Ref. Ares(2020)2273585 - 28/04/2020

HORIZON 2020

ETHICAL CODE AND UPDATES ON DATA PROTECTION

ROBORDER
740593

Deliverable Information
Work Package: WP8
Deliverable Number: D8.6
Date of Issue: 09/04/2020
Document Reference: 740593-ROBORDER-D8.6_EthicalCode_and_Updates_on_DataProtection
Version Number: 1.8
Nature of Deliverable: Report
Dissemination Level of Deliverable: Confidential
Author(s): CERTH
Keywords: Ethics Report, Ethics Approvals, Informed Consent, Information Sheet, Research with Humans, Data Protection Rules, Ethical Code, External Ethics Advisor, Ethics Advisory Board

Abstract:
Following the Ethics Review Assessment all Work Package (WP) 9 deliverables underwent and the recommendations reported by the Ethics Committee with a Ref. Ares (2019) 4518279 – 12/07/2019, this document reports on how these recommendations were addressed in order for the ROBORDER Consortium to deal with the ethics issues that had arisen during the project's lifetime.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740593

Document History

Date	Version	Remarks
15/01/2020	1.0	1st draft of the document
25/01/2020	1.1	Modifications and adjustments
25/02/2020	1.2	Copy of DPO's ethics approval incorporated in Annex & modifications
05/03/2020	1.3	Sent for internal review - CERTH
09/03/2020	1.4	Minor modifications and comments addressed
09/03/2020	1.5	Document sent to EAB and EEA for review and ethics approval
24/03/2020	1.6	Adjustments and modifications based on EEA feedback
31/03/2020	1.7	Adjustments and modifications based on EAB feedback
09/04/2020	1.8	Final document

Document Authors

Entity	Contributors
CERTH	[redacted]
CERTH	[redacted]
CERTH	[redacted]
CERTH	[redacted]
ORFK	[redacted]
EEA	[redacted]

Disclosure Statement: The information contained in this document is the property of ROBORDER and it shall not be reproduced, disclosed, modified or communicated to any third parties without the prior written consent of the abovementioned entities.

Executive Summary

Following the Ethics Review Assessment all Work Package (WP) 9 deliverables underwent and the recommendations reported by the Ethics Committee with a Ref. Ares (2019) 4518279 – 12/07/2019, this document reports on how these recommendations were addressed in order for the ROBORDER Consortium to deal with the ethics issues that had arisen during the project's lifetime.

The process of working with humans is elaborated by providing details of all the demonstrations/operational tests that will take place and the procedures followed by the Consortium in order to be compliant with EU regulations and Horizon 2020 guidelines.

More details on the recruitment process and the updated information sheet/informed consent form are provided to the reader in order to get a better grasp of the procedures the Consortium followed to recruit participants. In addition, certain data protection rules are set out and more information on the appointed Data Protection Officers (DPO) of the responsible partners are given.

The aspect of surveillance is further discussed by focusing on the legal framework followed and the ethical and societal impact this project could have. A specific Ethics Code is formed and explained.

Finally, the ethics reports from the External Ethics Advisor (EEA) and the internal Ethics Advisory Board (EAB) are laid out alongside their requested ethics approvals.

Table of Contents

Document History 2
Document Authors 3
Executive Summary 4
1 Introduction 8
1.1 ROBORDER in a nutshell 8
1.2 Purpose of this document 8
2 Research with Humans 10
2.1 Full details of demos/operational tests 10
2.2 Recruitment process 17
2.3 Updated information sheet 18
2.4 Updated consent form 19
2.5 Copies of ethics approvals 19
3 Personal data protection 20
3.1 Data Protection Officer 21
3.2 Process of personal data within the project 23
3.2.1 Previously collected data 23
3.2.2 Publicly available data 24
3.3 Data Protection Rules 24
4 Surveillance 27
4.1 Legal framework 27
4.2 Evaluation of ethical/societal impact 28
4.2.1 Misuse and protection measures 29
4.2.2 Dual use and protection measures 29
4.3 UxVs operations 30
4.4 Informing data subjects and non-involved people 30
4.5 Ethical Code 31
5 Ethics reports 33
5.1 External Ethics Advisor's report and comments 33
5.1.1 Report from
5.2 Internal Ethics Advisory Board's report 36
5.2.1 Report from
6 References 40
7 Annex I – Details on PUCs 41
8 Annex II – Updated information sheet/informed consent 45
9 Annex III – EEA Ethics Report 49
11 Annex IV – Initial Ethics Check Report 72
12 Annex V – CERTH's DPIA 80

List of Tables

Table 1. List of acronyms. 7
Table 2. Ethics Self-Assessment Questions (about Humans) 18
Table 3. Ethics Self-assessment Questions (Personal Data) 21
Table 4. DPOs contact details 22
Table 5. ROBORDER's contribution to EC's core ambitions for 2019-2024 29

List of Figures

Figure 1. Visualization of legal grounds and data subjects 39

List of Acronyms

Acronym	Meaning
AAN	National Aeronautical Authority (Autoridade Aeronautica Nacional)
AdSP-MTS	Autorità di Sistema Portuale del Mar Tirreno Settentrionale
AIS	Automatic Identification System
ANAC	Portuguese Civil Aviation Authority (Autoridade Nacional da Aviacao Civil)
BDI	Bulgarian Defence Institute
C2	Command and Control
CERTH	Center for Research and Technology Hellas
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSS	Decision Support System
EAB	Ethics Advisory Board
EASS	Estonian Academy of Security Sciences
EC	European Commission
EEA	External Ethics Advisor
EU	European Union
EUROSUR	European Border Surveillance System
GDPR	General Data Protection Regulation
GNR	National Republican Guard
GPS	Global Position System
HMOD	Hellenic Ministry of Defence
ICT	Information and Communication Technology
ISM	Industrial, Scientific, and Medical (frequency)
MoniCA	Monitoring and Control Application
ORFK	Rendőrség (Hungarian Police)
PR	Passive Radar
PRN	Photonic-based Radar Network
PSNI	Police Service of Northern Ireland
REA	Research Executive Agency
RF	Radio Frequency
RGB	Red Green Blue (camera)
RIB	Rigid Inflatable Boat
SPs	Sensor Peripherals
UAV	Unmanned Aerial Vehicle
UGV	Unmanned round Vehicle
USV	Unmanned Surface Vehicle
UxV	Unmanned Vehicle (of any kind)
VPN	Virtual Private Network
WP	Work Package

Table 1. List of acronyms.

1 Introduction

1.1 ROBORDER in a nutshell

ROBORDER is a platform that aims at developing a border surveillance system which will involve various unmanned mobile robots including aerial, water surface, underwater and ground vehicles, while incorporating multimodal sensors as part of an interoperable network: enhanced static network sensors such as border surveillance radars and customised mobile sensors installed on unmanned vehicles. Hence, ROBORDER will be able to operate in a wide range of operational and environmental settings and provide its operator with a complete and detailed situational awareness picture.

The main sensing technologies that are exploited within the scope of the project are: **(i)** passive radars that can extend the capabilities of the existing border surveillance radars, **(ii)** passive Radio Frequency-signal sensing devices to intercept emission sources that are present in area, enrich the overall situational awareness picture with this information, allowing for further characterizing the nature and behaviour of entities in the picture, and detecting unauthorized signal sources and **(iii)** other mobile sensors like thermal cameras (infra-red) and optical cameras.

The information collected from the aforementioned sensing technologies will be forwarded to ROBORDER's command and control (C2) unit, after the integration of various software services either for detection or for optimal situation awareness that will lead to the provision of an effective overview of the under surveillance area. This overview will be visible to the system's operators and will act as a Decision Support System (DSS). Translation of the intention of the operators into remote actions, automatic selection of the most appropriate composition of hardware (robots and available sensors), easy deployment and operation of the robotic swarm are some of the additional C2 functionalities of ROBORDER's platform.

1.2 Purpose of this document

In order to test and evaluate the platform's capabilities and the interoperability across all the involved services, a number of operational tests and demonstrations are performed throughout the project's lifetime. Following the development cycles and the foreseen evaluation approaches, the tests will include real operation scenarios both as demonstrations and as operational tests:

Prior and during these demos/tests, humans are going to be involved either as interviewees or as participants. In both cases, two types of data are going to be collected: personal data and evaluation data. Personal data are going to be collected prior to and after the demo/test

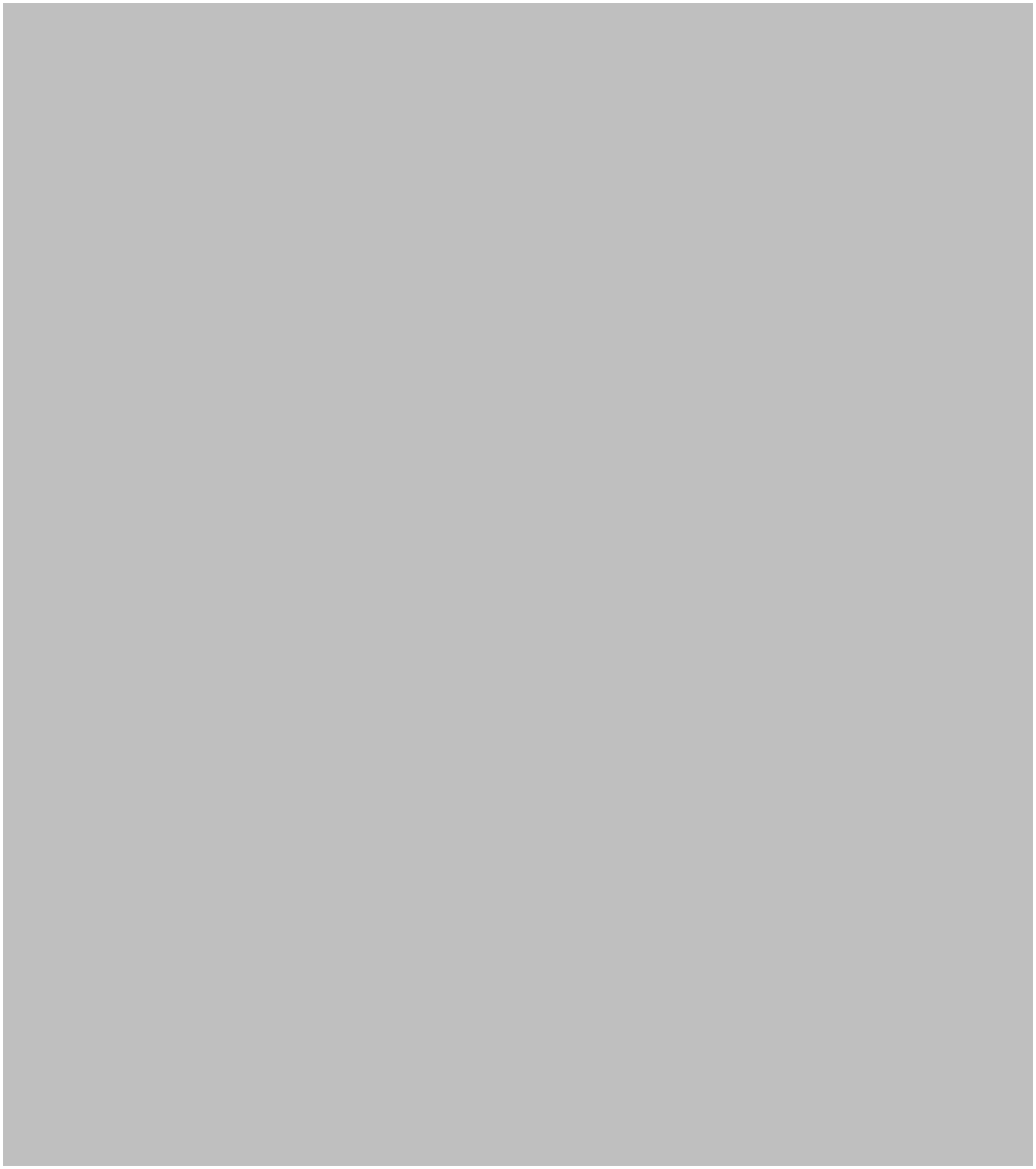
and will be used for the personalisation of the guidelines, ROBORDER's Decision Support System (DSS) as well as the logistics aspect of the demo/test's organisation. Evaluation data will be collected during the demo/test and will be used for assuring the platform's functionality and interoperability.

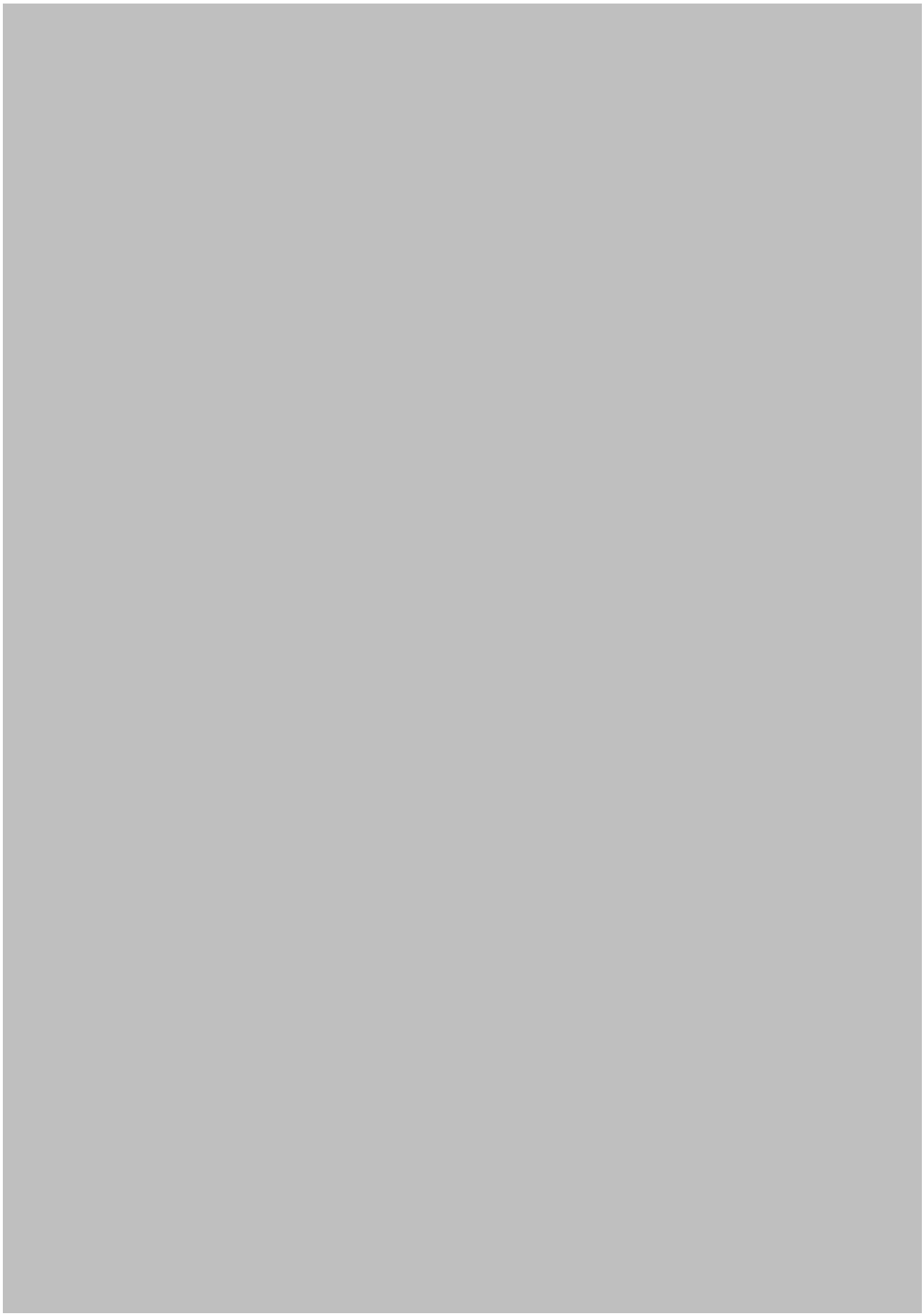
According to Horizon 2020 – Ethics Self-assessment (European Commission, 2019a), since ROBORDER's research involves human beings and collection of personal data, certain kind of information should be provided, and a number of documents should also be kept in file. This procedure has already been followed once more but following the termination of the responsible beneficiary (TEK) and the comments the Consortium received from the Ethics Committee in July 2019, all ethics documents will have to be updated with this newly inserted deliverable. D8.6 is compiled in order to address all the comments received both from the ethics review and the External Ethics Advisor that was sub-contracted by the former coordinator.

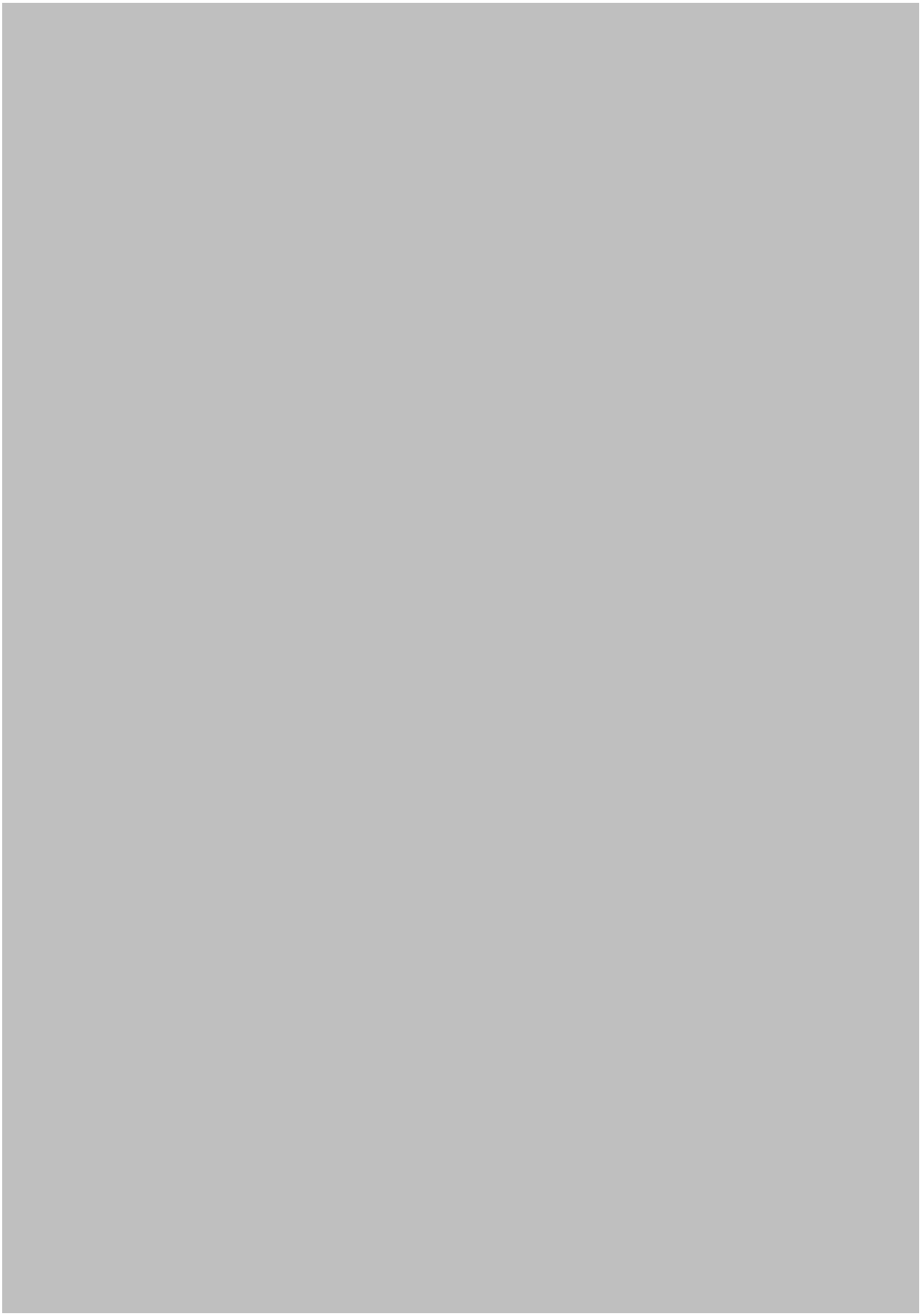
2 Research with Humans

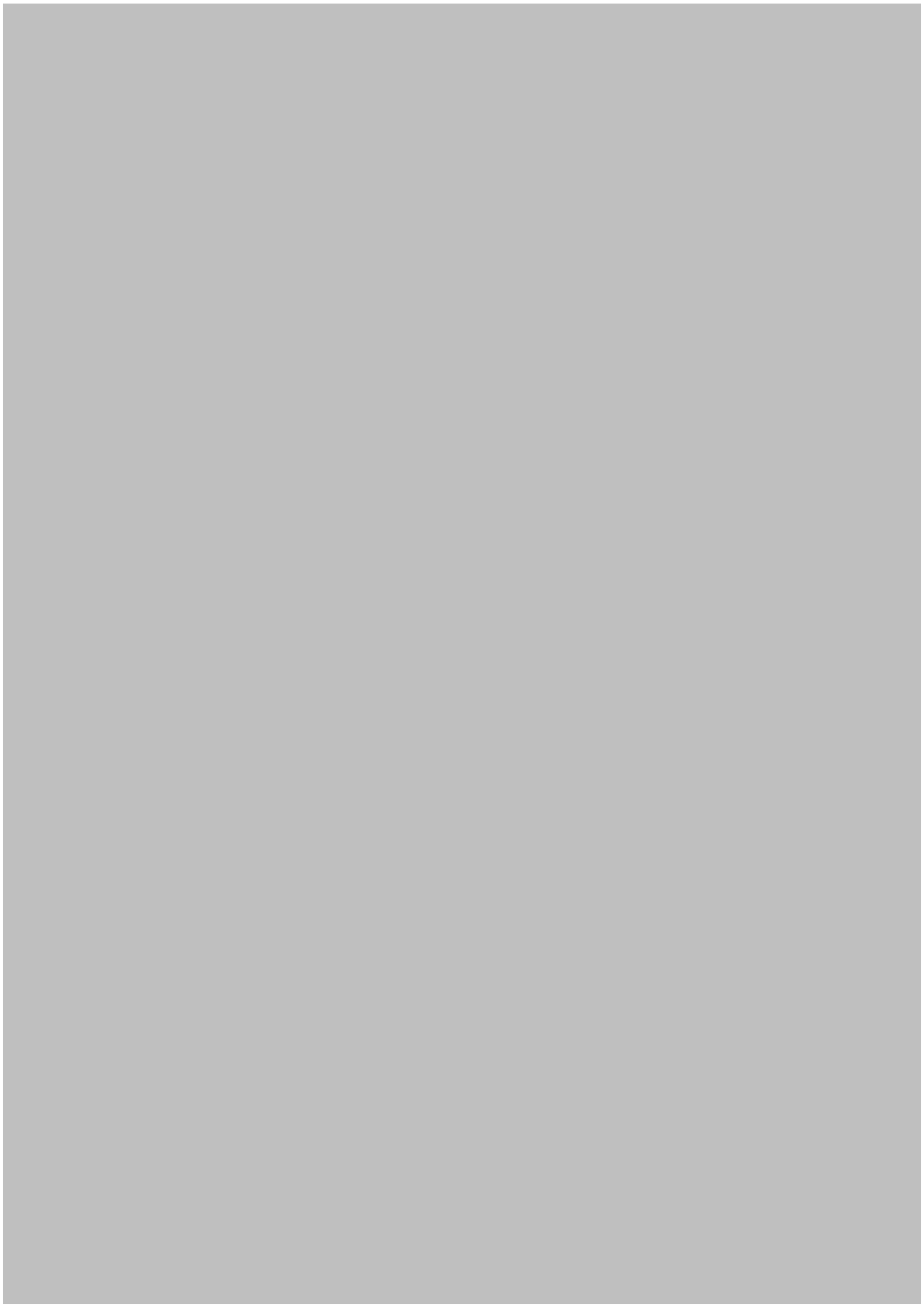
As aforementioned, ROBORDER's research involves working with humans. According to H2020 guidelines (European Commission, 2019a), working with human beings requires certain criteria to be met and specific documents to be provided. The following section focuses on the procedures followed in order to guarantee ROBORDER's compliance with these guidelines, while incorporating the pre-mentioned received comments.

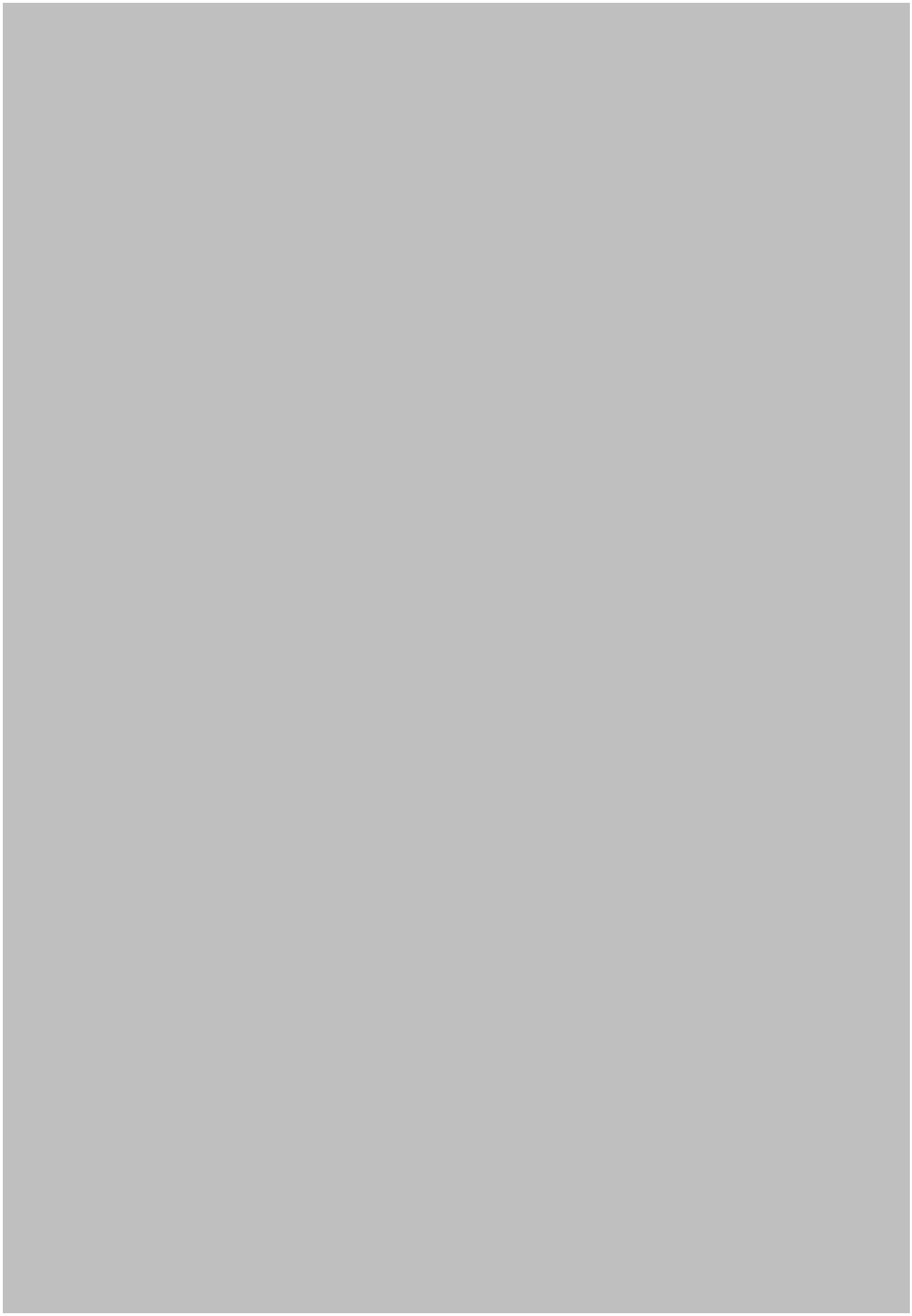
2.1 Full details of demos/operational tests

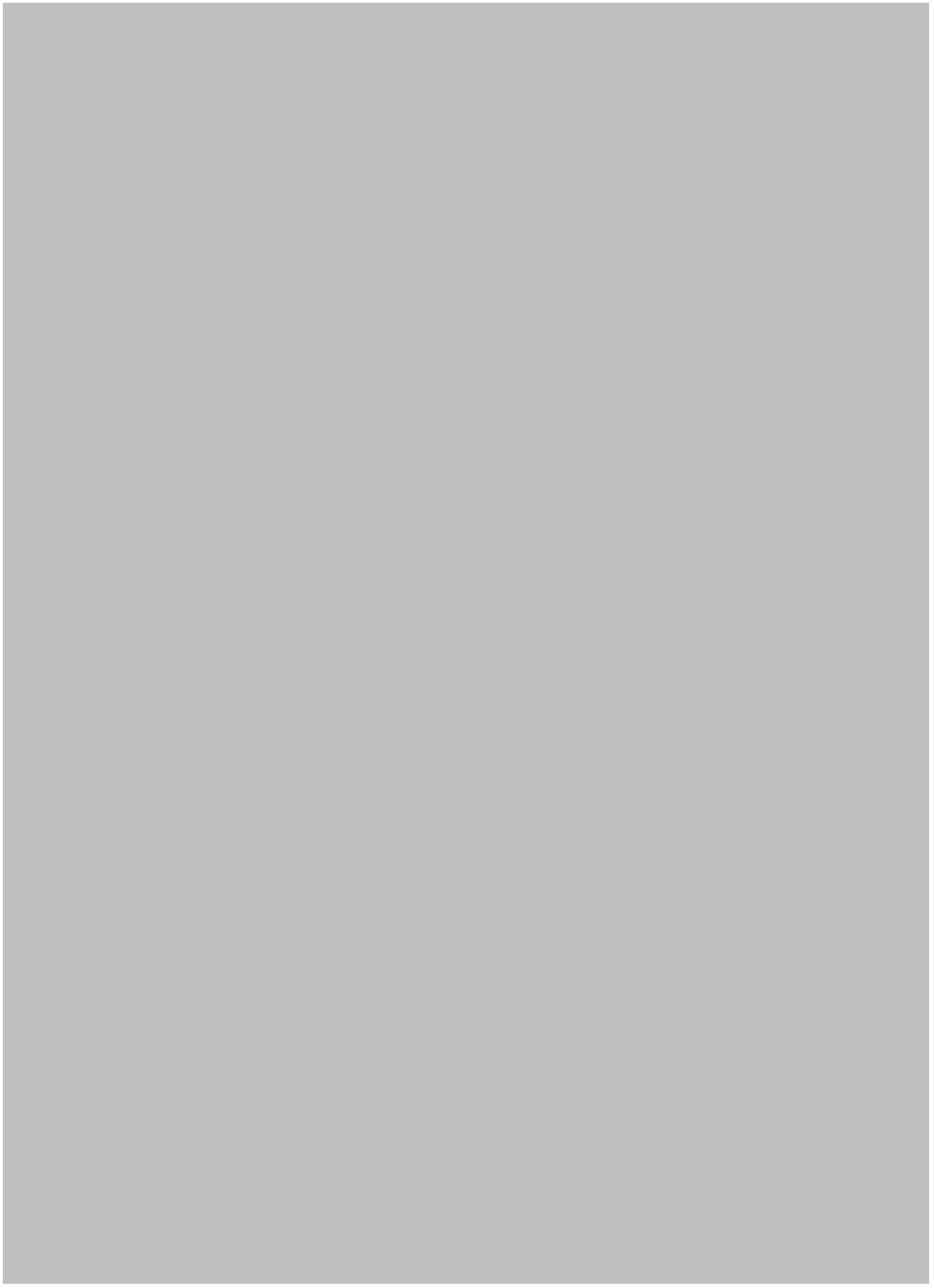












2.2 Recruitment process

ROBORDER's Consortium has identified the involvement of human participants in their demos/tests according to Horizon 2020 Programme: Guidance on How to Complete your Ethics Self-Assessment (European Commission, 2019a). The following questions have been responded to and the respective justifications have been given.

Question	ROBORDER Responses
Does your research involve human participants?	Yes; therefore, signed informed consents will be collected in order to ensure their will to participate in ROBORDER's demos/test, after they have been provided with a detailed information sheet. (the updated documents may be found in the Annex II below)
Are they volunteers for social or human sciences research?	Participants are employees of the responsible PUC partners and experts on operating the UxVs that are going to be used for the demos. Their participation in such demos/tests may be already foreseen upon their signature of contract/secondment with the respective ROBORDER partner; however, a signed informed consent will also be collected before their involvement in the demo/test in order to ensure their free will to participate under no pressure from their employers.
Are they persons unable to give informed consent (including children/minors)?	No.
Are they vulnerable individuals or groups?	No.
Are they children or minors?	No.

Are they patients?	No.
Are they healthy volunteers for medica studies?	No.
Does your research involve physical interventions on the study participants?	No.

Table 2. Ethics Self-Assessment Questions (about Humans)

In general, the Consortium will rely on **people already employed by them** and the **use of their own contacts**. ROBORDER partners have a wide network of colleagues that are able and willing to support the project's goals and participate in the demonstration/tests. Each partner can provide a number of participants that they think are suitable for each simulation, by taking into account their level of experience and expertise in the field of border security.

In this manner, the Consortium will be able to ensure that the recruited participants are relevant to the project and that they can provide the researchers with valuable feedback by evaluating various parameters of the demo/test that is being held. Additionally, managerial issues related to meetings, briefings and training will be highly mitigated, as the participants will be readily available to ROBORDER's partners – especially in the case of them being directly employed to ROBORDER.

Only adults will be contacted, in order to ensure that they will all be able to sign the consent themselves. Other than age (being over 18 years old), the Consortium will try to ensure a gender, socio-cultural and geographical balance among the participants.

In any case, after the partner has contacted the potential participant and the latter has agreed to participate in the demo/operational test, a more detailed information sheet will be provided to him/her and his/her signed consent is advised to be collected in order to proceed with the execution of the research. This step may not obligatory to some partners as the participants have already given their consent upon their signature of their contract/secondment/assignment; however, it is strongly advisable to acquire a signed informed consent from the employee, in order to ensure their **voluntary participation** and to justify that they were under no pressure when deciding for their participation in this specific demo/test.

In all cases, personal information and data that will be collected from the involved participants will be treated according to the project's Data Management Plan that has been established in deliverable D8.4 – Self-assessment and data management plan V2.

2.3 Updated information sheet

According to the prementioned Horizon 2020 guidelines (European Commission, 2019a) all recruited participants should be provided with the necessary information to fully comprehend the study that is being conducted – be it solely in writing or orally, as well – in a language that is understandable.

The updated ROBORDER information sheet:

- is written in relatively plain English vocabulary, but it is clearly stated that all potential participants are welcome to ask for clarifications or for a translation in case they think that they do not understand what it is asked of them;
- explicitly states that participation is voluntary and every participant has the right to withdraw;
- provides a detailed description of the project and this specific demo/test the participant is going to take part in;
- provides contact points for further information or withdrawal;
- states the type of (personal) data that is going to be collected and how they are going to be processed;

- has as an attachment the General Data Protection Regulation (GDPR) (2016/679);
- describes the procedures that are going to be followed in case of an incidental finding;
- explicitly mentions the participants' rights

A copy of the updated information sheet may be found in Annex II. The sections that are highlighted will be adjusted accordingly in each demo/test by the responsible partner in order to fully depict the research study that is going to be conducted.

2.4 Updated consent form

After having read the information sheet and asked any question or clarification they need, the participants will be asked to sign and consent to their participation in the study.

The updated consent form:

- states that the participant has been asked to participate in one of the Consortium demonstrations/operational tests;
- explicitly states that the participant has read the information sheet and understood it;
- explicitly states that the participant has a complete understanding of the way his/her (personal) data are being collected and processed;
- explicitly states that their participation is voluntary and that they have the right to withdraw at any point without providing a reason;
- contains a contact point in case of withdrawal;
- asks for the participant's name, signature and signature date.
- gives the participant the option to consent separately to different purposes and processing.

A copy of the updated consent form can be found in Annex II.

2.5 Copies of ethics approvals

CERTH has updated the information sheet ROBORDER's Consortium is going to use for its studies, as well as the participants' consent form (see section 2.3 and 2.4) The updated documents have been sent to CERTH's appointed Data Protection Officer (DPO) (see section 3.1), the internal Ethics Advisory Board (EAB) and the External Ethics Advisor for review. Copies of their opinions/approvals can be found in Section 5 in their submitted internal reports to CERTH.

3 Personal data protection

According to Art.4(1) of the GDPR 2016/679, **personal data** are defined as "*any information relating to an identified or identifiable natural person*", where an **identifiable natural person** is "*one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

During the demos/tests that are going to be conducted throughout the project's lifetime, basic personal data such as name, job title and contact information are going to be asked from the participants (identifiable natural persons). In addition, data are also going to be collected from the UxVs that will be operated in the field, which will be used for the detection and not the identification of a person in the demo/test area. However, since these data are going to be video recordings/images that could potentially capture identifiers of the person and location data that could lead to surveillance and/or tracking, specific rules should be set.

The following questions of the Horizon 2020 Guidelines (European Commission, 2019a) have been responded to in order to ensure the provision of the necessary information regarding these processes.

Question	ROBORDER Responses
Does your research involve processing of personal data?	Yes; apart from the collection of basic personal information via the informed consent forms and the evaluation forms that will be collected prior and after the demo, respectively; ROBORDER's research also involves the collection of imagery and videos of human participants in combination with their location data (in some PUCs). Therefore, their signed informed consents for the processing of such data are going to be collected before their involvement in the research. Information sheets with all the necessary information will also be provided to them beforehand. Additionally, information to be provided is: • technical and organisation measures for the protection of personal data (Section 3.1 for DPO involvement) • details on informed consent procedures (Section 2.3 & 2.4) • Details on the prevention of unauthorised access to the demo/test field and the collected personal data (Section 2.1 & 3.2) • details on data minimisation principle (Section 3.3) • details on the anonymization process (Section 3.3) • details on data transfers among the Consortium (Section 3.3 & 4.5)
Does it involve the processing of special categories of personal data (e.g. genetic, health, sexual, lifestyle, ethnicity, political opinion, religious	No

or philosophical conviction)?	
Does it involve processing of genetic, biometric or health data?	No
Does it involve profiling, systematic monitoring of individuals or processing of large scale of special categories of data, intrusive methods of data processing (such as, tracking, surveillance, audio and video recording, geolocation tracking etc.) or any other data processing operation that may result in high risk to the rights and freedoms of the research participants?	Yes; ROBORDER will collect imagery and videos of participants as well as location data, which can be linked to surveillance and tracking, in order to evolve the detection capabilities of the system. Other than that, no other data will be collected that could be related to the implication of a high risk towards the participant. Additional information that should be provided in this case is: • details on the methods used for surveillance and tracking (Section 2.1) • risk assessment for data processing activities (Data Protection Impact Assessment and CERTH's DPO approval can be found in Annex V) • details on how harm will be prevented and participants'' rights safeguarded (Section 3.3, 4.2, 4.4 & 4.5) • details on informing data subjects of the tracking that is going to take place (Section 4.4)
Does your research involve further processing of previously collected personal data (including use of pre-existing data sets or sources, merging existing data sets)?	No
Does your research involve publicly available data?	Yes; anonymised data will be publicly available and permission by the data owner is given through the signing of the informed consent (sub-section 3.2.2 and information sheet/informed consent in Annex II)
Is it planned to export personal data from the EU to non-EU countries?	No
Is it planned to import personal data from non-EU countries into the EU?	No

Table 3. Ethics Self-assessment Questions (Personal Data)

3.1 Data Protection Officer

According to Art. 37 of GDPR (2016/679), a Data Protection Officer (DPO) should be officially appointed in order to monitor compliance with the Regulation and other data protection law. In addition, he/she should assist all partners in every stage they think his/her contribution is needed in order to adequately safeguard the data processing and mitigate any risk of harm implicated to the participants. Moreover, all participants may reach back to the DPO of the organization that is running the demo/test, in case they have doubts or concerns regarding the conducted research activities.

CERTH has been in contact with its appointed DPO [redacted]) for guidance and advice on this matter and prepared a dedicated file reporting all activities that are going to take place during ROBORDER's demos/test and will possibly collect and process personal data. This file is to ensure the coordinator's compliance with Art. 30 of GDPR and will be kept up to date as soon as alterations and updates arise regarding data controllers or activities per se. Moreover, CERTH's DPO has also reviewed the updated informed consent form and information sheet and provided his approval via email on Jan. 31st, 2020. Lastly, he has been involved in the Data Protection Impact Assessment CERTH has drafted for the project and which may be found in Annex V.

In addition to CERTH's (coordinator) DPO, the table below contains DPOs' contact details of all partners that will conduct a demo or an operational test and will collect and process personal data via the informed consent and the evaluation forms.

Partner	Appointed DPO and contact details
CERTH	**Name**: [redacted] **Email**: [redacted] **Address**: 6th km Charilaou-Thermi Road, P.O. Box 60361, 57001 Thermi-Thessaloniki, Greece
ORFK	**Name**: [redacted] **Email**: [redacted] **Address**: Teve u.4-6, 1139, Budapest, Hungary
HMOD	**Name**: [redacted] **Email**: [redacted] **Address**: Mesogeion 227-231, Cholargos, 15451, Athens, Greece
GNR	**Name**: [redacted] **Email**: [redacted] **Address**: Largo da Estação Marítima de Alcântara-Mar, 1399-049, Lisboa, Portugal
BDI	**Name**: [redacted] **Email**: [redacted] **Address**: 2 Prof. Tsvetan Lazarov Blvd., 1592, Sofia, Bulgaria
SPP	**Name**: [redacted] **Email**: [redacted] **Address**: no 42, Bulevardul Geniului, postal code 060117, Romania, Bucharest, District 6
PSNI	**Name**: [redacted] **Email**: [redacted] **Address**: Police of Northern Ireland
EASS	**Name**: [redacted] **Email**: [redacted] **Address**: 12012, Tallinn, Estonia
AdSP MTS	**Name**: [redacted] **Email**: [redacted] **Address**: Viale Giovanni Amendola, 18 int. 15, 19121, La Spezia, Italy
MJ	**Name**: [redacted] **Email**: [redacted] **Address**: Edifício PJ Nova Sede, Rua Gomes Freire, 1169-007, Lisboa, Portugal

Table 4. DPOs contact details

No personal data are going to be collected or processed by technical partners and UxV providers; however, in case of the arisen need to do so or in case of an incidental finding, this type of data will be treated according to the partner's **privacy policy**, which is publicly

available on each partner's website. This measure is being adopted as not all partners are obliged to appoint a DPO for this cause due to their organisation's nature.

3.2 Process of personal data within the project

According to Article 4(2) of the GDPR, the processing of data includes "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*.

As a part of this deliverable, updated information was asked from all partners involved in the demos/operational tests in order to identify what type of data will be collected during their simulations. Their responses may be found in section 2 and indicated that **basic personal data**, such as name, job title, contact details, will be collected via the informed consents that will be require from the participants prior to their involvement in the demo/test. Additionally, the evaluation form that will be collected at the end of each demo/test from the participant by the responsible PUC partner will also contain the same personal information for the personalisation of the guidelines provided to the involved partners, as well as the formation of the DSS requested by each end-user.

These data are going to be collected, processed and safely stored by the responsible partner for the demo/test in secure and locked locations in order to avoid their corruption or breach. A digital copy may also be stored by some partners in secure servers that require a unique username and password, or decryption means in order to access them and will be deleted (the latest) upon the completion of the project.

Regarding the data collected from the UxVs during the demo/operational test, they will be telemetry data (such as GPS position, speed, aircraft attitude, etc.) and imagery/RBG-thermal video recordings from the cameras attached to the UxVs. These data will be transmitted to ROBORDER and will be kept safe during this process

These data will only be used for the detection of an object/person and not the latter's identification; therefore, no personal data are going to be processed during this procedure. If, for any reason, the distance or angle of the footage will allow the identification of a participant, the recording will be edited to make people unidentifiable with the use of a blurred mask or a mosaic effect.

Given the fact that ROBORDER will have the participants' consent to collect and process their data, the partners will have a lawful basis to act as such, in accordance with GDPR's Article 6(1). Additionally, the lawful basis for this processing also applies to the purposes of the legitimate interests pursued by ROBORDER's Consortium and the European Commission based on the signed Grant Agreement between the two.

3.2.1 Previously collected data

According to the partners input provided to CERTH with updated information about their PUCs, no PUC responsible partner will use previously collected data for the execution of the demo/test. The only case that this might be applicable would be the possible case of using their own contacts (outside of their organisation) in order to invite people that might be interested in such studies and they feel at ease contacting in order to invite them to participate, watch or provide feedback to the relevant partners. This will be conducted on a personal basis and no obligations or pressure will be inflicted on the contacted people.

3.2.2 Publicly available data

The collected data from the signed informed consents will not be publicly available due to their nature. Full names, email addresses and phone numbers will only be collected for managerial reasons, such as participants' lists, transportation, catering, calling in emergency situations etc. This type of data will only be available to the directly involved partners and will not be publicly available.

Anonymized edited data, on the other hand, such as blurred images from the footage collected from the UxVs or the outcomes of the evaluation forms provided to the responsible PUC partner at the end of the demo/test will be publicly available via the publication of scientific papers in journals and magazines or dissemination material, in order to successfully protect the participants' privacy, yet disseminate the project's outcomes in an effective manner.

3.3 Data Protection Rules

ROBORDER will base its data protection rules on the basic principles laid out in the GDPR:

- **Lawfulness, fairness, transparency**

As mentioned earlier, ROBORDER has identified its lawful basis for data processing which is the acquisition of a signed consent from the participant, by which he/she agrees to take part in the demonstration/operational test that is going to be executed and allows the responsible partner to process his/her data. Additionally, this processing is necessary for the purposes of the legitimate interests pursued by ROBORDER's Consortium and the European Commission based on the signed Grant Agreement between the two.

In this manner, ROBORDER ensures that it is treating the collected data in a fair way by providing the potential participant with all the necessary information they need in order to decide whether they would like to participate in this research study or not and hence, not misleading them in any way. Moreover, giving the potential participant the opportunity to ask any further question regarding the research if they feel like the information provided to them with the information sheet is not enough, indicates that the ROBORDER Consortium is willing to act in a transparent and open way. Lastly, all involved partners have appointed a DPO to whom both partners can turn for assistance and participants for clarifications or doubts.

- **Purpose limitation**

The purposes of the conducted research are clearly stated in the information sheet provided to the potential participants and are limited to: setting out the user requirements, designing the system and the used technologies for object/individual/activity detection based on the outcomes of the evaluation forms (feedback provided to involved partners from the participants) or demos/operational tests that are going to take place. If the purposes change along the way, the updated ones should be reported in the respective deliverables and mentioned in the information sheet provided to the upcoming participants.

- **Data minimisation**

ROBORDER should only collect data that are adequate, relevant and limited to what is necessary for its purposes. The personal data collected from the Consortium interaction with the participants are limited to:

  - their names (mostly because they were either the project's employees or recruited through the use of the Consortium's own contacts, therefore basic personal information is already known to the researcher),
  - their job title (for the pre-mentioned reason and for reassuring that they can provide the Consortium with valuable feedback from their participation in the demo/test),

- their email address/phone number (for contacting them for briefing and in case of emergency).

These personal data should be sufficient to the Consortium's needs in order to fulfil its purposes and they should undergo a review before the following demo is conducted, in order to evaluate which of them are still of use and which should be deleted.

Regarding the data collected from the UxVs during the demos/operational tests, as stated in the previous section, they are only going to be used for the detection of the person and will not be stored anywhere in the UxV or ROBORDER's system for more than the project's duration.

- **Accuracy**

By using the Consortium's own contacts for recruiting participants for the demos/operational tests, ROBORDER mitigates the risk of acquiring false or misleading personal data. All collected data should undergo a thorough check by the responsible partner in order to reassure that the data is correct and updated. This process becomes easier when having to deal with colleagues and acquaintances, as they are easier to keep in touch with. Additionally, by involving professionals in the demos/tests (e.g. UxV operators) the Consortium makes sure that the vehicles are going to be properly operated and will accurately focus on the data needed for the project's scopes and objectives.

- **Storage limitation**

The storage of the informed consents and evaluation forms that will contain personal data will be securely stored in the premises of the responsible partner until the project's end in order for the involved partners to run back to them for information regarding the system's improvement. As long as the data collected from the demos/tests are concerned, they are going to be securely stored in servers which are password protected and will be accessed only by the involved partners. This will be done in order for the involved partners to have proper time to evaluate and assess the collected data and to see how they can further improve ROBORDER's system.

Temporary storage will assist the Consortium with the monitoring of the project's progress and with the writing of scientific articles in journals or magazines in order to encourage future relevant researches. However, all personal data will undergo an evaluation before the following demo/operational test takes place to reassure that the previously collected ones are indeed of need.

- **Integrity and confidentiality (security)**

As ROBORDER aims at a "Privacy by Design" approach, all collected personal data are going to be treated in full confidentiality and will not be shared outside of the Consortium unless ROBORDER is required to share this information with the European Commission/national authorities as a part of its obligations – which is also stated in the information sheet provided to the participant. All participants will, of course, have the right to access, edit or delete their data upon request.

Regarding the protection of the collected data, ROBORDER's Consortium has made sure to be equipped with the necessary means in order to physically and digitally protect the data they collect. As mentioned above, hard copies of the signed informed consents that will be handed out to participants will be securely stored in areas in the responsible partner's facilities and digital copies that may be created will be stored in secure servers in the responsible partner's premises. Each person involved will have a unique set of username and password in order to access them.

For partners to share this information with the rest of the Consortium for the development of the platform's tools, they would have to make sure to **anonymize** the collected data before sharing them with the rest of the Consortium partners. Therefore, no personal data are going to be transferred and circulated among the Consortium.

More specifically, the data collected from the UxVs operated on the field (e.g. videos and imagery) will undergo a review by the object detector (operated by CERTH) based on a neural detection network which will automatically blur and cover human faces that could have been captured in the footage. The collected footage will also undergo an additional review by CERTH's object detector in order to blur and consequently anonymise any footage that might have been missed by the neural detection network. Following these two procedures, the data collected may be shared with the rest of the partners.

Moreover, in case of an accidental collection of personal data during the execution of the demo/test, ROBORDER will enforce its "incidental findings policy", which is the following:

- In case a person working for ROBORDER has enacted an illegal activity with the sole purpose of testing the system and has been detected by the system, the local practitioner authority (e.g. National Police or Navy) will issue said person with a Letter of Commission stating that he or she has performed the action resembling an illegal act for the sole purpose of testing the system. No further action is needed.
- In case a person not involved in any way in the project engages in an illegal activity detected by the system, then the person will be handed over to the border police units present who will carry out standard operational procedures determined by regulations on the given case, and all relevant data has to be secured/encrypted and handed over to the police as evidence.
- Any data collected from video, imagery or other sensors that incidentally may be considered relevant for the identification of individuals not involved in the project will be immediately isolated and erased from all storage devices (e.g. cameras).

- **Accountability principle**

ROBORDER's Consortium (especially the PUC responsible partners) is responsible for complying with the GDPR while it is conducting this research by keeping up to date the prementioned file in Section 3.1. In addition, by establishing these rules and by basing them on GDPR's main principles, ROBORDER makes sure it holds itself accountable towards its research participants. It will also make sure that it keeps its data protection rules updated according to the latest EU Directives/Regulations/national legislation, by reviewing the situation before the following demo/test is to be conducted.

4 Surveillance

ROBORDER is a project focused on surveillance, which aims at developing and demonstrating a border surveillance system. According to EC's ethics self-assessment (European Commission, 2019a) surveillance and data collecting technologies may raise concerns regarding a potential harmful impact on human rights. Therefore, the following sections are dedicated to the legal framework ROBORDER has based its actions on, the measures adopted, and the procedures followed by the Consortium, in order to mitigate and successfully deal with this risk.

4.1 Legal framework

In order to justify its purposes and its actions, ROBORDER relies its research on multiple EU regulations that are currently in force. More specifically:

- **Schengen Borders Code (Regulation (EU) 2016/399)**

In this regulation certain rules are established regarding the movement of people across borders of the EU. It is stated that border controls should take place in order to prevent people from engaging in illegal activities (such as illegal migration, trafficking, smuggling etc.) that could harm the Union's internal security. It is also mentioned that movement across the external crossing points should only take place within fixed opening hours. Border surveillance is an important part of border controls, as it is mostly used for monitoring these areas "*outside the fixed opening hours*", in order to prevent illicit activities from taking place. In addition, it is also stated that border guards may *use stationary or mobile units* (Art. 13(2)) or other *technical means, including electronic means* (Art. 13(4)) to carry out border surveillance.

- **Frontex Regulation (Regulation (EU) 2016/1624)**

This regulation describes Frontex's main tasks, which, among others, are monitoring migration flows and the management of the external borders, launching border interventions in case of illegal activities and cooperating with European Agencies. Additionally, Art. 47 explains what type of data can be collected and processed and these are: personal data of people that are suspected to be involved in cross-border crimes, personal data that are crossing external borders without authorisation and other identifiers (such as licenses plates etc.) that are linked to people being involved in one of the prementioned situations. These data, though, should be deleted as soon as they are communicated to the competent authority/agency and they should be classified according to EC's rules established in Commission Decision (EU, Euratom) 2015/444.

- **EUROSUR Regulation (Regulation (EU) No 1052/2013)**

The European Border Surveillance System (EUROSUR) is established in this regulation in order to assist Frontex and the Member States' national authorities with exchanging information and cooperating in operations. The surveillance data that will be shared to the involved authorities will be collected from ship reporting systems, satellite images and sensors mounted on vehicles/vessels, crafts (Art.2(3)). However, collected personal data from these sources can only be shared in a secure manner and through EUROSUR's communication network (Art. 7). "*Any exchange of personal data in the European situational picture and the common pre-frontier intelligence picture should constitute an exception*".

As a conclusion, surveillance at the borders of EU and internationally (see United Nations' Convention against Transnational Organized Crime) is foreseen in multiple in-force legal acts. They include new technologies as means of surveillance and data is collected, processed and shared with the competent authorities in a secure and safe manner, always taking into consideration the protection of personal data and privacy. ROBORDER attempts to contribute to the enhancement of the current border control measures with its new

technologies, in order to mitigate at the greatest extend any illegal acts that might be taking place at the Union's borders. This will, of course, be done by bearing in mind all possible ethical and societal implications that may arise, mostly due to the process of data collected from the UxVs and the possibility of misuse, which will be further elaborated in the section below.

4.2 Evaluation of ethical/societal impact

In order to succeed in safeguarding the human rights of the people involved in this project (be it in the demos/test or in its actual use after its completion), an analysis of possible ethical or societal implications should be done at this point, in order to pinpoint the sectors that most attention should be paid to.

To begin with, one may find a great variety of bibliography on concerns about protection of personal life and privacy, especially in relation to technology. There is a constant debate on whether these aspects should be traded off with security and freedom, both of which are part of EU's **Fundamental Rights** (2012). Moreover, the use of UxVs, cameras or sensors for the collection and process of (personal) data also raises concerns regarding **privacy** and **data protection**. Therefore, it can be easily comprehended why this subject usually raises tensions and controversy among EU citizens, humanitarians and migrants.

As mentioned earlier, ROBORDER does not intend to collect and process personal data of people that it does not have signed informed consents from. If a case of an incidental finding arises, then the Consortium will enforce the respective policy in order to avoid any breaches of personal data to people that do not have the "need-to-know" or other relevant authorisation. In addition, as long as the personal data required for the signing of the consent is concerned, it is mostly because the participants are already existing contacts of the Consortium, therefore basic personal information is already known to the responsible partners for the demos/tests. Moreover, all participants will be informed of the activities that are going to take place during these simulations (including the surveillance and recording aspect) through the information sheet provided to them prior to any commencement of relevant work; and all non-directly involved people will also be informed of the demo/test taking place at that current moment through the installation of signs stating so in the field of the simulation.

Complementary to the justification above and explaining the positive outcomes this research could have in the future when completed, EC's new elected president has set out 6 core ambitions for the Union for the next 5 years (European Commission, 2019b):

- A European Green Deal;
- An economy that works for people;
- A Europe fit for the digital age;
- Protecting our European way of life;
- A stronger Europe in the world;
- A new push for European democracy.

ROBORDER could significantly contribute in 4 of them – the following table describes how:

Ambition	Relevant Content	ROBORDER contribution
A European Green Deal	Preserving Europe's natural environment	Through its UxVs, ROBORDER will collect data that could prevent an environmental crisis taking place at the borders, e.g. oil spills.
A Europe fit for the digital age	Grasping the opportunities from the digital age within safe and ethical boundaries	ROBORDER will be able to prevent illicit activities taking place at the borders while collecting data that are treated with respect and in accordance with in-force EU Regulations.

Ambition	Relevant Content	ROBORDER contribution
Protecting our European way of life	-Upholding the Rule of Law -Strong borders and a fresh start on Migration -Internal security	ROBORDER will be able to protect EU citizens from criminals that are acting either at their borders or that are planning to act within them. People who are crossing the borders without authorisation will be the focus of attention without denying entrance to people who are after it in an orderly manner. The internal security of the Union will be enhanced and protected.
A stronger Europe in the world	-Defending Europe	The fact that ROBORDER acts at the border areas of the Union gives it the ability to also monitor larger scale upcoming attacks (e.g. terrorist attacks or possible affiliations with terrorist organizations) that could target a whole country.

Table 5. ROBORDER's contribution to EC's core ambitions for 2019-2024

4.2.1 Misuse and protection measures

ROBORDER's Consortium has already taken some measures in order to safeguard its research from possible misuse. More specifically, it has laid out a detailed security guidelines section in the Grand Agreement (Section 5.1.6) involving experienced security researchers that will take over when a relevant cause arises. A proper dedicated training of the involved participants is also foreseen as an additional measure in order to properly inform all participants of how to act during the demos/test and how to be safe at all times during this timeframe. In addition, it has also taken the appropriate steps in order to protect sensitive information, as all technical deliverables containing details and their implementation have been classified as EU-RESTRICTED, in order to avoid access to people who do not have the "need-to-know". With this classification, all forms of information communicated among technical partners and end-users will be in an encrypted mode using ZED! software, which is used by the Consortium. Lastly, the data used in the implementation and integration tests taking place before the execution of the demos/tests are dummy data.

4.2.2 Dual use and protection measures

According to Council Regulation (EC) No 428/2009, a dual-use item may be a software or another type of technology that could potentially be used both for civilian and military purposes. As ROBORDER provides a solution for technologically advanced means of surveillance and monitoring in a Member State's borders, it could be potentially used and exploited by militaries throughout Europe for such purposes. Since the technology and equipment used by ROBORDER is by no means destructive or lethal, it could be used to enhance the current defensive capabilities and to strengthen the feeling of security among European citizens.

However, as stated in the Grant Agreement (Section 5.1.5) the Consortium does not intend to directly apply any military standards on their system.

4.3 UxVs operations

As mentioned above, during the demonstrations, aerial, ground and surface vehicles are going to be operated in order to collect data and detect individuals/objects. More information was required from the partners involved in UxVs regarding how they have acquired their approval for operating their vehicle in the demo/test location.

For the **Portuguese** demo (PUC 3.1), the involved partners are already in contact with the manager of the Lagos airdrome in order to acquire the necessary license for operation from ANAC via the foreseen procedure for flying an aircraft that weighs more than 25kg. Moreover, an additional authorization is also sought after from AAN in order to be able to capture aerial imagery.

For the **Greek** demo (PUC 1.1), the demo is going to take place in a military base of the Hellenic Ministry of Defence; therefore, the authorization for the location's blocking and UxV operation will be given internally with the communication of this request from the respective partner involved in ROBORDER to the responsible department of HMOD.

For the **Hungarian** demo (PUC 1.3), permission will be acquired by the UAV providers that are going to operate their vehicle in the field as soon as the location and specific date are decided upon. Forms are available for download at https://www.nkh.gov.hu/dokumentumtar/pdf-elonezet/-/p/2353655/formanyomtavany-itm-uj-pdf and should be sent to rpas@itm.gov.hu. For USV providers, they are only permitted an autonomy level 1 and an autonomy level 2, which means that the operator has to be physically present in the vehicle and hold the wheel. Additionally, if the demo takes place in public roads (and not in an experimental facility), an additional permission needs to be acquired through the e-Government portal: https://uvreoffice.kozut.hu/uvr-eoffice-web/login. That has to start 42 days before the tests and it lasts for 10 days.

4.4 Informing data subjects and non-involved people

Given the fact that surveillance, monitoring and images/video/audio recordings of individuals is taking place in the context of these demos/tests, details on the procedures for informing the research participants should be provided. After assessing each demo/test case, it was decided that the responsible partners will inform the participants for such activities in the **information sheet** they are going to provide them with before commencement of any work. Additionally, all participants are given the opportunity to ask the involved partners for any relevant information they need in order to make sure that they fully understand the scope of the research and to properly assess the impact this may have on their privacy for that given timeframe of the demo/test.

Additionally, and for the proper notification of other people that may be present at the demo/test location (e.g. other employees that may be present at the responsible partner's facilities), officials will be placed in strategic points and signs will be set out in the perimeter of the location indicating that a demonstration/operational test is taking place at the moment and that the field is being monitored and recorded. Moreover, briefings of officials and employees that are not involved in the demos/test but must be present in the field will take place prior to the commencement of any relevant work.

The Data Protection Officer of the ORFK has re-assessed the situation on data processing in regard to ROBORDER according to the planned change and uncertainty of the demonstration location in Hungary. Currently it is not known whether the demonstration will take place in an area with restricted access or in those parts of the border area which are not

restricted from public access. In the second case it is possible that a person walking or driving across the demonstration area will be recorded on the footage without giving any prior consent. Analysing the actions necessary to prevent such situations, ORFK has assessed that closure of that area, thus restricting freedom of movement is not justified nor in balance with the need to prevent such. Therefore, as an alternate solution, ORFK DPO decided to register a specific ORFK data process according to GDPR Art. 6. (1) point e) and publish it on its website in order to inform third parties.

In every case that personal data or identifiers of other people (not involved in the demo/test) are accidentally collected during the simulation, ROBORDER will enforce the incidental findings policy (see section 3.3) and act accordingly.

4.5 Ethical Code

Taking all the above into serious consideration, ROBORDER can form its ethics policy that is going to base its research on, in order to be in accordance with H2020 guidelines and EU regulations.

- **Understand social and ethics challenges**

As mentioned above, the Consortium understands the reasons why a surveillance system may raise concerns among citizens, as it might seem as an intrusion to their privacy. The Consortium will keep conducting desk-top research and monitoring the situation in order to have a deeper knowledge of the subject and to be able to successfully handle it. Experienced security professionals are already involved in the project, who can prove of help to reassuring citizens and research participants that their involvement in this project will not cause any harm to them. Responsible partners for demos/operational tests should be available to communicate with their participants and provide them with all the information they need.

- **Put high priority on transparency and accountability**

The Consortium should always be transparent and open about the procedures they follow and the data they collect towards the participants. They should state in detail in the information sheet which activities are going to take place in this specific demo/test and what will be asked of the participant to do. They should always be explicit and precise. In addition, they should clearly state what type of data are going to be asked and collected from the participant during his/her involvement in the research. The participant will of course have access to his/her data in order to review, edit or delete them upon request from the data controller.

- **Have a lawful basis**

For its research purposes, ROBORDER will have a lawful basis to act as stated above by fully informing the participants about their involvement in the project and letting them freely and voluntarily decide whether they would like to participate or not. By no means should there be any kind of pressure over the participants and they should become aware that they are free to withdraw at any stage of the research without providing any reason. All this information will of course be clearly stated in the information sheet they will be provided with. In addition, in case of a demo/test taking place at the responsible partner's premises, the DPO will be aware and will provide his/her consent before commencement of any work. In case of a demo being conducted outside of a partner's premises, the UxV operator should make sure that they notify the National Data Protection Authority and guarantee their consent and accordance to national legislation before commencement of any work.

Given the fact that ROBORDER will have the participants' consent to collect and process their data, the partners will have a lawful basis to act as such, in accordance with GDPR's Article 6(1). Additionally, the lawful basis for this processing also applies to the purposes of the legitimate interests pursued by ROBORDER's Consortium and the European Commission based on the signed Grant Agreement between the two.

Regarding people that have not provided the Consortium with their consent to participate but they are present in the field of the demo/test, the responsible partner should always make sure that they set up signs or allocate officials in strategic points to make sure they inform non-involved people that this specific space is being recorded. If that proves inadequate and an incidental finding of a person not being directly involved in the simulation appears, the responsible partner should enforce the incidental findings policy and act accordingly, with no infringement to the person's privacy.

- **Pay respect to Human Rights**

In order to further mitigate any ethical concerns that may arise, ROBORDER will always take into serious consideration the Human Rights declared in EU's respective Charter (2021) and put special focus on the right on liberty and security, the integrity of a person, the protection of private life and the protection of data. ROBORDER has as a goal the enhancement of the current border security systems and will attempt to minimize criminality in these areas to the maximum extent, increasing levels of security among EU citizens. In addition, certain Data Protection Rules has already been set out (see section 3) and are already followed by the Consortium in order to protect the data collected and the outcomes of the research.

- **Protect collected data**

As mentioned above, the Consortium has established a set of rules in order to properly collect and process (personal) data during the project's lifetime. Only basic personal information (such as name, contact details etc.) is to be collected from the participants in the stage of the consent form. This is merely because the Consortium used their own existing contacts, therefore basic personal information is already known. In the information sheet it should be clearly stated which data will be collected the demo/test (e.g. video footage), how they are going to be used (only for the detection of the person and not their identification), where and by whom they are going to be processed.

Additionally, as the technical partners will need the collected information in order to adjust and modify their technologies, all collected personal data are going to be anonymized, before being shared with the technical partners. Moreover, in case of an incidental finding that involves a suspicious person, the data that are going to be shared with the authorities will be encrypted and secured, in avoidance of a possible breach to the public. In case of an incidental finding of a person that is by no means involved in this research and there is no suspicion over them, then the data are going to be immediately deleted from all storage devices (e.g. UxVs cameras). As a consequence, no personal data are going to be transferred to the rest of the Consortium.

Only data considered necessary for the successful conduct of the research should be collected, which are the data that will help ROBORDER's technologies detect a person in a certain area and not identify them.

- **Keep monitoring reforms in order to be updated**

Since technology and society are constantly evolving, new ethics issues may arise or be addressed. Therefore, the Consortium should always closely monitor the updates and reforms all EU Regulations may undergo and make sure that they comply with them. This will be succeeded by having periodic reviews (before the next demo/test is to be carried out) in order to make sure that everything is done according to EU/national legislation.

5 Ethics reports

In this sector, the ethics reports alongside the ethics opinions/approvals from the External Ethics Advisor (EEA) and the internal Ethics Advisory Board (EAB) are provided.

5.1 External Ethics Advisor's report and comments

CERTH has taken the submitted EEA report (D9.6 – in Annex III) into serious consideration and addressed his comments/suggestions in order to compile this deliverable. The updated input from the ethics deliverables, alongside the updated information provided to CERTH by all partners involved in the demos/operational tests and the acquisition of all the proposed ethics approvals have contributed in compiling this new deliverable for the amendment of the ethics issues that have arisen in these last years of the project's lifetime.

The first EEA's report alongside the Ethics Check Report that were taken into consideration when compiling this deliverable can be found in Annex III and Annex IV, respectively. When drafting this deliverable, an additional report was requested from the EEA in order to ensure ROBORDER's current compliance with the European Regulations. After reviewing the report, some additional comments were ensured to be addressed, such as the Dual Use section which can be found above. The complete report may be found below.

5.1.1 Report from [redacted] EEA

5.1.1.1 Past EEA work

The EEA –besides minor exchanges – performed detailed reviews of the deliverables D9.1 to D9.6 and proposed a methodology for the systematic evaluation of the outcome under the aspects of Ethical, Economic, Legal, Political and Societal criteria (EELPS). Seven related EEA reports (EEA repot #1) were delivered in August 2018. All input has been documented in D8.6, Annex IV with sub-Annexes.

5.1.1.2 Actual EEA work

5.1.1.2.1 Tasks

In preparing the next ethics-related project steps, the EEA was tasked to review the draft deliverable D8.6 and to deliver:

a) "...approval of/opinion on the updated informed consent and information sheet. (D8.6, Annex II)

b) a brief report on how he is being involved in ROBORDER's processes and on how ethics issues are dealt with"

Work has been supported by the "Initial Assessment" report, V0.4. The EEA assessment should also include tracking and assessing of how the earlier EEA recommendations have been regarded an implemented.

5.1.1.2.2 Informed Consent and Information Sheet and Ethics Approval

The document D8.6 ANNEX II contains a brief project status summary, lists the project partners, describes the principles of handling personal data and privacy, the Data Protection Officer, and the template of the "Informed Consent Statement".

This has to be confirmed and signed by all participants and individuals of which personal data issues will be concerned.

EEA Comments:

- It is understood that only very few numbers of partners and individuals will be concerned with this issue.
- GDPR is the guiding framework.
- The Form is considered appropriate for its purpose.
- The form will be applied to project partners.
- For external participants (e.g. in trials, demos, exercises) it remains somewhat unclear how their personal data will be treated.

These comments may be used as **Ethics Approval** for the informed consent and information sheet (Annex III of D8.6)

5.1.1.2.3 Cooperation of the EEA

So far, the EEA has communicated with and reported to the coordinators mainly electronically. No specific personal meetings were held or requested.

There were few earlier telcos with the old and new coordinator persons, but mainly on the contractual issues.

5.1.1.3 Implementation of Ethical Issues

5.1.1.3.1 General

Time given and resources available allowed only a limited review and assessment of the project's "ethical" status, including D8.6 and its Annexes. The Coordinator confirmed that the EEA input of 2018 (EEA Report # 1) were regarded.

5.1.1.3.2 D8.6 Review Process

The Deliverable follows the main functions of the ROBRDER system to perform, including:

- unauthorized border crossing,
- early identification of boats,
- tracking of organized crime,
- detection of drug trafficking,
- detection of jamming attacks and
- detection of pollution accidents,

and describes the proper handling of the main requirements of ethical impacts in the project according to the EEA's first report including:

- research with humans (requirement #5)
- protection of personal data (requirements #6 and #10)
- other ethical issues (# 14) and
- general ethical requirements including surveillance and "ethical code".

Discussion of Dual Use features (requirement #15) of the ROBORDER results could not be identified beyond the documentation of the earlier EEA's Dual Use (requirement #15) comments.

Regarding and implementing the recommendations of the EEA are confirmed but cannot be assessed in detail here.

It remains unclear how and how far the results of the Internal EAB have been implemented in D8.6 and possibly in other deliverables.

(Most) references (D8.6, Section. 6) are not referenced in the text.

5.1.1.4 Evaluations by the EEA

5.1.1.4.1 D8.6 and its Annexes

The ROBORDER team invests considerable effort into the adequate specification to meet the Ethical requirements of the project (see also Section 5.1.1.3 above).

After reviewing the deliverable, it is understood that most of the EEA's previous recommendations have been taken into serious consideration by the Consortium while drafting D8.6. As this deliverable serves as an update on the previous submitted ethics deliverables (D9.x), it is assumed that the same applies for these, as well.

Annex I of D8.6 is considered appropriate for the setting up of the pilot use cases (PUC).

Annex II on "Updated information sheet/informed consent" is considered appropriate for "research with humans" in regard to the information the Consortium will provide the participants with, the data they will collect and the rights the data subjects have.

In Annex III "EEA Ethics Report", the report #1 of the EEA has been adequately documented here.

Annexes IV (Ethical Check Report) and V (Data Protection Impact Assessment (DPIA)) are considered appropriate. However, the EEA could only give them a brad screening.

Generally, and specifically concerning D8.6 and Annex II there, the EEA considers the ethical issues handled properly in this project. Additional recommendations of this EEA report should be considered, and these measures documented.

5.1.1.5 Further Findings and Recommendations

5.1.1.5.1 Guidance for Future Users

The "Ethical Code" as described in D8.6 mainly addresses the matters and requirements of the Project and its partners. It is advised that this valuable work will also be transformed into an "Ethical Guideline" for future users. Much of D8.6 could be directly used for that, possibly formulated more general as future use will imply a broader spectrum of scenarios, broader than those of the ROBORDER project. This Ethical Guide should become part of the D&E work.

5.1.1.5.2 Dual Use

The characteristics and the ethical and societal consequences of the Dual Use capabilities and potential of the ROBORDER results have not been found discussed and evaluated although many of them appear obvious. (see also EEA comments in Section 2.2.1.5 of Annex III)

5.1.1.5.3 Extended socio-political and ethical evaluation

In Annex III, the EEA has also provided in Section 6 – Annex 2 some recommendations on how to map and evaluate the key elements of the ROBORDER output against the variety of ethical risks and on assigning responsibilities. It is suggested that these or similar recommendations will be implemented in WP6.

Also, a method for extended socio-political evaluation has been suggested by the EEA in Annex III. The suggested EELPS evaluations are discussed. Performing that in great detail may be somewhat beyond the scope of the project. However, it should be regarded as a substantial recommendation in the D&E discussions and deliverables as a valuable tool for future users.

5.1.1.5.4 Communications

There was very little technical discussion and exchange between the project and the EEA. A direct contact and possible better harmonization of the work of the internal EAB and the EEA could have possibly improved the work on ethics. Maybe that will still be feasible during the remaining phases of the project.

5.2 Internal Ethics Advisory Board's report

CERTH has contacted ROBORDER's internal EAB in order to assist them in the compilation of this deliverable. ROBORDER's EAB is constituted from experienced security professionals that could provide insightful feedback regarding ethics issues:

An additional report was requested in order to ensure ROBORDER's compliance with the European Regulations, in which the Board's ethics opinion/approval may be found.

5.2.1 Report from

5.2.1.1 Summary

Surveillance by mobile robots is a relatively new technology, especially in the non-military applications. In addition, there is still no established practice, precedent cases or res iudicata related to such innovations as surveillance by mobile robots. As ROBORDER is dealing with such machines and it must be compliant with GDPR during demonstration and testing, Data Protection Rules had to be elaborated. The Data Protection Rules and the Informed Consent Sheet is in accordance with GDPR and – considering that there is no established practice in this aspect yet – it is thorough as possible. Regarding the Hungarian pilot, an internal workshop was held at ORFK HQ with participation of the appointed DPO in February 2020. On that workshop, a series of actions have been decided to provide the best possible coverage regarding information provided to data subjects, including those who became data subjects due to accidental findings (e.g. entering area under surveillance by the test system). Taking everything into account, the ROBORDER Consortium had did everything in its capability and competence to cover the privacy aspect of the project and issues raised in the initial assessment are addressed as well. The author of this report is a Doctor of Law and Political Sciences, member of the Europol Data Protection Experts Network with 15 years of experience in data protection, author of multiple papers on the topic.

5.2.1.2 Methodology

After initial assessment of ethical issues, an internal assessment procedure has been initiated at the ORFK in order to clarify the position of ROBORDER activities according to privacy framework. This report was done using the input from the ad-hoc working group established for this internal assessment procedure. It consisted of experts delegated by the following entities:

1. Department of EU Subsidies (chair)
2. General Secretary of the High Commissioner (DPO)
3. General Department for Border Policing
4. Bács-Kiskun County Police
5. Scientific Council of the Hungarian National Police
6. Aviation Security Department of the Airport Police Directorate
7. Communication Service
8. [redacted], andragogist, contracted expert
9. [redacted], Task Leader, Ethical Advisory Board member delegated by ORFK

After preparations and initial discussions over email and teleconferences, the working group had a workshop in Budapest, on the 25th of February, where positions were discussed, and the joint opinion was formulated in order to not only envisage but also realize the highest possible level of privacy without endangering any of the innovations undertaken in the Grant Agreement signed for this project.

5.2.1.3 Scope of the assessment

This position did not cover the data process in the envisaged final and operational ROBORDER system, only the data process carried out in ROBORDER project as an innovation action. This is because of two main reasons: first, data process by an authorized law enforcement system is mainly falling under the Police Directive instead of GDPR (except when it is used for research purposes for example); second, authorization of such a system would eventually come with related amendment of relevant regulatory framework, which may constitute specific, well justified, proportional and reasonable data process authorizations.

During the assessment it was concluded that during the project it is inevitable to process the following personal data:

1. full name
2. audio and/or video record, including photos
3. username (and password where third-party authentication not possible)
4. e-mail address
5. phone number

from the following data subjects:

- contracted experts
- staff of ORFK participating in the project.

In addition, as currently it is not known whether the demonstration will take place in an area with restricted access or in those parts of the border area which are not restricted from public access. It was concluded that closing off a border area where people are living because of the project would not be proportional nor justifiable. Therefore, in the second case it is possible that a person walking or driving across the demonstration area will be recorded on the footage without giving any prior consent. This is considered as an accidental finding however it will result in capturing video record which may be appropriate for identification of the individual (this cannot be determined in advance). Considering the possibility, this will also result in a data processing and as such, included in the scope of assessment.

5.2.1.4 Opinion on the data process in ROBORDER project

According to the definitions and scope of Police Directive[1], innovation activities carried out during the ROBORDER project are not included in the subject-matter of the directive:

Art. 1. (1) of Police Directive: "This Directive lays down the rules relating to 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, including the safeguarding against and the prevention of threats to public security."

[1] Directive (EU) 2016/680 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

According to the Police Directive, if ORFK, as a law enforcement authority wishes to process data for innovation purposes, such as ROBORDER, GDPR has to be applied:

Art. 9. of Police Directive: *"Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply unless the processing is carried out in an activity which falls outside the scope of Union law."*

Therefore, data processing in ROBORDER project has to be carried out according to GDPR, regardless which partner is carrying out the task.

Security of borders is a public interest and the responsibility of the state as declared in The Constitution as well as multiple laws and international treaties. In Hungary, the competent authority responsible for border security is the ORFK. The reason for the ORFK to participate in the project ROBORDER is to better serve this public interest through innovative solutions. As the achievements of the project are of public interest, the application of GDPR Article 6. (1) e) is proportional and justified.

Art. 6. (1) e) of GDPR: *"[Processing shall be lawful only if and to the extent that at least one of the following applies:….]*

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; […]"

The same article of GDPR allows to have more than one legal ground for data processing. In order to increase transparency and strengthen the legal ground of data processing where possible, ORFK concurs with the opinion of the Consortium that the informed consent has to be acquired (GDPR Art. 6. (1) a)), even where the data process itself is also based on a contract (in case of contracted experts), covered by GDPR Art. 6. (1) b).

Last but not least, regarding the demonstration planned in Hungary, as leader of the task including the planned demonstration, ORFK considers itself the representative of the controller towards third persons residing in Hungary (especially towards local residents of the demonstration area) and therefore will provide extended information on data processing according to GDPR Art. 30. which will be published on its official website in Hungarian language due time ahead of the demonstration. The information sheet will be prepared according to the internal Data Protection Rules of the ORFK: Command No. 39/2019 (XI.19.) of the Chief High Police Commissioner of Hungary.

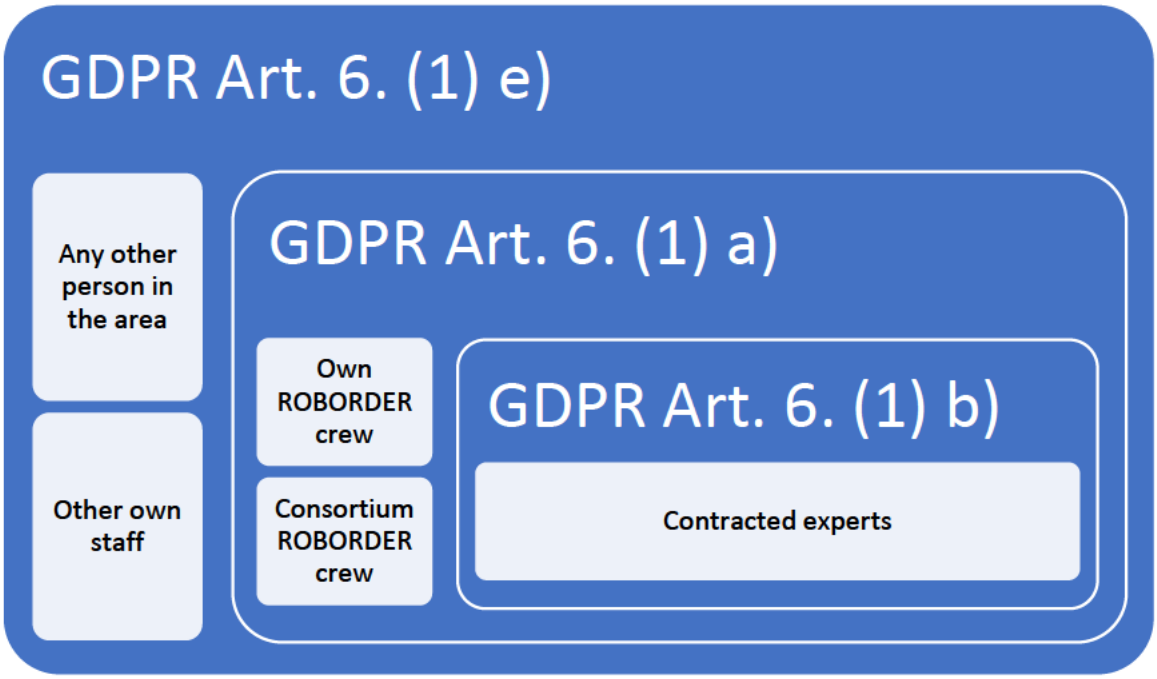


Figure 1. Visualization of legal grounds and data subjects

5.2.1.5 Additional communication measures

In order to minimalize accidental findings (record video on third persons), local residents will be informed about the planned demonstration in advance by using local media channels and the ORFK website, just like it would be in case of a sporting event, Head of State visit, movie shooting or other events which may result in increased surveillance activity. As the location of the demonstration is not yet decided and in the current pandemic situation the date cannot be determined for sure either, it is not possible to start a communication on this right now.

5.2.1.6 Collaboration with the Independent Ethics Advisor

Under these circumstances, personal meetings are not feasible, therefore collaboration is facilitated via sharing documents. In case discussion is needed, a teleconference will be put up, however so far this was not necessary.

5.2.1.7 Conclusion

This partial EAB report presented an example how the EAB contributes in case of end-users to deal with ethical issues, especially related to field demonstrations. The initial assessment showed some gaps which needed small updates, but no major corrections, but those gaps were closed, for example by implementing an additional WP, WP9. Taking everything into account, the ROBORDER Consortium had did everything in its capability and competence to cover the privacy aspects of the project and issues raised in the initial assessment are addressed as well on both Consortium as well as individual partner level

6 References

Charter of Fundamental Rights of the European Union (2012). Official Journal C326. 26.10.2012. p. 391–407. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the *security rules for protecting EU classified information*. *Official Journal* L72. 17.3.2015. p. 53–88. [online] Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015D0444

Council Regulation (EC) No 428/2009 of 5 May 2009 *setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items*. Official Journal L134. 29.5.2009. p. 1–269. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009R0428

European Commission (2019a). *Horizon 2020 Programme - Guidance: How to complete your ethics self-assessment, v6.1.* [online] Available at: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

European Commission (2019b). 6 *Commission priorities for 2019-24*. [online] Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024_en

Directive (EU) 2016/680 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. Official Journal. L119. 4.5.2016. p. 89–131. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur). Official Journal L295. 6.11.2013. p. 11–26. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R1052

Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code). *Official Journal* L77, 23.3.2016, p. 1–52. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0399&from=EN

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). *Official Journal* L119. p. 1–88. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

UN General Assembly (2001). *United Nations Convention against Transnational Organized Crime: resolution / adopted by the General Assembly*. A/RES/55/25. 8.1.2001. [online] Available at: https://www.refworld.org/docid/3b00f55b0.html

7 Annex I – Details on PUCs

Details on demonstrations/operational tests

Pilot Use Case description [PUCX.X: Title]

[Please indicate the no. and title of your PUC and provide a description: where it is going to take place (city, country), when (exact date, if not known yet, project month), what is the purpose - which WPs/sub-tasks would you like to test, which activities are going to take place and what the participants will be asked to do in the pre-mentioned activities]

Participants recruitment procedure

[Please indicate how you recruited your participants (e.g. people employed in the project, use of own contacts, snowball techniques, participants from a previous study that you have their written consent to re-contact them? etc. do you plan to provide them with an information sheet and get their signed consent before the commencement of any work?)]

Types of data collected

[Please identify which type of data will be collected during the informed consent (e.g. basic personal data: name, age, contact details, job title, etc.? sensitive data: health, sexual lifestyle, ethnicity etc.?)

Also indicate what type will be collected during the demo/test by UxVs/cameras/sensors (e.g. video/audio recordings? images? etc. – are they going to be used for detection ONLY or for the identification of a person as well?]

Are any of these data:

Publicly available: ☐

Previously collected: ☐

If previously collected, do you have a lawful basis to use them in this case?
(consent, contract, legal obligation, vital interest, public task, legitimate interest)

☐ YES ☐ NO

UxV details
Total No. of UxVs ☐

[Please provide as much technical details as possible regarding the equipment employed and the procedures of the activities in which Personal Data will be collected / processed.

Please indicate whether you have obtained the required permission to operate your UxV – if yes, describe how you acquired it – if not yet, describe how you will. Make sure to abide by both EU regulations and national legislation.]

Filming in Real Time	Yes	☐	No	☐
Transfer of Data to Third Parties	Yes	☐	No	☐
Process interconnections	Yes	☐	No	☐

Recipients to whom personal data may be disclosed

[Please identify and describe the recipients of the Personal Data involved in the activities (e.g. data subjects themselves, employees within the organisation, government / regulatory authorities, other organisations processing data on behalf of the Data Controller, other third parties)]

Transfer of personal data abroad

[Please describe if the Personal Data will be transferred. If yes, please specify if it will be transferred to EU Member States and / or other third countries.]

Security measures during the demo/test

[Please describe the security measures planned for the simulation exercise to ensure compliance all EU Directives

and informing people of the surveillance that is going to take place in that location for a specific amount of time (e.g. putting up signs indicating the commencement of a demo/test, restricting people to access the simulation area)]

Security measures for processing and/or storing personal data

[Please describe the security measures relating to processing and / or storing of Personal Data. This involves, not exclusively, methods of storage and exchange (e.g. LAN, cloud, secure servers), data structure and preservation (e.g. encryption, anonymization), data-merging or exchange plan and commercial exploitation of data sets.

RESPONSIBLE FOR THE PROCESSING (Data Controller)

Name _____

ID _____ Activity _____

Address _____

Post Code _____ City _____ Country _____

Phone _____ Mobile _____

E-mail _____

PERSON OF CONTACT (regarding the demo/test)

Name _____

Phone _____ Mobile _____

E-mail _____

ORGANISATION

Name _____

Department _____

Address _____

Post Code _____ City _____ Country _____

Phone _____ Mobile _____

E-mail _____

Type of Organization *(tick where appropriate)*

Government Department	☐	Public Corporation or Authority	☐
Health	☐	Civil Partnerships	☐
Education	☐	Company	☐
Financial Services	☐	Foundation / Association	☐

Other: _____

Nature of Business:

Please describe the nature of business of your organisation.

DETAILS OF DATA PROTECTION OFFICER

Name _____

Address _____

Post Code _____ City _____ Country _____

Phone _____ Mobile _____

E-mail _____

8 Annex II – Updated information sheet/informed consent

General Information

You have been requested to participate in a research conducted by ROBORDER's Consortium which is coordinated by CERTH (Centre for Research and Technology – Hellas). ROBORDER is a project funded by the European Commission regarding an autonomous swarm of different robots for border surveillance. This document will provide you with all the necessary information you need in order to fully understand why this research is taking place and what it involves, before you decide whether you would like to participate.

Participation

It should be noted here that your participation is completely **voluntary,** and you can **withdraw** at any time of the process without providing any reason. In order to do so, please contact [responsible partner], whose contact details can be found at the end of this document. After contacting him/her, you will be asked whether you would like us to permanently delete your data or if you agree with this data to continue being processed. In addition, you might be asked the reason why you would like to withdraw from the research, but you are not obliged to answer. In addition, in the case of being recruited by your employer, please make sure you are under no unjust pressure to participate. Therefore, we would like to ask you to carefully read the following, make sure that you fully understand the research and its scope and ask for any clarifications or translation, in case you think you need it.

The project

ROBORDER aims at developing and demonstrating a fully functional autonomous border surveillance system with unmanned mobile robots including aerial, water surface, underwater and ground vehicles which will incorporate multimodal sensors as part of an interoperable network. The main goal would be to enhance the current surveillance system with detection capabilities for early identification of criminal activities at border and coastal areas along with marine pollution events.

ROBORDER's research started in May 2017 and will be completed in February 2021 – more information can be found at the project's website: https://roborder.eu. As stated above, this research is funded by the European Commission under Horizon 2020 (Grand Agreement No.: 740593, Call: H2020-SEC-2016-2017, Topic SEC-20-BES-2016, https://cordis.europa.eu/project/rcn/209949/factsheet/en) and is run by 25 partners across Europe:

1. Centre for Research and Technology Hellas (Greece)
2. Fraunhofer Gesellschaft zur Foerderung der Angewandten Forschung E.V. (Germany)
3. Sisekaitseakadeemian (Estonia)
4. Teknologian tutkimuskeskus VTT Oy (Finland)
5. Everis Spain SL (Spain)
6. Police Service of Northern Ireland (United Kingdom)
7. Ministerio da Administracao Interna (Portugal)
8. NATO Science and Technology Organisation (Belgium)
9. Orszagos Rendor – Fokapitanysag (Hungary)
10. Robotnik Automation SLL (Spain)
11. Serviciul de Protectie si Paza (Romania)
12. Elletronika GMBH (Germany)
13. Ministry of National Defence (Greece)
14. Sheffield Hallam University (United Kingdom)
15. Autorita di Sistema Portuale del Mar Tirreno Settentrionale (Italy)
16. OCEANSCAN – Marine Systems & Technology LDA (Portugal)

17. Institut Po Otbrana (Bulgaria)
18. Copting GMBH (Germany)
19. Ethniko kai Kapodistriako Panepistimio Athinon (Greece)
20. CSEM – Centre Suisse d'Electronique et de Microtechnique SA – Recherche et Developpement (Switzerland)
21. Consorzio Nazionale Interuniversitario per le Telecomunicazioni (Italy)
22. Ministerio da Justica (Portugal)
23. Cyberlense LTD (United Kingdom)
24. Inspectoratul General al Politiei de Frontiera (Romania)
25. EVADS – everis Aerospace and Defence Division (Spain)

Description of the research

[state what the research will involve: where it is going to take place, when, how long will it last, why is it going to take place (which WP/sub task will you test), which specific activities will it involve, what will the participants be asked to do, what personal data are going to ask from the participants or collect from the UxVs – be as specific as possible – this information can be copied-pasted from the PUC Details document CERTH has asked you to fill in]

By taking part in the pre-mentioned activities, you will be asked to provide this information:

- Name
- Professional affiliation
- Contact information
- … [add all kinds of information you'll be asking from the participant]

Photographs and video/audio recordings will be made during your participation in this research (e.g. interviews audio recordings, video recording of participation in the demonstration etc.). This information will be used for adjusting the project's user requirements, system design and used technologies for object/individual detection. Additionally, the information you will provide us with may also be used for the writing of articles in journals or industry magazines, conference presentations and workshops or for further dissemination purposes. No other use of your information will take place without your written permission. You can also review these recordings upon request to [responsible partner]'s responsible concerning the research:

Name:
Address:
E-mail:

Benefits gained with the research and possible harm caused to participants, if any

Although, there will be no immediate benefits from participating in this research, the outcomes will contribute to enhancing European Union's resilience against criminal activities taking place at the borders, as well as, against environmental disasters. No physical harm or damage is expected to be inflicted on the participants.

Personal data and privacy

[responsible partner] is only collecting and processing personal data in connection with the research's informed consents and for so long as it is required by the project. Only the absolute necessary data for the project will be collected and processed. These data will be kept strictly confidential and will not be shared outside of the Consortium **UNLESS** we are required to share your information with the European Commission/national authorities as a part of our obligations.

The description of the personal data register and information concerning the rights of the data subject in accordance with EU General Data Protection Regulation (2016/679) is in attachment with this document.

All personal data are processed in accordance with EU General Data Protection Regulation (2016/679). Video and still imagery will be collected but only for the purposes of **detection** of persons, **not their identification** (i.e. detection of the presence of humans in an image or video). This information will be used for the purposes of Search and Rescue missions by border authorities and prevention of criminal or illicit activities. ROBORDER will not perform identification of persons through any data collected during the project.

In case of **incidental findings**, meaning that the ROBORDER system detects anything illegal or unintentionally captures personal data through its sensors (e.g. cameras) that may lead to the identification of individuals, one of the following procedures will be followed according to each case:

- In case a person working for ROBORDER has enacted an illegal activity with the sole purpose of testing the system and has been detected by the system, the local practitioner authority (e.g. National Police or Navy) will issue said person with a Letter of Commission stating that he or she has performed the action resembling an illegal act for the sole purpose of testing the system. No further action is needed.
- In case a person not involved in any way in the project engages in an illegal activity detected by the system, then the person will be handed over to the border police units present who will carry out standard operational procedures determined by regulations on the given case, and all relevant data has to be secured/encrypted and handed over to the police as evidence.
- Any data collected from video, imagery or other sensors that incidentally may be considered relevant for the identification of individuals not involved in the project will be immediately isolated and erased from all storage devices (e.g. cameras).

Contact Points

- For information regarding the research/withdrawal (Data Controller):
  Name:
  Affiliation:
  Address:
  Email:
  Phone:
- Coordinator's Data Protection Officer:
  Name: [redacted]
  Affiliation: CERTH – Center for Research and Technology Hellas
  Address: 6th km Charilaou-Thermi Road, P.O. Box 60361, 57001 Thermi-Thessaloniki, Greece
  Email: [redacted]
- [responsible partner] Data Protection Officer:
  Name:
  Affiliation:
  Address:
  Email:

Each ROBORDER partner stated above is a joint-data controller, meaning that all partners have a common objective/purpose regarding the data processing; have designed this process together and have a common information management set of guidelines.

Your rights

- **Right to access**: you may access your data and ask copies of your data whenever you like.
- **Right to rectification**: you may ask us to rectify the information you have provide us with in case you think that something is missing or is incorrect.
- **Right to erasure**: you may ask us to erase your personal data at any given moment without a specific reason.

- **Right to object**: you may ask us to stop processing your personal data and withdraw at any given moment from the research
- **Right to data portability**: you have the right to ask us to transfer your personal data t another party or directly to you.

INFORMED CONSENT STATEMENT

I have been requested to participate in a research conducted by ROBORDER's Consortium, [responsible partner] coordinated by CERTH – Centre for Research and Technology Hellas.

☐ I have read **the Information Sheet concerning the research** and gained sufficient understanding about the research.

☐ I have read **the description of the personal data register and information concerning the rights of the data subject** and gained sufficient understanding about the processing of my personal data and the rights that I have concerning processing of my personal data.

☐ I understand that it is completely voluntary to participate in this research and consent to the processing of my personal data. I have at any time the **right to withdraw my consent** to any of the above without announcing any specific reason for my withdrawal. The contact person at [responsible partner] for this purpose is:

Name:
Affiliation:
Address:
Email:
Phone:

With my signature I hereby confirm my participation in the described research and state my voluntary consent to the processing of the personal data in accordance with the information contained in the above-mentioned documents.

Full Name:
Professional affiliation:
Email address:
Phone:
Signature of Participant:

Date: ___/___/20__

9 Annex III – EEA Ethics Report

HORIZON 2020

GEN – REQUIREMENT NO.19

ROBORDER
740593

Deliverable Information
Deliverable Number: D9.6 **Work Package:** 9
Date of Issue: 05/11/2018
Document Reference: 740593-ROBORDER-D9.6-GEN Requirement No. 19
Version Number: 1.0

Nature of Deliverable:
Report

Dissemination Level of Deliverable:
Confidential, only for members of the Consortium (including the Commission Services)

Author(s): [redacted] (EEA)
Keywords: external ethics advisor report
Abstract:
Report by the ethics Advisor to be submitted to the Commission with the periodic reports

Document History

Date	Version	Remarks
08/10/2018	1.0	Final version

Document Authors

Entity	Author
EEA	[redacted]

Disclosure Statement: The information contained in this document is the property of <PROJECT CONSORTIUM> and it shall not be reproduced, disclosed, modified or communicated to any third parties without the prior written consent of the abovementioned entities.

Executive Summary
Report by the External Ethics Advisor

Table of Contents

Document History....50
Document Authors....50
Executive Summary....51
Table of Contents....52
List of Tables....53
List of Figures....53
List of Acronyms....54
1 General Situation....55
1.1 Related Security Skills....55
1.2 A Specific Ethical Focus....55
1.3 Communications....56
2 Activities of the EA....56
2.1 Preparation and Concept....56
2.2 Requirements Review....57
2.2.1 Review of Deliverables....57
2.2.2 Some General Issues....58
2.3 Mapping of Requirements to Components....58
3 Ethical and Societal Evaluation....60
4 Way Ahead....61
5 Annex 1 Review Sheets....61
5.1 D9.1....61
5.2 D9.2....62
5.3 D9.3....64
5.4 D9.4....65
5.5 D9.5....68
6 Annex 2 EELPS Evaluation Proposal....70

List of Tables

Table 1: Relevance of Ethical Issues..... 59
Table 2: Referencing of Ethical Requirements 59

List of Figures

Figure 1: Integrated risk, cost and qualitative socio-political assessment 56
Figure 2: A Typical EELPS Result 61

List of Acronyms

Acronym	Meaning
EEA	(External) Ethical Advisor
[redacted]	[redacted] Ethical Advisor
EEAB	External Ethical Advisory Board
QCA	Qualitative Criteria Analysis
EELPS	Ethical, Economic, Legal, Political, Societal: An acronym of an assessment methodology and tool
POPD	Protection of personal data
ICT	Information and Communications Technology
GDPR	General Data Protection Regulation

Table 6 – List of acronyms

1. General Situation

1.1 Related Security Skills

[redacted] was invited in 2017 to join the EEAB of ROBORDER. [redacted] has worked in a number of national and EU Security R&D projects in domains of security and disaster management concepts, design of scenarios and use cases for experimentation and exercising, development of assessment methodologies and tools, planning and execution of exercises and demonstrations of security related solutions, evaluation of project outcomes and of exercise results, and supporting dissemination and exploitation with numerous publications and marketing activities.

1.2 A Specific Ethical Focus

In more recent projects of the past 6 years [redacted] has, beside the typical activities above, concentrated on methodologies for assessing security investments and security measures form the viewpoint of social, ethical, political and legal, environmental and business related factors that influence the planning and decision on security measures. Most of these criteria are of qualitative character which makes the assessment even more sophisticated than e.g. the calculation or simulation of damages.

Nevertheless, these factors often explicitly or in a more hidden form ultimately dominate decisions on security more than the pure desire to reduce risk at a reasonable level of cost. This was also realized as an important aspect in security research and has consequently given certain priority in HORIZON 2020 SEC research. So socio-economic assessment must be embedded in risk analysis and cost-benefit evaluations, this way building a triple of assessment strands combined to an integrated assessment of security measures.

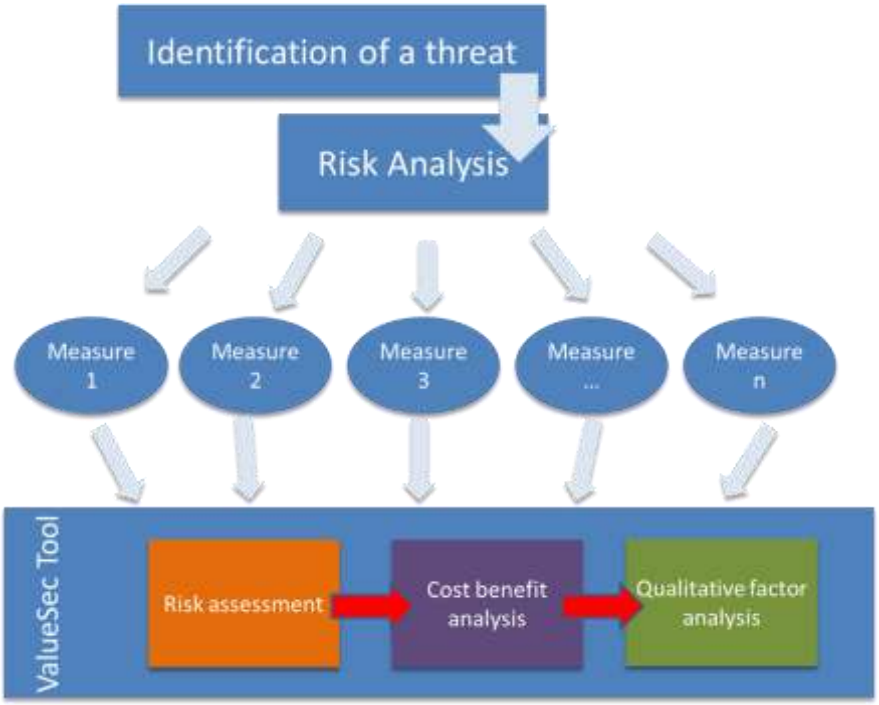


Figure 2 Integrated risk, cost and qualitative socio-political assessment[2]

This background and the associated cooperation with sociological oriented partners do form the main motivation to act as EEAB member in this project. The ethical criteria to be regarded are part of the "qualitative factor analysis" in **Error! Reference source not found.** above. M ore details are discussed in chapter 0.

1.3 Communications

Communication of the EEA and the project team, in particular with the coordinator, has been organized via e-mail exchanges and telephone. There was no physical meeting during the reporting period.
Communication went very prompt, reliable and task-oriented.

2. Activities of the EA

2.1 Preparation and Concept

The Advisor started with the analysis of the main project documents. From there, a first estimation of the importance of ethical implications was gained, of the technical and operational solutions to be developed in ROBORDER.
So the ethical escorting of and advice to ROBORDER will concentrate on these questions:

- Which are the project requirements that are relevant for ethical impacts
- How will the operational concepts regard the ethical side
- How will the technical solutions have impact on ethical reservations and appreciations in society, groups or individuals
- In which type of scenarios are ethical evaluations particularly sensitive

[2] From ValueSec, WP7

- In this sense, scenarios should include assumed threats and attacks, the ROBORDER operational concept, and the technical components (sensors, platforms, networks etc.)

It is realized that the ROBORDER will have to regard high "standards" of estimating and treating ethical implications. This is usually a two-way street, finding out (a) which ethical requirements should be regarded from the start – to be developed in WP9, an (b) how will the final ROBORDER solutions be evaluated under critical ethical examination

2.2 Requirements Review

In Aug. and Sept. 2018, evaluated the series of draft Deliverables of WP9: D9.1 to D9.5. A template for systematic review of the deliverables was created. Comments of the reviewer are marked in the column to the right, whether they are of general (G) interest or more specifically related to Ethics (E).The individual review results are supported by a number of general Notes that apply to all or a number of deliverables (see 0), a suggested scheme for mapping of requirements (chapter 0). This is followed by a proposed systematic evaluation of the ROBORDER ethical implications, along the methodology discussed briefly already in chapter 0. (See also chapter 0). References, quotations, acronyms etc. should be harmonized throughout all deliverables.

2.2.1 Review of Deliverables

The individual review sheets as delivered to the coordinator are copied into Annex 1 of this D9.6. Only some highlights are extracted here:

2.2.1.1 D9.1- Research with Humans- Req.#5

There should be a more systematic referencing of the various documents (from the EU in particular) on treating ethics. There seemed still to be a confusion, naming "ethical and legal requirementsl" in the same context, although these are different things.

2.2.1.2 D9.2-Protection of Personal Data -Req't#6

There are too many texts from regulations. Focus is on privacy. POPD, however, is more, e.g. it includes right to manage, withdraw, right of transparency, ownership etc. Some "elastic clauses" of the GDPR are criticised as a warning. However, this is not a project issue to be regarded but not solved in ROBORDER. Again, too much text from regulations. More focus should be given on what it means for the project.

2.2.1.3 D9.3-POPD -Req. # 10

It seems relevant only for two partners instead of "all". There are still formal deficits. There seems no necessity to "...transfer outside the EU and European Economic Area... due to technical reasons", and I would not agree to this, particularly when based on the extremely vague formulation. "The existence of automated decision-making, including profiling": This definitely needs specification and transparency to the data owner and the operator.

2.2.1.4 D9.4-Other Ethical Issues- Req.#14

Requirements should not be limited to UAVs but also cover: autonomous border surveillance system with unmanned mobile robots including radars, aerial, water surface, underwater and ground vehicles....heterogeneous robots ...command and control unit, decision support tools, etc. A suggestion of a systematic mapping of ethical implications and ROBORDER elements is described in chapter 0).

2.2.1.5 D9.5-Dual Use-Req.#15

Terms such as "performance", "misuse", "adequate measures..." are rather vague and should be more clearly defined, what they mean in ROBORDER. It is unclear why and how National Data Protection Authorities will be involved. The process of "In cooperation, they identify risks and devise strategies when required to diminish and deal with likely risks" needs to be specified. Staying "free of military standards" may not be achievable. In particular in ICT, there is no clear distinction between military and civil standards.

2.2.2 Some General Issues

There are some recommendations of the EA that may apply to all or more than one of the five deliverables reviewed:

- Establish list of references
- Refer to references in the WORD hyperlink mode
- Establish and complete list of acronyms (maybe one for all deliverables D9.x)
- Introduce a "common" introduction that briefly describes for an "external" reader the ROBORDER platform, the planned use cases for experimenting with the "test bed" and the "simulation mock-up", and the key roles of players in these experiments
- Copies from relevant regulations in the deliverables should be kept to a minimum while the focus should be on describing what the referenced regulations etc. will specifically mean for the ROBORDER project.
- At some points, it should be clearer distinguished between the terms ethical, legal, societal and political implications and whether they are relevant in (a) the ROBORDER trials and (b) the future possible application/operation of a ROBORDER-type platform or component.

2.3 Mapping of Requirements to Components

For a better understanding of an outside evaluator of ethical etc. aspects, but also as a common reference inside the project, it may be helpful to have a more systematic overview of (a) the key ROBORDER technologies and components to be addressed, (b) which kinds of ethical, societal etc. requirements need to be met and (c) in which deliverable they are documented.

Table 7: Relevance of Ethical Issues

ETHICS SYSTEM	Data Protect'n	Privacy	Physical health	Mental health	Societal factors	Environment	Politics	Respon-sibility	???
Technologies [3]									
IT security	X[4]								
Data eval.	X		To be filled						
Concept of operations									
Command & Control	X				X				
Handling of false...		X							
Scenarios, Use Cases									
???									

Overview of the handling of ethical and societal issues in ROBORDER
Dx.y = related project deliverable

Table 8: Referencing of Ethical Requirements

ETHICS SYSTEM	Data Protect'n	Privacy	Physical health	Mental health	Societal factors	Environment	Politics	Responsibilities	???
Technologies[5]			?						
IT security	D9.2								
Data eval.				To be filled					
Concept of operations									
Command & Control									

[3] Should be broken down into the individual technical/system components
[4] Sample Maks only
[5] Should be broken down into the individual technical/system components

Handling of false...									
Scenarios, Use Cases									
???									

This is only a very draft scheme which of course would need to be completed and explained in detail by the project team. The EA could give some advice or review.

3. Ethical and Societal Evaluation

In [redacted] role as Ethical Advisor, he offers also to contribute to the evaluation of the coming ROBORDER system and platform when it will be exploited and implemented in simulated or real live environments. CESS has been involved in a number of EU projects where [redacted] and team have developed a methodology and a set of tools for the evaluation of the

- efficiency (risk reduction),
- the economic impacts (Cost-Benefit)
- ethical impacts

of security "Measures". Those "Measures" to be evaluated could be any kind of advanced technology solutions (as in ROBORDER), organizational and/or procedural measure, investment in training and skills, and others, or a combination of several single measures.

From an ethical, societal view, the EA would refer you to the so called EELPS6 methodology and tool. It was developed in a former project ValueSec (http://valuesec-project.atosresearch.eu) under the acronym QCA (qualitative criteria assessment) and further modified and applied in a series of Use Cases in three more recent projects, ECOSSIAN (http://ecossian.eu), CIRAS (http://www.cirasproject.eu) and PULSE (http://www.pulse-fp7.com). On the basis of the knowledge gained in these projects, a simplified EXCEL-version of the tool has been created by [redacted].

It should be a good D&E issue, also appreciated by the Commission, when projects this way make use of results of former EU projects, in our case from the late FP7/SEC program.

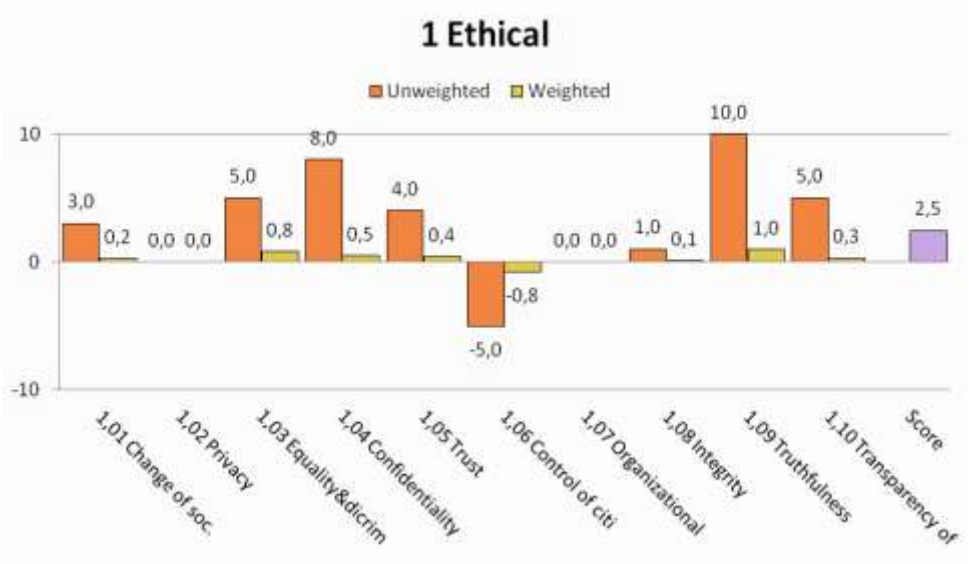
Depending on the final number of deliverables still to be reviewed by the EA, there may remain some budget left to contribute more substantially on this EELPS evaluation issue of ROBORDER.

Some input to D6.1 and D6.8, could be created, e. g. a separate chapter on EELPS evaluation. This would of course require some closer cooperation with the platform's functional architects, the test case designers, and with those responsible for the WPs/Tasks related to ethical and societal implications.

A typical high-level EELPS result is presented in **Error! Reference source not found.**.

[6] Ethical, Economical, Legal, Political, Societal implications

Figure 3 A Typical EELPS Result[7]



The figure shows the relative impact of a security measures on society, in terms of ethical criteria. Criteria can be specifically defined or chosen from a large list of pre-dfined ones. [redacted] first step, a scheme could be offered, of EELPS evaluation criteria and a description of the EELPS evaluation methodology. In the project, we could present a demonstration of the methodology and tool for a selected use case or few use cases. The Methodology could also be recommended as voluntary or even as a mandatory step in future processes of implementing the ROPORDER technical system/platform in the real environment. This recommendation may become a chapter in the exploitation report D7.8. According to the EA contract we could book this activity as an extended "assessment of project deliverables". The text on this EELPS subject as delivered to the Coordinator in Aug. 2018 is also attached at 0 Annex2.

4. Way Ahead

The Ethical Advisor will continue working for the project according to tasks assigned by the coordinator. His role in monitoring and evaluating ethical criteria will cover two different p.o.v.:

a. The ethical aspects and criteria which need to be realized and regarded in the design of the ROBORDER system and the experiments of whichever type, and in the use of personal data, as discussed in the D9.x deliverables, and
b. The ethical, societal, legal etc. impact and implications a system such as the ROBORDER platform or its components will have when it would be fielded and operated in the "real world".

As discussed in chapter 3, [redacted] offers to perform an EELPS evaluation, at least a demonstration sample. This Idea has been well received by the coordinator.

5. Annex 1 Review Sheets

as delivered to the coordinator on 25 Aug. 2018

5.1 D9.1

[7] Sample test case form previous projects

ROBORDER
Review of Documentation
Review of Deliverable D9.1
Title: H - REQUIREMENT NO.5 – (Research with Humans)
Reviewer: [redacted]
Review date: Aug. 2018
General Notes:
Introductory remark: I am making statements here which may also apply for the other deliverables that I still have to review. I would not always repeat them in the further review sheets. I will not identify typo or grammar flaws (maybe with a few exceptions).

(2) This is the first Deliverable I am reviewing. The information I have on the planned "Simulation Mock-up" is very limited. E.g. al list and short description of the basic requirements as numbered from No5 to No 19 would be very helpful.
(3) There is no reference to such "simulation mock-up" in the WP objectives as they are described on the ROBORDER home page. What is the relation of this towards the planned "test-bed" and the final "ROBORDER platform" demonstrations
(4) For an evaluation of ethical aspects, it would be helpful to know more about the planned use cases and about the roles of the participants in the tests and demonstrations.
(5) Lists of Acronyms and list of references are either incomplete or missing

Pg/chpt/para	Review Contents	Ethical/ General	
1	What does the "H" mean in the headline?- Research with HUMANS? The abstract is not self explanatory enough	G	
6	List of acronyms t.b. completed	G	
7/1/1	What is "every single law"? e.g. of all partner nations?, across the EU? They will substantially differ between member states.	E	
	If you refer to the H2020 ethical guidelines, please name the relevant sources. There are numerous H2020 documents talking of Ethics. It may reach from e.g. http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm ? up to https://www.echr.coe.int/Documents/Convention_ENG.pdf Please set up and maintain a list of references & ref. documents	G	
7/2/2	Here you talk about "...all set of ethical AND legal requirements". This is much more than "ethical" alone. Who has set the legal requirement and where are they set?	E	
9/3/1	Correction: "....will be identifyied..."		
9/3/2b)	Do you mean unauthorized instead of unable, or both?	G	

5.2 D9.2
ROBORDER
Review of Documentation
Review of Deliverable D9.2
Title: POPD – REQUIREMENT NO.6 – Protection of Personal Data

Reviewer: [redacted]
Review date: Aug. 2018

General Notes:

(1) I think the approach in this deliverable, quoting, explaining, even copying a huge number or paragraph of the different EU regulations is not too helpful for the individual Consortium partners. It is rather a justification towards the Commission than on what you did the Analysis.

(2) Nevertheless, when I take the role of a potential Consortium partner, I would have preferred a guideline on what is really to be expected within the project and which typical personal data will be needed and what partners need to practically do in order to comply with regulations, with the GDPR in particular.

(3) Annexes I and II are for sure helpful, and with some recipe and references to the important paragraphs of GDPR and maybe other regulations should have done the job.

Pg/chpt/para	**Review Contents**	**Ethical/ General**	
1	POPD: I assume it to mean Protection Of Personal Data. It is not even contained in the list of acronyms	G	
4	Again, a list of main references to documents is missing	G	
8/2/3	All sources quoted here should be referenced in a list of references	G	
8/3/3, last line	Last line: What exactly do you expect here from the EA to "...deem appropriate"?	E	
8/3/4	The "solution" should not only "safeguard privacy" but also other ethical, legal societal and political implications such a "solution" will have an impact on	E	
9/2.1/1 bullet 5	What means "strictly necessary", how is it defined, who identifies it, who is authorized to decide? If this is not the right place where to specify more precisely, you should refer to a document where this is or will be done in the project.	E	
10/ 2.1 bullets1&2	I do miss a paragraph on **transparency**, data **ownership**/ proprietary **rights**, the right to remove or alter personal data, and on the **obligation** of the data user to inform the owner on the location and type of use of personal data: see e.g. the recent Facebook scandals. ('data ownership rights'); refer to GDPR Articles 13 and 14. Also the need of the data user/controller to inform data owners/ data subjects on the type of data storage, purpose, exploitation, profiling and possible transfer.		
11/3/1&2	Please enter the quoted references into the list of references.		
12/3,1,2/2 e)	This is another "elastic clause"		
13/3.1.3/1	Correction: "...decission..."		
13/3.1.5/3	This is another "elastic clause"		
15/4/1	~~GDPR 2016/679? I only know of "REGULATION (EU) 2016/679 "~~		
15/4/2	I don't think it is helpful to copy the regulation rather than just highlighting what is important for the project. The		

	quoted article contains obligations of member states, not of Consortium members... It is overloading partners; leaving pg.16,pargr3 &4 and referring to the practical Annexes should be enough		

5.3 D9.3
ROBORDER
Review of Documentation
Review of Deliverable D9.3
Title: POPD - REQUIREMENT NO. 10
Reviewer: [redacted]
Review date: Aug. 2018

General Notes:

(1) If I screened the annexes correctly, there are only two partners (VTT and Hungary Police) who will collect and deal with the personal data?
(2) So this whole process of POPD seems somewhat over-emphasized (see below remarks when you say "all" partners
(3) On the other hand, the report text and Annexes III and IV suggest that all partners may be involved with personal data. Isn't this a contradiction or discrepancy?
(4) Informed consent Forms (Annex III) still missing from Hungary Police. Or will it be requested from all partners?

Pg/chpt/para	Review Contents	Ethical/ General	
1	The Abstract talks about "...Collection and Processing of Personal Data Assessment" of all Consortium partners". On the other hand, the Annexes II say that there will be only two partners. Isn't this a contradiction?	G	
8/2/2	Annex II is not the "last" attachment; you also have I to IV	G	
9/ last para.	Again: why "all" partners if only two will handle personal data? You should say which partners will have to fill this Annex III template and where it will be documented	G	
10/para3	I am missing my name – or is there a difference between "ethical Advisor" and "External E. A."? Is INSTITUT PO OTBRANA the same as Bulgaria Defense Institute ?	G	
11/2 √ No.2 &5	The exception for "public interest, scientific or...research purposes or statistical...." opens almost **any options for abuse,** although it is stated in (50),and many following paragraphs of the GDPR. Whenever you quote this exception (as you do also in other deliverables) you should mention that this is not a blank acceptance but is clearly specified/limited in (156) and many other places of the GDPR e.g. Art. 89. This also applies to other Deliverables	E	

	where this exception is quoted.		
12/ Header:	Are these "Principles Applicable..." or principles to be applied ? "aplicable" doesn't mean much!	E	
15	This or a similar paragraph on acknowledgements should also show in the other deliverables	G	
148/Annex III/pg.2	Pargr.2 on "**Personal Data**" refers to "Attachment 1...". Where is it? Is it Attachment to D9.3 or to Annex III or to Finnish Personal Data Act (523/1999)? Pargr. "**Consent....**" refers to "Section2": Section 2 of what? Again, reference is made to Attachment 1 (?) Paragr."**Further information** ...": again, there is no "Section2 "	G	
148/149: Annex III	Again, according to Annex I, there will be only two partners relevant.	G	
150/ Annex IV	Pargr. "**Purpose of**...." refers to Task 1.5, which I cannot identify in the document. I assume you mean Task 1.5 of the GA Annex1 (??). Nevertheless, I think the purpose of processing will also involve other Tasks, e.g. use case descriptions (T1.4), data processing (T. 2.1), evaluation of results (WP6) and more.	E	
151	Para. "**Recipients....":** ...VTT's ...project members: is that clearly limited? where registered? Who can nominate "project members"?	G	
151	Pargr. **"Transfer....":** I don't see the necessity to "...transfer outside the E..U.. and European Economic Area... due to technical reasons", and I would not agree to this, particularly when based on the vague formulation "...due to technical reasons" (this can be everything).	E	
151	Para: "**The existence of automated decision-making, including profiling":** This definitely needs specification and transparence to the data owner and operator "**The Period...":** Why 5 years? from which data onwards? After the end of the project?	E	
151	Para. **"Principles....":** needs specification	E	
151	Para **"Right to lodge**....": This makes only sense, if the "Supervisory Authority" for the project in named.	G	

5.4 D9.4
ROBORDER
Review of Documentation
Review of Deliverable D9.4
Title: OEI REQUIREMENT NO. 14 (Other Ethic Issues)
Reviewer: [redacted]
Review date: Aug. 2018

General Notes:

(1) see page 2 below

Pg/chpt/para	Review Contents	Ethical/ General	
1	What is **OEI**? Is not even in the list of Acronyms	G	
1&3	Executicve Summary (same as Abstract) : Too short	G	
7/8	D9.4, is limited to UAVs. From Annex I, however, I conclude that ROBORDER aims at a fully-functional autonomous border surveillance system with unmanned mobile robots including radars, aerial, water surface, underwater and ground vehicles....heterogeneous robots ...command and control unit, decision support tools, etc. Not knowing details about the technologies and the concept of operations yet, I assume, however, that all these technologies and their operation will have ethical implications and underlie national and/or EU regulations. I could imagine, that each of these technologies and its operation would have some impact on "Other" ethical etc. implications	E	
	See my Text and Tables below; you may want to use it in the introduction to all documents on ethical requirements. Of course this is a template only that would need extension and completion.		
9	Who am I? EAB member? EEA? EEAB Member?	G	
10	**References** : This header should show in the ToC	G	

Suggestion on a systematic mapping of driving ROBORDER elements and their possible ethical implications.

Schematic overview of treating Ethical requirements in the ROBORDER project

For a better understanding of an outside evaluator of ethical etc. aspects, it may be helpful to have a more systematic overview of (a) the key technologies and components to be addressed, (b) which kinds of ethical, societal etc. requirements need to be met and (c) in which deliverable they are documented. Many requirements, are documented in WP1 (e.g. T1.3), others in WP9.

From my p.o.v., the key **elements** that "drive" ethical implication include (to be completed):

- Technologies of the different kinds (drones, sensors, air, ground, water, underwater)
- IT security &data protection, incl. data storage, data management, analysis and communications
- Data evaluation, algorithms etc.
- Concept of operations (no-go areas: ethical, logical, geographical,..; tele-operations)

- Command & Control functions and processes
- Handling of false positives and false negatives
- Scenarios and Use Cases
- ???

The possible **ethical risks** and required restrictions will include (to be completed):

- Protection of personal data, incl. transparency and ownership handling
- Violation of privacy
- Impact on physical health
- Impact on mental health
- Impact on societal cohesion, stability, ...
- Environmental effects
- Possible political conflicts (e.g. in border areas)
- System failure modes
- Responsibilities in case of failures, damages, risks, ...
- ???

Overview of the handling of ethical and societal issues in ROBORDER
X = Relevance

ETHICS SYSTEM	Data Protect'n	Privacy	Physical health	Mental health	Societal factors	Environment	Politics	Respon-sibility	???
Technologies [8]									
IT security	X[9]								
Data eval.	X		To be filled						
Concept of operations									
Command & Control	X				X				
Handling of false...		X							
Scenarios, Use Cases									
???									

Overview of the handling of ethical and societal issues in ROBORDER
Dx.y = related project deliverable

ETHICS SYSTEM	Data Protect'n	Privacy	Physical health	Mental health	Societal factors	Environment	Politics	Responsibilities	???
Technologies[10]			?						

[8] Should be broken down into the individual technical/system components
[9] Sample Maks only

IT security	D9.2								
Data eval.				To be filled					
Concept of operations									
Command & Control									
Handling of false...									
Scenarios, Use Cases									
???									

This is only a very draft scheme which of course would need to be completed and explained in some more detail.

5.5 D9.5
ROBORDER
Review of Documentation
Review of Deliverable D9.5
Title: DU – REQUIREMENT NO. 15 – Dual Use
Reviewer: [redacted]
Review date: Aug. 2018

General Notes:

(1) I agree that according to the H2020 Template, ROBORDER involves technology with military potential. In how far an authorization is required (Template under chpt.4), I cannot judge.
(2) Some of the attributes such as "performance", "misuse", "adequate measures..." are rather vague and should be more clearly defined, what they mean in ROBORDER (details below).
(3) #s 1. to 10. on pg.10, I assume, are quotations from the GA and cannot easily be changed. I, however, doubt some of them to really make sense (see below)
(4) Classification "RESTREINT EU": Why do you use the French term here? The English version is EU RESTRICTED (and b.t.w., the correct French wording would be RESREINT UE (not EU)).

Pg/chpt/para	Review Contents	Ethical/ General	
6	The figure is Figure1, not 2	G	
7/2	It would be nice to have concise Answers right at the end if the 3 questions	E	
8/3/2	"...due confirmation by the competent National Data Protection Authorities...". Will you state somewhere which Nations those will be?	G	

[10] Should be broken down into the individual technical/system components

8/3/3	I think, only stating "In cooperation, they identify risks and devise strategies when required to diminish and deal with likely risks" may not be sufficient. Which process has been or is being defined in the ROBORDER project in order to achieve this? Where is/ will it be documented?	E	
9/3.2/1	Not having GA 5.1.5 in front of me, it is not generally true that "...civilian needs...are much less demanding in terms of performance than military " . I think, risks may not arise from performance rather than from the potential to be dual(ly) used or even misused.	E	
9/3.2/3	"...not applying directly..." and "...adequate measures are put in place..." are rather vague promises. What is a "...higher degree of applicability..."?	E	
10/3.2/1.	"...military standard..." : Having in mind passive radars, drones, cameras, radio communications etc, I doubt whether you will stay absolutely free of military standards. I even think it is not necessary to say so. Particularly in ICT, there is no border between military and civil standards.	E	
10/3.2/4.	"...easily detectable...": should that be advised?	G	
10/3.2/7.	There is no rationale why the ROBORDER components should have "...shorter flight endurance than military ones".	G	
10./3.2	Last sentence "... the research published results will be cautiously selected." Please revise semantics of the sentence.	G	
11/3.2.1/1	Line4 "..dual use threat." Dual use, per definition in not necessarily a threat. I therefore would write here instead: "...threat of misuse or abuse".	E	
11/3.2.1/2	Line2: Maybe better write: "...sensitive information and technology..."	E	
12/4/Table3	Line Item 1: If you mark it with "YES", you need to say something on how you will regard export regulations, licensing, who will do the authorization etc. From the whole text if D9.5, I would conclude you better mark line item 1 also with "NO". If you leave it YES, then Column 3/line1 of the template would require answers to the 3 questions in column 3, which may become very complex and difficult. My suggestion is to say No with a footnote that there is some Dual Use potential but no Dual Use activity in the project.	G	

6. Annex 2 EELPS Evaluation Proposal

as delivered to the Coordinator on 25 Aug. 2018

ROBORDER
Review of Documentation
Proposal of assessing ethical and related implications
Review of Deliverable D9.x
Title:
[redacted], EAB
Review date: Aug. 2018

General Notes on the evaluation of Ethical, societal etc. implications:

(1) For an evaluation of ethical aspects, it would be helpful to know more about the planned use cases and about the roles of the participants in the tests and demonstrations.
(2) In my role as EAB member, I will try to distinguish between at least two categories of ethical impacts:
    a. the ethical aspects and criteria which need to be realized and regarded in the experiments of whichever type, as discussed in the D9.x celiverables, and
    b. The ethical, societal, legal etc. impact and implications a system such as the ROBORDER platform will have when it would be fielded and operated in the "real world"
(3) Do you think this (4) is a useful approach? The reviews of the D9.x deliverables relate to task a. above.
(4) Throughout this general approach of discussing requirements, it should be more clearly distinguished between ethical, legal, societal and political implications of (a) the ROBORDER trials and (b) the future application of a ROBORDER-type platform
(5) In my role of an EAB, I may also contribute to the evaluation of the coming ROBORDER system and platform when it will be exploited and implemented in a real live environments (task b. above)
(6) We (CESS) have been involved in a number of EU projects where we have developed a set of tools for the evaluation of the
    i. efficiency (risk reduction),
    ii. the economic impacts (Cost-Benefit)
    iii. ethical impacts of security "Measures". Those "Measures" to be evaluated could be any kind of advanced technology solutions (as in ROBORDER), organizational and/or organizational measure and others, or a combination of all.
(7) From an ethical, societal view, I would refer you to the so called EELPS[11] methodology and tool. It was developed in a former project ValueSec (http://valuesec-project.atosresearch.eu) and applied in a series of Use Cases in two more recent projects, ECOSSIAN (http://ecossian.eu) and PULSE (http://www.pulse-fp7.com).
(8) It is always a good D&E issue and highly appreciated by the Commission, when projects make use of results of former EU projects, in this case from late FP7/SEC
(9) Depending on the final number of deliverables to be reviewed by me, there may remain some budget left to contribute more substantially on this EELPS evaluation issue to ROBORDER.

[11] Ethical, Economical, Legal, Political, Societal implications

(10) I could imagine creating some input to D6.1 and D6.8, e. g. a separate chapter on EELPS evaluation
(11) This would of course require some closer cooperation with the platform functional architects, the test case designers, and those responsible for the WPs/Tasks related to ethical and societal implications
(12) In a first step, I could offer a scheme of EELPS evaluation criteria and a description of the EELPS evaluation methodology
(13) In the project, we could present a demonstration of the methodology and tool for a selected Use Case or few Cases
(14) The Methodology could also be recommended as voluntary or even as a mandatory step in the future process of implementing the ROPORDER technical system/platform in the real environment. This may become a chapter in the Exploitation report D7.8
(15) According to the EA contract (SoW), we could book this activity as an extended "assessment of project deliverables".
(16) Let us talk about the details later, if you in principle would agree to tis suggestion.

11 Annex IV – Initial Ethics Check Report

Ethics Check Report

Grant Agreement number:	740593
Project Acronym:	ROBORDER
Project title:	Autonomous swarm of heterogeneous RObots for BORDER surveillance
Funding scheme:	H2020-SEC-2016-2017-1
Start and end date:	From 01/05/2017 to 30/04/2020

Date of panel meeting:	26 - 28 June 2019

1. Project scope

ROBORDER aims at developing and demonstrating a fully-functional autonomous border surveillance system with unmanned mobile robots including aerial, water surface, underwater and ground vehicles, capable of functioning both as standalone and in swarms, which will incorporate multimodal sensors as part of an interoperable network.

The system will be equipped with adaptable sensing and robotic technologies that can operate in a wide range of operational and environmental settings. To provide a complete and detailed situational awareness picture that supports highly efficient operations, the network of sensors will include static networked sensors such as border surveillance radars, as well as mobile sensors customised and installed on board unmanned vehicles. A number of supplementary technologies will also be applied that will enable the establishment of robust communication links between the command and control unit and the heterogeneous robots. Moreover, detection

capabilities for early identification of criminal activities and hazardous incidents will be developed. This information will be forwarded to the command and control unit that will enable the integration of large volumes of heterogeneous sensor data and the provision of a quick overview of the situation at a glance to the operators, supporting them in their decisions.

2. Identifying the ethics issues raised by the Project (panel assessment)

Section 1: HUMAN EMBRYOS/FOETUSES		YES/NO/ NOT CLEAR
Does this research involve Human Embryonic Stem Cells (hESCs)?		NO
If YES:	- Will they be directly derived from embryos within this project?	
	- Are they previously established cells lines?	
Does this research involve the use of human embryos?		NO
If YES:	- Will the research lead to their destruction?	
Does this research involve the use of human foetal tissues / cells?		NO
Section 2: HUMANS		YES/NO/ NOT CLEAR
Does this research involve human participants?		YES
If YES:	- Are they volunteers for social or human sciences research?	YES
	- Are they persons unable to give informed consent?	NO
	- Are they vulnerable individuals or groups?	NO
	- Are they children/minors?	NO
	- Are they patients?	NO
	- Are they healthy volunteers for medical studies?	NO
Does this research involve physical interventions on the study participants?		NO
If YES:	- Does it involve invasive techniques?	
	- Does it involve collection of biological samples?	
Section 3: HUMAN CELLS / TISSUES		YES/NO/ NOT CLEAR
Does this research involve human cells or tissues? (*other than from Human Embryos/Foetuses, see section 1)*		NO

If YES:	- Are they available commercially?	
	- Are they obtained within this project?	
	- Are they obtained from another project, laboratory or institution?	
	- Are they obtained from a biobank?	
Section 4: PERSONAL DATA		YES/NO/ NOT CLEAR
Does your research involve processing of personal data?		YES
If YES:	- Does it involve the processing of special categories of personal data (e.g. genetic, health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction.)?	NO
	- Does it involve processing of genetic, biometric or health data?	NO
	- Does it involve profiling, systematic monitoring of individuals or processing of large scale of special categories of data, intrusive methods of data processing (such as, tracking, surveillance, audio and video recording, geo-location tracking etc.) or any other data processing operation that may result in high risk to the rights and freedoms of the research participants?	YES
Does your research involve further processing of previously collected personal data (including use of pre-existing data sets or sources, merging existing data sets)?		YES
Does your research involve publicly available data?		NOT CLEAR
Is it planned to export personal data from the EU to non-EU countries?		NO
Is it planned to import personal data from non-EU countries into the EU?		NO
Section 5: ANIMALS		YES/NO/ NOT CLEAR
Does this research involve animals?		NO
If YES:	- Are they vertebrates?	
	- Are they non-human primates (NHPs)?	
	- Are they genetically modified?	
	- Are they cloned farm animals?	
	- Are they endangered species?	
Section 6: NON-EU COUNTRIES		YES/NO/ NOT CLEAR
If non-EU countries are involved, do the research activities undertaken in these countries raise potential ethics issues? Switzerland		YES

Is it planned to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, etc.)?		NO
Is it planned to import any material from non-EU countries into the EU?		YES
If YES:	Technical data from Switzerland to the EU	
Is it planned to export any material from the EU to non-EU countries?		YES
If YES:	Technical data from the EU to Switzerland	
Does this research involve low and/or lower-middle income countries?[12]		NO
Could the situation in the country(ies) put the individuals taking part in the research at risk?		NO
Section 7: ENVIRONMENT & HEALTH AND SAFETY		YES/NO/ NOT CLEAR
Does this research involve the use of components that may cause harm to the environment, to animals or to plants?		NO
Does this research involve endangered fauna and/or flora/or protected areas?		NO
Does this research involve the use of elements that may cause harm to humans, including research staff?		YES
Section 8: DUAL USE		YES/NO/ NOT CLEAR
Does this research involve dual-use items within the scope of Regulation 428/2009, or other items for which an authorisation is required?		YES
Section 9: EXCLUSIVE FOCUS ON CIVIL APPLICATIONS		YES/NO/ NOT CLEAR
Could this research raise concerns regarding the exclusive focus on civil applications?		NO
Section 10: MISUSE		YES/NO/ NOT CLEAR
Does this research have the potential for misuse of research results?		YES
Section 11: OTHER ETHICS ISSUES		YES/NO/ NOT CLEAR
Are there any other ethics issues that should be considered?		NO

3. Ethics issues

a) Were the ethics issues correctly addressed by the project participants?

[12] If the research involves low and/or lower-middle income countries, respective benefit sharing measures should be planned.

☐ Yes ☒ Partially ☐ No

The Consortium has partly addressed the previous ethics requirements providing, inter alia, details of measures to address risks of dual use and misuse of the project's outcomes. However, several ethics issues still remain.

Humans:

- Copies of ethics approvals for the research with humans (simulations and interviews) are needed before the commencement of the relevant work.
- Further details are needed on informed consent procedures for the project's activities, also with regards to the recruitment of participants who are not directly involved in the project. Such details need to be described in the informed consent form templates and information sheets.
- Further details are needed on the recruitment procedures for the involvement of persons who are not employed within the project.

Personal Data:

- Copies of the opinion or confirmation by the competent Institutional Data Protection Officer and/or authorization or notification by the National Data Protection Authority prior to the entry into force of the GDPR (D9.2 - related to Req. No. 6) have not yet been provided.
- There is some contradictory information with regards to personal data processing within the project. Although the Consortium has stated that no personal data will be collected (GA), the informed consent form templates that have been provided include information regarding participants' consent on the use of their videos and or images (GA). Moreover, several partners declare that they will collect personal data (D9.1 & D9.3). Detailed information on the involvement of personal data in the project needs to be provided.
- It is not clear whether publicly available data will be used in this project and if so, whether it can be freely used for the purposes of the project.
- In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has a lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects is needed.

Other outstanding ethics issues:

- Approvals covering all operations of UxVs are needed before the commencement of the relevant work.
- An explanation as to how the Independent Ethics Advisor's suggestions for addressing the ethics issues that arise from the project have been/will be taken into consideration is needed.
- A report from the internal Ethics Advisory Board, regarding how the ethics issues are dealt with in the project, as well as how the Ethics Advisory Board collaborates with the Independent Ethics Advisor, is needed.
- An evaluation of the ethics implications of the surveillance/profiling technologies produced by this project (including but not limited to misuse). The Independent Ethics Advisor has suggested performing an evaluation of the ethics implications of the project using an assessment methodology described as Ethical, Economic,

Legal, Political and Societal Impact (EELPS) tool which the Consortium may take into account.

---

b) Is there appropriate supervision/monitoring of ethics issues (e.g. via an Ethics Advisor, Ethics Mentor, Ethics Board or the discussion of ethics at management meetings?)

The project has an internal Ethics Advisory Board - EAB and an Independent Ethics Advisor – IEA. The IEA has submitted a well-detailed ethics report (D9.6), with suggestions on how the ethics issues raised by the project can be addressed. Information is needed as to how the Consortium has taken into consideration the IEA's advice. No report from the internal EAB has been made available to this Panel.

---

4. Necessary documents

a) Please indicate below whether the documents necessary to meet the ethics requirements are available to the Panel?

Partially

---

b) List of missing documents:

- Copies of ethics approvals for research with humans.
- Copies of the opinion or confirmation by the competent Institutional Data Protection Officer and/or authorization or notification by the National Data Protection Authority (D9.2 - related to Req. No. 6)
- Approvals for each operation of UxVs

---

5. Assessment of the ethical compliance

a) What are your requirements

The beneficiaries must submit to REA:

1. Copies of ethics approvals for the research with humans (simulations and interviews) before commencement of the relevant work.

2. Full details of the studies with human participants involved in the simulation mock-up, and other related project activities must be submitted. These details must also include clarification on the dates planned for such studies, as well as link to the respective WP/sub task of the project.

3. Further details on the informed consent procedures in relation to all of the activities of the project. Revised templates of the informed consent forms and information sheet to reflect such details must be submitted to the REA.

4. Further details on the recruitment procedures of human participants not employed within the project.

5. Copies of the opinion or confirmation by the competent Institutional Data Protection Officer and/or authorization or notification by the National Data Protection Authority if obtained preGDPR.

6. The host institution must confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO will be made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the General Data Protection Regulation 2016/679, a detailed data protection policy for the project.

7. Clarification as to whether and by which partner, personal data will be processed in the project.

8. An explicit confirmation that the data used in the project is publicly available and can be freely used for the purposes of the project.

9. In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has a lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects.

10. As the research involves intrusive methods of data processing, including surveillance, an explanation as to how the data subjects will be informed of the existence of these intrusive methods of data processing, their possible consequences and how their fundamental rights will be safeguarded.

11. The document Data Protection Rules and an Ethical Code must be submitted.

12. Approvals covering all operations of UxVs, before the commencement of the relevant work.

13. An explanation as to how the Independent Ethics Advisor's advice for addressing the ethics issues that arise from the project, have been/will be taken into consideration.

14. A report from the internal Ethics Advisory Board providing information on how the ethics issues are dealt with in the project, as well as how the Ethics Advisory Board collaborates with the Independent Ethics Advisor.

15. A report from the Independent Ethics Advisor including also information on the project's activities and how the ethics issues they raise are being handled.

16. An evaluation of the ethics implications of the surveillance/profiling technologies produced by this project (including but not limited to misuse).

---

b) Overall assessment

☐ Excellent ☐ Good ☒ Satisfactory ☐ Unsatisfactory

The project has shown some compliance with ethics requirements; however, several ethics issues still remain to be addressed.

---

c) Do you recommend a European Commission further Ethics check?

☒ Yes ☐ No

In view of the number and severity of the ethics issues that remain, a further Ethics Check is recommended.

---

d) Do you recommend a meeting with project representatives during the further check?

☐ Yes ☒ No

---

e) Do you recommend a site visit?

☐ Yes ☒ No

---

f) Do you have other recommendations?

No.

---

12 Annex V – CERTH's DPIA

Data Protection Impact Assessment (DPIA)

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
ROBORDER aims at developing and demonstrating a fully functional border surveillance system with unmanned mobile robots including **aerial, water surface, underwater and ground vehicles**, capable of functioning both as standalone and in swarms, which will incorporate **multimodal sensors** as part of an interoperable network. The system will be equipped with adaptable sensing and **robotic technologies** that can operate in a wide range of operational and environmental settings. To provide a complete and detailed situational awareness picture that supports highly efficient operations, the network of sensors will include static networked sensors such as border surveillance radars, as well as mobile sensors customised and installed on board unmanned vehicles. In order to test the system's capabilities and to check its interoperability, 3 demonstrations and 7 operational tests are going to take place during the project's lifetime, which will involve **humans** for the testing of real-life scenarios. Before commencement of any relevant work involving humans, the necessary signed informed **consent** will be collected. Additionally, in these demos/tests, data (**location**, **imagery**, **videos**) will be collected through the pre-mentioned means which will be processed by the involved partners and will be temporarily stored until the demo's/test's end (location, imagery, videos) or until the project's end (hard copies of signed informed consents). The need for a DPIA arose due to the fact that ROBORDER is a large-scale project that involves the novel application of used technologies and collection of data that could be related to tracking (e.g. the participant's geo-location).

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Collection: Personal data (**name**, **surname**, **professional affiliation**, **phone**, **email address**) will be collected through the collection of the signed informed consent that is going to be asked from the participants before their involvement in the demos/tests that are going to take place during the project's lifetime. In addition, the participants' **geolocation**, **images** and **videos** are going to be collected on the field of the demos/tests.

Use: The data collected from the informed consents aim at providing ROBORDER's Consortium with the **legal basis** in order to proceed with the involvement of the aforementioned humans in their studies (demos/operational tests). These data are only collected due to the reason why the people that are going to be involved in the demos/tests are already directly involved in the project or are already existing contacts of the Consortium, therefore basic personal information is already known to the Consortium. The geolocation, imagery and videos will be used for the purposes of detection of persons, not their identification (i.e. detection of the presence of humans in an image or video). This information will be used in so much as to validate the algorithms employed for the **detection** and is intended to be used by competent authorities (border control practitioners) for the purposes of Search and Rescue and prevention of criminal or illicit activities after project conclusion. ROBORDER will not perform identification of persons through any data collected during the project.

Storage: The signed informed consent will be **safely stored** in the premises of the Pilot Use Case leader partners until the **project's end** (Feb. 2021), in order to be available for demonstration in case of an inspection or an audit. The data collected from the field (imagery, videos, geolocation) will only be temporarily stored in ROBORDER's system (until the **demo's/test's end**) in the case of a real-time, online processing is not applicable, due to the technical partners' equipment capabilities. This will depend on which technical partner/UxV provider is involved in each Pilot Use Case and what are their system's capabilities. Nonetheless, the participants are going to be informed prior to their involvement via the information sheet that is going to be provided to them.

Deletion: Regarding the hard copies of the collected signed informed consents, after the project's end (Feb. 2021) they are going to be destroyed with paper shredders and no digital copies will be kept. The data collected from the field will be immediately deleted from the system as soon as the demo/test is completed. No copies will be kept in additional servers or communication channels.

Sharing: The collected data will be shared only among ROBORDER's Consortium but will be pseudonymized before being shared with the technical partners.

Likely high-risk processing: As the project involves the use of innovative technology (novel use of already existing technologies – unmanned vehicles) and also uses an individual's location in order to detect them in a field, a DPIA could prove of importance.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Nature of data: Basic personal data (name, surname, contact details) and geo-location, imagery and videos collected from the field of the demo/test. Special Category data: N/A Data quantity: Up to this point, there is not a specific limit of data that will be collected during the demos/tests; however, the involved partners will only collect data that are considered absolutely necessary for the improvement of ROBORDER's detection capabilities, in compliance with the "data minimization" principle. Storage: Basic personal data collected from the signed informed consents will be safely stored in the premises of the partner that is responsible for the demo/test until the end of the project. Data collected from the field of the demo/test is going to be temporarily stored only until the demo/test end and only if a real-time, online processing is not supported by the equipment of the involved technical partner/UxV provider. Individuals affected: The only individuals that are going to be affected are the study's participants. They are going to be fully informed about the demo/test before agreeing to participate and they are going to be free to withdraw their participation at any time without any given reason. Geographical areas covered: The only confirmed geographical area that is confirmed to be covered during these demos/tests is the town of Portimao in Portugal. Other countries that are going to be involved are Greece and Hungary (with exact locations to be pending at the moment).

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Relationship with individuals: The humans that are going to be involved in the demos/tests are mostly directly involved in the project, therefore they are familiar with its scope and objectives. Additionally, they might be already existing contacts of members of the Consortium in order to make sure that they are suited to participate in this study and to provide fruitful and valuable feedback. No other participants will be sought after or recruited (e.g. volunteers). Use of their data: Nonetheless, they are still going to be asked to provide the Consortium with a signed informed consent, after they have read and fully comprehended the information sheet also provided to them. The information sheet contains information on what types of data the involved partners will collect and for what reasons they are going to be used. State-of-the-art: Although, UxVs and other relevant technologies are already in use when it comes to border control and surveillance, ROBORDER aims and moving past this state and suggests novel ways of using this exiting technology (the state-of-the-art and the proposed innovations of the project can be found in the Ambition section of the ROBORDER's Grant Agreement – section 1.4). Existing concerns: There are some concerns over border control and surveillance systems as they both raise doubts over the protection of personal life and privacy. Additionally, the use of unmanned vehicles, which will have incorporated sensors and cameras also raises concerns over the pre-mentioned fields. ROBORDER, however, is based on multiple EU regulations that are currently in force and they foresee such kinds of research in these fields in order to mitigate criminal acts taking place at the borders (e.g. Schengen Borders Code - Regulation (EU) 2016/399, Frontex Regulation - Regulation (EU) 2016/1624, EUROSUR Regulation - Regulation (EU) No 1052/2013). Approved code of conduct: N/A at this moment.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
Goals and achievements: The data processing that is going to take place during the project's lifetime aims at developing and demonstrating a fully functional border surveillance system with UxVs that could successfully **detect** the presence of a suspicious object/action/human near the border area. The data that are going to be collected and processed during the demos/tests that are going to be conducted aim at the development and improvement of ROBORDER's detection capabilities. Benefits: Although, there will be no immediate benefits from participating in this research, the outcomes will contribute to enhancing European Union's resilience against criminal activities taking place at the borders, as well as, against environmental disasters. No physical harm or damage is expected to be inflicted on the participants.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
Individuals' views: All partners that are going to be involved in each Pilot Use Case (demos/tests) will be asked to fill in a document in which they should provide the rest of the Consortium and the participants with details about the demo/test (what is going to be the main goal, what data they are going to collect, how they will be used, what will they ask the participant to do etc.). Other involvement: All partners have been encouraged by CERTH (Project's Coordinator) to involve their Data Protection Officers in this process in order to assist them with such issues. CERTH has also sought its DPO's opinion/approval. As the input from all involved partners in the demo is asked from the involved partners (end-users and technical partners) information regarding security and safety will also be provided.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data

minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Lawful basis: signed informed consent from the participants before commencement of any relevant work to encourage fairness and transparency. For the participants that are already directly involved in the project, this step may not take place, as their contracts describe in detail the project's scope and their role in it. However, the signature of the informed consent is advised by the coordinator (CERTH). Purpose limitation: The purposes of the study are explained and listed in the information sheet the participants are going to be provided with before agreeing to participate in the demo/test. Prevention of function creeps: Technical partners involved in the demos/tests, UxV providers and the project's system integrator are going to ensure the all the necessary security measures are already adopted before commencement of any relevant work with humans. Additionally, the data are going to be pseudonymized before being shared with the Consortium in order to protect the participants' privacy. Data quality and data minimization: The data quality is going to be ensured by the participation of people that are directly involved in the project and are familiar with its scope and objectives. In this manner, it is going to be easier to focus on the data that are necessary for the progress of the project; also ensuring data minimization. The involved partners are only going to collect data that will help them improve the system's detection capabilities and will not collect additional data that are out of scope and may also pose a threat to the participant's privacy. Provided information: All the necessary information about the Pilot Use Case (demo/test), what it is going to be asked of the participants, what data will be collected, what are the goals and objectives are going to be listed in the information sheet that is going to be provided to potential participants before their agreement for involvement in these demos/tests. Additionally, they are all provided with the opportunity to ask for any further clarification they think they might need or a translation of the document (clearly stated in the document). Individuals' rights: With the followed procedures the individuals are given the rights of information and data access/edit as they are always entitled to access and edit their data with the help of the data controller. Additionally, they are also given the right to withdraw at any given point of the demo/study with no apparent reason and also the "right to be forgotten". International transfers: No transfer of personal data will be conducted with the Swiss partner of the Consortium - CSEM.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** *Remote, possible or probable*	**Severity of harm** *Minimal, significant or severe*	**Overall risk** *Low, medium or high*

Violation of data privacy	Possible	Significant	Medium
Data Breach	Possible	Significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** *Eliminated, reduced or accepted*	**Residual risk** *Low, medium or high*	**Measure approved** *Yes/no*
Violation of data privacy	pseudonymization of data before sharing	reduced	Medium	yes
	incidental findings policy	reduced	Low	Yes
	deletion of data after the end of the demo/test	reduced	Low	Yes
Data Breach	storage of data in safe servers and locked containers (if needed)	reduced	medium	Yes

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:	The Consortium during the preparation of the Grant Agreement.	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	The Consortium during the preparation of the Grant	If accepting any residual high risk, consult the ICO before going ahead

	Agreement.	
DPO advice provided:	25/2/2020	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: The document has been reviewed for compliance. Processing can proceed. Please fill in the name of the person responsible for keeping the DPIA under review.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Sofia Kyrampalidou & Konstantinos Ioannidis	The DPO should also review ongoing compliance with DPIA