the research activities from an ethical, privacy and security point of view and work together against potential misuse of the research findings.

The aim of this deliverable is to describe and clarify to the partners the notion of 'misuse', to identify those technologies, materials, methods and knowledge, either generated or used during the NESTOR research, that could be used for unintended malicious and unethical purposes despite the researchers' benign intentions, to describe, analyse and evaluate the relevant risks through a risk assessment and to suggest proportionate measures to prevent potential misuse of the research findings.

Therefore, specific risks will be identified per category and analysed by the responsible partners (risk holders). Appropriate procedures have been established and will be followed by the NESTOR Consortium to early detect any risks of misuse and prevent their occurrence (*ex-ante* mechanisms) and additional measures will be implemented by the NESTOR Consortium as a whole and the risk holders individually to avoid their occurrence or to minimise their severity and impact upon potential materialisation (*ex-post* mechanisms). These mechanisms constitute the project's mitigation strategy.

Finally, the concluding remarks are presented.

All the information included in the present deliverable will be communicated to the NESTOR Consortium through a dedicated session during the 3rd Project Meeting in October 2022.

Any updates will be incorporated in the deliverables of T1.5 'Ethics and Societal Issues Management' (D1.5 and D1.6, due in M12 and M18 respectively).

2 POTENTIAL MISUSE OF THE NESTOR RESEARCH

2.1 DEFINITION OF "MISUSE"

The European Commission through its 'Guidance How to complete your ethics self-assessment' has issued guidelines in order to help all parties involved in H2020-funded projects take the necessary measures to avoid potential misuse of research findings. The main questions for understanding the notion of misuse are the following:

- If materials/methods/technologies and knowledge involved or generated were modified or enhanced, could they harm humans, animals or the environment?
- What would happen if the materials/methods/technologies and knowledge involved or generated ended up in the wrong hands?
- Could the materials/methods/technologies and knowledge involved or generated serve purposes other than those intended? If so, would such use be unethical?

To identify any possible misuse, it is important to start by considering the risks associated with the research planned and any unethical ways in which the materials, methods, technologies and knowledge involved or generated could be used. The **research most vulnerable to misuse** is research that:

- provides knowledge, materials and technologies that could be channeled into crime or terrorism;
- could result in chemical, biological, radiological or nuclear weapons and the means for their delivery;
- involves developing surveillance technologies that could curtail human rights and civil liberties;
- involves minority or vulnerable groups or develops social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.

2.2 RISK ASSESSMENT

2.2.1 Methodology

For the risk assessment to be conducted, a questionnaire has been circulated to the NESTOR Consortium partners aiming at collecting information on the technologies, materials, methods and knowledge that are used or generated during the project's research activities and that could be misused by third parties to serve malicious or unethical purposes. The questionnaire is presented below:

D8.7 QUESTIONNAIRE

Before starting filling in the questionnaire, please read the text below:

The European Commission through its 'Guidance How to complete your ethics self-assessment' has issued guidelines in order to help all parties involved in H2020-funded projects take the necessary measures to avoid potential misuse of research findings. The main questions for understanding the notion of misuse are the following:

- **If materials/methods/technologies and knowledge involved or generated were modified or enhanced, could they harm humans, animals or the environment?**
- **What would happen if the materials/methods/technologies and knowledge involved or generated ended up in the wrong hands?**
- **Could the materials/methods/technologies and knowledge involved or generated serve purposes other than those intended? If so, would such use be unethical?**

To identify any possible misuse, it is important to start by considering the risks associated with the research planned and any unethical ways in which the materials, methods, technologies and knowledge involved or generated could be used. The **research most vulnerable to misuse** is research that:

- provides knowledge, materials and technologies that could be channeled into crime or terrorism;
- could result in chemical, biological, radiological or nuclear weapons and the means for their delivery;
- involves developing surveillance technologies that could curtail human rights and civil liberties;
- involves minority or vulnerable groups or develops social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.

MITIGATING MEASURES:

- ✓ Establishment of a **project's Ethics Advisory Board** for constant ethical monitoring
- ✓ **Approval/Opinion by an internal Ethics Committee** (where applicable)
- ✓ Establishment of a project's **Security Advisory Board** led by the project's Project Security Officer for ensuring security-related monitoring
- ✓ **Authorised access to the sensitive material only by the WP/Task Leaders** and only by the personnel of the partners that have a **need-to-know**
- ✓ **Limited dissemination of deliverables** that include sensitive material **only amongst the Consortium and the European Commission (CO)** or **EU-Restricted Deliverables**
- ✓ Information that includes details on the technologies, methods, materials, knowledge that could be misused **to be filtered prior to publications or dissemination events and not be communicated to the public**.
- ✓ Use of **dummy data**
- ✓ **Encryption** of databases that include sensitive material that could be misused
- ✓ Other technical, organisational and security **measures** such as anonymisation of personal data, DPIA etc.
- ✓ **Training of the staff** involved in the task's research activities

Partner: <NAME OF THE NESTOR PARTNER>

1. What could be potentially misused from the research?

Name the technologies, methods or knowledge (and the respective WPs and tasks during which they are involved or generated) that may pose one or more of the risks mentioned in the table below.

Risk	WP	Task	Technology/Method/Knowledge
Research provides knowledge, materials and technologies that could be channeled into crime or terrorism	WPx	TX.x	
Research could result in chemical, biological, radiological or nuclear weapons and the means for their delivery			
Research involves developing surveillance technologies that could curtail human rights and civil liberties			
Research involves minority or vulnerable groups or develops social or behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people			

2. What could happen if this technology or knowledge ended up in the wrong hands and was used for malicious purposes?

a) Name the possible event(s): .....

b) How likely is that this event actually occurs? Choose the level from 1 to 4.

In case of more events, answer this question for each event separately.

Level	Description of the Event Occurrence Level
1	The event is extremely unlikely to occur.
2	The event is unlikely to occur.
3	The event might occur.
4	The event is likely to occur.

3. How severe would the impact be?

Choose the level from 0 to 5.

In case of more events, answer this question for each event separately.

Level	Description of the Event Severity Level
0	The event will have no impact
1	The event will have isolated impact not above task-level / very low impact beyond the project
2	The event will have impact on a work-package-level / low impact beyond the project
3	The event will have impact on more work packages / medium impact beyond the project
4	The event will have impact on the overall project, but limited to single deliverable(s) or parts of the project / high impact beyond the project
5	The event will have serious impact on the results promised in the Description of Action /severe impact beyond the project

4. How can the risks be prevented or mitigated?

a) Name the proposed mitigation measures **(check the mitigating measures on the first page and include the ones relevant in your case – add more if any).**

.....

b) How effective can those measures be?

Choose the level of effectiveness from 1 to 5.

Level	Effectiveness of Mitigation Action
1	Full availability of necessary resources; Very low cost/time/resource consumption; High chance of success; 0 - ≤10% probability of undesirable impact
2	Moderate availability of necessary resources; Medium cost/time/resource consumption; Moderate chance of success; >10% - ≤40% probability of undesirable impact
3	Low availability of necessary resources; High cost/time/resource consumption; Low chance of success; >40% - ≤60% probability of undesirable impact
4	Remote availability of necessary resources; Near unacceptable cost/time/resource consumption; Remote chance of success; >60% - ≤80% probability of undesirable impact
5	Safety problem and/or non-compliance to regulations; Unavailable necessary resources; Unacceptable cost/time/resource consumption; Zero chance of success; >80% - ≤100% probability of undesirable impact

2.2.2 Risk-assessment results

NESTOR is a research project that aims at demonstrating 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. NESTOR long-range and wide area surveillance capabilities for detection, recognition classification and tracking of moving targets (e.g., persons, vessels, vehicles, drones etc.) is based on optical, thermal imaging and Radio Frequency (RF) spectrum analysis technologies fed by an interoperable sensors network including stationary installations and mobile manned or unmanned vehicles (aerial, ground, water, underwater) capable of functioning both as standalone, tethered and in swarms. 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 centers in AR environment being interoperable with CISE and EUROSUR.

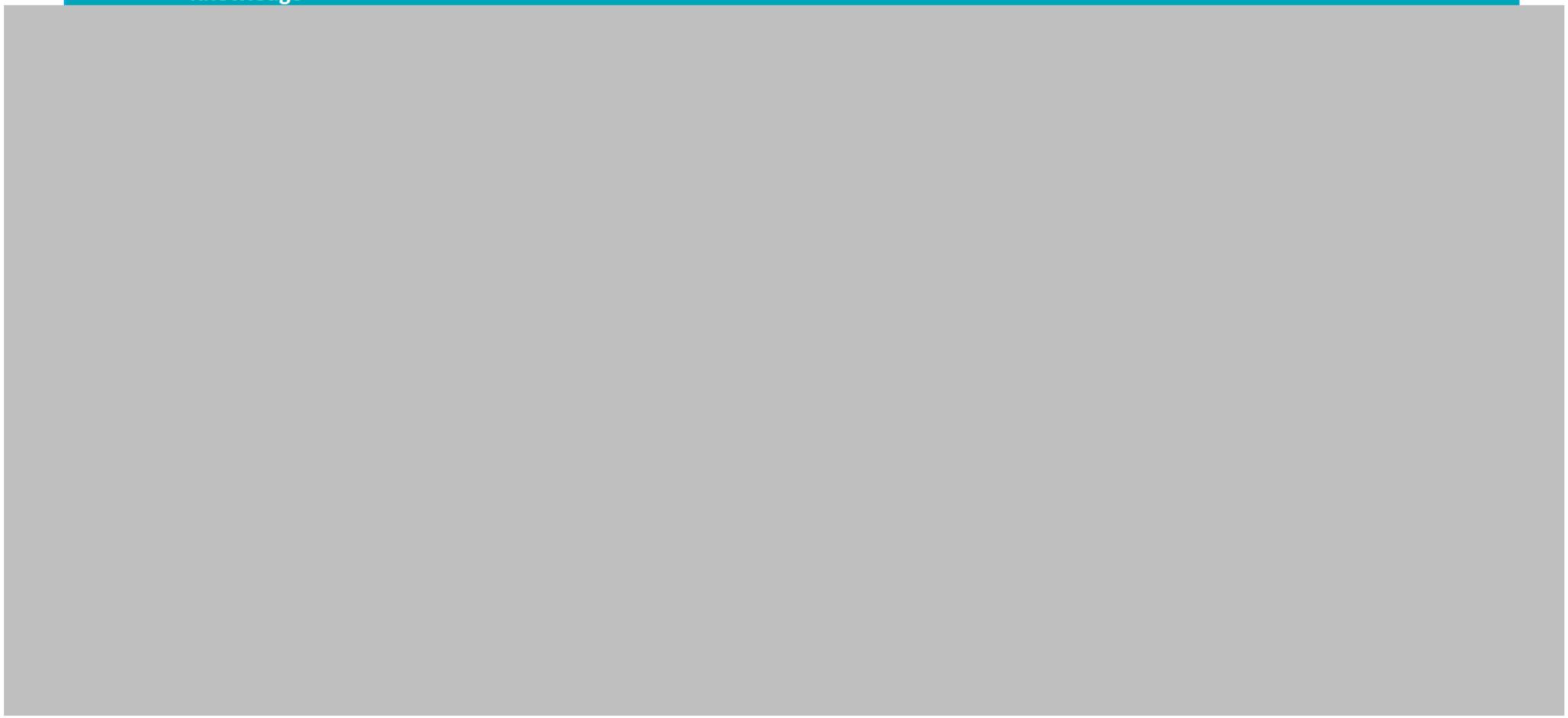
Simultaneously, the project's aim is to strike a balance between the improvement of situational awareness on the European borders and the protection of human rights and freedoms.

For the NESTOR objectives to be met, knowledge will be created, and different technologies will be used and developed in order to be tested during dedicated project's tasks and during the three pilot demonstrations of WP6. Some of this knowledge and technologies might entail risks for misuse.

At this stage, the following risks have been identified and described by the Consortium partners and presented per category. Their level of occurrence has been assessed by the responsible Consortium partners (risk holders) after considering the nature of the risks and the establishment of appropriate preventive procedures in the NESTOR project (*ex-ante* mechanisms). In addition, their level of severity has been assessed by the risk holders after considering the nature of the risks and their potential impact in case they would be materialized. Proportionate measures that consist of both *ex-ante* and *ex-post* mechanisms have been specified by the risk holders and the final assessment on the effectiveness of these measures is presented in the tables below:

Risk category: Research provides knowledge, materials and technologies that could be channeled into crime or terrorism

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Severity Level	Mitigating actions	Effectiveness Level



WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Severity Level	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Severity Level	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Severity Level	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Severity Level	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Severity Level	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Severity Level	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Severity Level	Mitigating actions	Effectiveness Level

Risk category: Research involves developing surveillance technologies that could curtail human rights and civil liberties

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Level	Severity	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Level	Severity	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Level	Severity	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Level	Severity	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Level	Severity	Mitigating actions	Effectiveness Level

Risk category: Research develops social or behavioral profiling technologies that could be misused to stigmatize, discriminate against, harass or intimidate people

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Severity Level	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Severity Level	Mitigating actions	Effectiveness Level

WP/Task	Technologies, Materials, Methods, Knowledge	Event/ Risk	Event Occurrence Level	Event Severity Level	Mitigating actions	Effectiveness Level

2.3 THE NESTOR MITIGATION STRATEGY

The NESTOR Consortium, being aware of the identified risks as they have been addressed and analyzed above in chapter 2.2 by the risk holders, will follow a strategy and will implement the following mechanisms in order to early detect and prevent or mitigate the risks related to potential misuse of the research findings:

***Ex-ante* mechanisms:**

These procedures have been already established and will be collectively followed in the project for the prevention of all types of potential risks of misuse.

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.

    a. The **EtAB** consists of the PEO (KEMEA) who chairs the Board and two more members: a member from the Consortium (CENTRIC) and an External Advisor (VUB) that are qualified in ethical and legal matters. The EtAB reviews each and every deliverable that may raise ethical or legal concerns including those related to the potential misuse of research findings. The comments and recommendations of the EtAB are included in the respective table that accompanies all project's deliverables (Ethics Review Form in the Appendix). Additionally, they participate in the project's meetings, pilot demonstrations and other events in order to be aware of the project's research activities and to early address potential risks and propose mitigating measures. Moreover, the PEO prepares the ethics deliverables of WP8 which are reviewed by the other EtAB members prior to submission. Due to the severity of the ethics issues, two specific reports will be drafted by the EtAB (D8.8, D8.9).
    b. The **SAB** consists of the PSO (KEMEA) who chairs the Board and two more members from the Consortium (CERTH and CDBP). The SAB deals with any security concerns and monitors the research activities from this viewpoint. The responsibilities of PSO are to advise and review all security and sensitive material and matters of the project and to supervise and check compliance during the project lifespan. It is the main role of the SAB to assess the sensitivity of input and deliverables prior to publication and to assess the sensitivity of the information handled by the Consortium during the lifecycle of the project.
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 as explained above.

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.
7. The project's research activities that involve technologies with a potential of misuse will be carried out **in a controlled environment** with the participation of **volunteers** that will follow the informed consent procedure, **qualified LEAs staff** and **well-trained staff**.

***Ex-post* mechanisms:**

These measures will be implemented by the NESTOR Consortium collectively or the risk holders individually to avoid the materialisation of potential risks of misuse or to minimise their severity upon occurrence.

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. The NESTOR Consortium will be **trained prior to the use of tools and technologies** based on the training material created as part of T6.2. The training material will also include **ethics guidelines related inter alia to the prevention of misuse**.
4. **Encryption** of databases that include sensitive information will be implemented during the execution of specific tasks and **complex passwords** will be utilised 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.
5. Specific technologies will operate in a **secure encrypted network channel (VPN)**;
6. **Anonymisation** and **pseudonymisation** of personal data processed as part of T3.1 and T3.4 will be implemented in compliance with the GDPR requirements. Extended reference to the data protection procedures to be followed, security measures and anonymisation/pseudonymisation techniques is made in D8.3 POPD-Requirement No.3 and D8.1 H-Requirement No.1.
7. A **Data Protection Impact Assessment** will be conducted by the controller CENTRIC (procedure in progress) prior to the start of the T3.4 data processing operation. Another DPIA has been conducted by the controller CERTH as regards the T3.1 and T3.4 data processing operations. The DPIAs will be updated during the lifetime of the project.

8. A **privacy notice of article 14(5)(b) GDPR** will be made publicly available to facilitate the data subjects of T3.1 and T3.4 to exercise their rights and prevent or minimise the risks related to the curtailment of the rights to privacy and personal data protection.

Lastly, an **Incidental Findings Policy** has been drafted for the NESTOR project and is part of D8.1 H-Requirement No.1. The policy will be updated depending on the project's progress and additional needs that may occur during its lifetime. In case any of the aforementioned identified risks is materialised, the Incidental Findings Policy will be followed.

Any misuse of technologies that could lead to health and safety risks for the research staff and the participants is out of the scope of the present deliverable. The relevant risks will be mitigated based on the procedures described in D8.5 EPQ-Requirement No.5.

3 CONCLUSION

The present deliverable explains the notion of 'misuse' to the NESTOR partners (Section 2.1), includes a risk assessment as regards the technologies and knowledge generated or used during the research that could be misused, i.e., could be used for unintended malicious and unethical purposes (Section 2.2) and presents a mitigation strategy (Section 2.3).

The potential undesirable events have been identified and described by the Consortium, their occurrence level has been assessed by the risk holders after taking into consideration the nature of the risks and the effectiveness of the preventive procedures already established in the NESTOR project (*ex-ante* mechanisms), the severity level has been assessed after considering the nature of the risks and their impact upon potential materialisation, the implemented measures were described and, finally, their level of effectiveness was presented.

The identified risks belong to the following three categories:

- Research provides knowledge and technologies that could be channeled into crime or terrorism;
- Research involves developing surveillance technologies that could curtail human rights and civil liberties;
- Research develops social or behavioural profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.

The risk related to research resulting in chemical, biological, radiological or nuclear weapons and the means for their delivery is not applicable in the NESTOR research.

No vulnerable individuals or groups are involved in the project's research activities as further described in D10.1 H-Requirement No.1, hence, relevant risks have not been identified.

No automated decision making is involved, and human intervention and oversight are ensured. NESTOR takes an intelligence-led approach to focus on detecting events that are highly correlated with known illicit activity on the borders and there is always human-in-the-loop decision making, hence, relevant risks have not been identified.

The Consortium will take all necessary safeguards to prevent or mitigate the potential misuse of technologies and knowledge generated or used during the project's activities. The mitigation strategy includes a variety of *ex-ante* and *ex-post* protective measures that are

considered effective and can ensure a high level of security of any sensitive information used or produced within the project. The *ex-ante* mechanisms are procedures that have been already established and will be collectively followed in the project for the prevention of all types of potential risks of misuse, while the *ex-post* mechanisms are additional measures that will be implemented by the NESTOR Consortium collectively or the risk holders individually to avoid potential materialisation of risks or to minimise their severity upon occurrence.

The information included in the present deliverable will be made available to the NESTOR Consortium through a dedicated session during the 3rd Project Meeting in October 2022.

Updated information, if any, will be included in the deliverables of T1.5 'Ethics and Societal Issues Management' (D1.5 and D1.6, due in M12 and M18 respectively).

4 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
- European Commission, (7 January 2020), Guidance note – Potential misuse of research, version 1.1, https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-misuse_en.pdf
- Grant Agreement No 101021851 – Annex A Description of the action
- Grant Agreement Amendment AMD-101021851-3

Appendix A: 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 Support Team Member	KEMEA-
Internal Peer Reviewer(s)	CENTRIC – (EtAB member), External ethics expert– (EtAB Member)

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: Good Author's reply:
Innovation level	Reviewers' comment: Good Author's reply:
Correspondence to project and programme objectives	Reviewers' comment: Good 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 B: 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 and reviewed by the 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.	**No** **EtAB comments:**
This deliverable is based on research activities (either during pilots or during the execution of other tasks) that may involve children or adults unable to give informed consent or vulnerable individuals/groups.	**No** **EtAB comments:**
Informed Consent Forms for the participation of humans in research have been/will be signed.	**No** **EtAB comments:**
Measures for the protection of vulnerable individuals/groups have been/will be implemented.	**No** **EtAB comments:**
Incidental findings, i.e., findings that are outside the research's scope, may be detected as part of the research activities described in this deliverable (criminal activity or personal data of non-volunteers during trials).	**No** **EtAB comments:**
Data Protection	
This deliverable is based on research activities that involve processing of personal data.	**No** **EtAB comments:**
This deliverable is based on research activities that involve processing of special categories of personal data according to Article 9 GDPR. Special categories of personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the	**No** **EtAB comments:**

purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation).	
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:**