



**An Enhanced Common Information Sharing Environment for Border
Command, Control and Coordination Systems**

Grant Agreement Number: 833881

D.1.5 Legal, Societal, Ethical Initial Report

Deliverable Identifier:	D.1.5
Deliverable Due Date:	2020/05/31
Deliverable Submission Date:	2020/06/02
Deliverable Version:	v.1.0
Author(s) and Organisation:	Tuomas Tammilehto (Laurea)
Work Package:	WP1 Project Coordination & Management
Task:	Task 1.4 Legal, Policy, Societal and Ethical Management
Dissemination Level:	PU: Public



Document Control Page

Deliverable Number:	D.1.5	
Deliverable Title:	Legal, Societal, Ethical Initial Report	
Deliverable Version:	v.1.0	
Work Package Number:	WP1	
Work Package Title:	WP1 Project Coordination & Management	
Submission Date:	2020/06/02	
Dissemination Level:	<input checked="" type="checkbox"/> PU: Public <input type="checkbox"/> CO: Confidential, only for members of the Consortium (including the Commission Services) <input type="checkbox"/> RE: RESTREINT UE (Commission Decision 2015/444/EC)	
Status:	<input checked="" type="checkbox"/> Draft <input checked="" type="checkbox"/> Consortium reviewed <input checked="" type="checkbox"/> Peer reviewed <input checked="" type="checkbox"/> Management Support Team reviewed <input checked="" type="checkbox"/> Project Coordinator accepted	
Author(s):	Tuomas Tammilehto	Laurea
Contributor(s):	Sari Sarlio-Siintola	Laurea
Peer Reviewer(s):	Georgia Melenikou	KEMEA
Security Assessment:	<input checked="" type="checkbox"/> Passed <input type="checkbox"/> Rejected Comments: -	
Funding Authority:	European Commission	
Funding Program:	Horizon 2020 Secure Societies Work Programme 2018 – 2020	
Topic:	SU-BES03-2018 Demonstration of applied solutions to enhance border and external security, Subtopic [2018]: Open	
Rights:	ANDROMEDA Consortium	

Version History

Version	Date	Edited by	Description
v.0.1	2020/05/15	Tuomas Tammilehto (Laurea)	1 st draft
v.0.2	2020/05/28	Tuomas Tammilehto (Laurea)	2 nd draft: annexes, illustrations added etc.
v.0.3	2020/05/29	Tuomas Tammilehto (Laurea)	Ready for review
v.0.4	2020/05/31	Georgia Melenikou (KEMEA)	Minor comments
v.0.5	2020/06/01	Dimitris Myttas (KEMEA)	Review by the SAB
v.0.6	2020/06/01	Alkis Astyakopoulos (KEMEA)	Review approval by the PM
v.1.0	2020/06/02	Athina Foka (MMAIP)	Final version submitted

Executive Summary

The ANDROMEDA project aims to unlock the full potential of CISE, by validating in a long period of time CISE-compatible command, control and coordination systems from several Coast and Border Agencies. At the same time, it is envisaged to further enhance, validate and demonstrate CISE by extending its scope for land borders and adapting relevant C2 solutions and associated services. This will be accomplished by extending the CISE data model based on the use cases and requirements and adapting state-of-the-art command & control systems for full compliance with the enhanced model and CISE message exchange patterns. The project architecture will follow a hybrid scheme in order to allow the usage of the End User CISE Nodes/Gateways and at the same time to allow the testing and validation of the extended data model. The project will leverage on the developments, results and experience of the consortium from current and previous research projects (PERSEUS, CloseEye, MARISA, RANGER), from National Procurement projects of CISE Nodes and Adaptors and on the CISE infrastructure of the End Users.

Disclaimer

The content of the publication herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the ANDROMEDA consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the ANDROMEDA Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the ANDROMEDA Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

©ANDROMEDA Consortium, 2019-2021. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Table of Contents

1.	Introduction	8
1.1	Purpose of the document	8
1.2	Reference documents.....	8
1.3	Definitions	8
1.4	Structure of the document.....	9
1.5	List of Acronyms	9
2.	The Overview of Ethics and Ethics Work in ANDROMEDA	10
3.	Ensuring Research Integrity with Ethical Standards	13
4.	Converting Ethical Requirement into Ethical Features of the ANDROMEDA solution.....	14
4.1	Legal, Ethical and Societal Aspects.....	14
4.2	Implementing Ethical Requirements into Features.....	15
5.	The Trials	17
5.1	Research Integrity and Action Plan	17
5.2	The Validation of the Ethical Features	17
5.3	Ensuring Ethical Use of ANDROMEDA Solution during the trials	17
6.	Conclusions.....	19
7.	Annex A: The Ethical Requirements	20
8.	Annex B: Template for Ethical Self-Assessment	25
9.	Annex C: CNIL Software - Privacy Impact Assessment.....	28
10.	Annex D: Ethics Compliance Check	33
11.	Annex E: The Ethics Paper Trail	36
12.	Annex F: Quality Review Report	38
12.1	Reviewers	38
12.2	Overall Peer Review Result.....	38
12.3	Consolidated Comments of Quality Reviewers.....	38

Table of Figures

Figure 1: Dimensions of Ethics	10
Figure 2: Ethics Governance Model.....	13
Figure 3: The Ethical Layers	15
Figure 4: Ethics Governance Model.....	16
Figure 5: Ethics Governance Model.....	18
Figure 6: Visualisation of the CNIL PIA software.....	32

Table of Tables

Table 1: WP8 Deliverables and their Content 11

1. Introduction

1.1 Purpose of the document

The present document has been generated in the framework of the Program H2020 Project “An Enhanced Common Information Sharing Environment for Border Command, Control and Coordination Systems” (ANDROMEDA hereinafter), on call SU-BES03-2018-2019-2020 ”Demonstration of applied solutions to enhance border and external security”, according to the terms of the Proposal on ANDROMEDA, agreed and adapted in the Grant Agreement (Grant Agreement Number: 833881).

The purpose of the D1.5 Legal, Societal, Ethical Initial Report is to provide initial analysis and assessment of ethical and societal aspects of the ANDROMEDA project as part of the project management WP1 and the task T1.4 Legal, Policy, Social and Ethical Management. It elaborates the basic structure for the T1.4 work and provides templates for the ethical guidance and steering concerning the ANDROMEDA ethical features, the ANDROMEDA research integrity and ANDROMEDA ethics in trials.

1.2 Reference documents

[1] The ANDROMEDA Grant Agreement

[2] European Commission 2019. *How to complete your ethics self-assessment*. Version 6.1. Available online at: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf [Accessed 28.5.2020].

1.3 Definitions

List of Definitions	
Maritime surveillance	It means the set of activities aimed to understand, prevent wherever applicable and manage in a comprehensive way all the events and actions relative to the maritime domain which could impact the areas of maritime safety and security, law enforcement, defence, border control, protection of the maritime environment, fisheries control, trade and economic interest of the EU. Since the aim of ANDROMEDA is to improve maritime security communities’ information exchange, situational awareness, decision making and reaction capabilities with a data fusion toolkit based on various heterogeneous and homogeneous data and information, the focus is correspondingly on that information sharing, collaboration and decision making aided by ANDROMEDA data fusion services. Ethical, legal and societal considerations of the ANDROMEDA solution therefore encompass the ANDROMEDA technology, how the technology will be used in various maritime surveillance activities, as well as the ANDROMEDA governance/business/procurement models either as part of the European Maritime Surveillance ecosystem or independently.
Personal data	It means any information relating to an identified or identifiable natural person (‘data subject’). Information such as name, identification numbers, social security numbers, addresses and such are easy to recognize as personal data (direct identifiers). Important is also the information that relates indirectly to a single person. This kind of information can be location data, IP addresses or online user credentials. Also, the information that describes physical, genetic, psychological, cultural or social attributes that can be linked to single individual is considered personal data. Information can also fall under the category of personal data if it can be easily linked to a single identifiable person or through easily accessible registers.

List of Definitions	
Code as Law	It is the deliberate employment of technology to regulate human behaviour. Used as a term to refer to the idea that technology is an instrument that is or can be used to achieve regulation. Synonyms: Code as Code; Techno-Regulation.
Privacy by Design (PbD)	It is the principle or concept according to which privacy should be promoted as a default setting of every new ICT system and should be built into systems from the design stage. Although often used roughly as a synonym of Privacy Enhancing Technologies (PET), ‘Privacy by Design’ can better be regarded as the <i>idea behind</i> PETs
Privacy-Enhancing Technology (PET)	It is a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system.
BIG DATA	Big Data changes the way data analysis is performed and thought. It includes processes of analysis, capture, research, sharing, storage, visualization and safety of information. Associated with the OSINT, Big Data is being able to map standards of behaviour and tendencies.

1.4 Structure of the document

In the first chapter an introduction to the subject will be provided.

In the following chapters, first an overview of the so-called governance model will be presented together with the tasks related to ethics.

Afterwards, the governance model for ethical and societal issues will be elaborated on three aspects: a) research integrity, b) ethical requirements conversion into ANDROMEDA features, and c) ethics in trials.

1.5 List of Acronyms

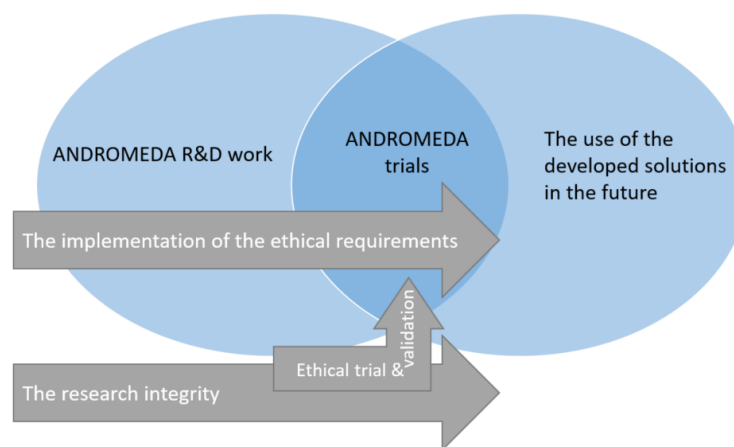
List of Acronyms	
CISE	Common Information Sharing Environment
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
EM	Ethics Manager
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
IPR	Intellectual Property Right
PbB	Privacy by Design
PIA	Privacy Impact Assessment
WBS	Work Breakdown Structure
WP	Work Package
WPL	Work Package Leader

2. The Overview of Ethics and Ethics Work in ANDROMEDA

R&D projects aiming to develop technological solution are often more multidimensional from an ethics point-of-view that they seem at first. There are the ethical requirements for the research and development process *per se*, but also all that ensures that the solution is ethically and socially sustainable. Therefore, ethical issues in this project include both respecting research integrity during the R&D work (see figure 1 below: the research integrity -arrow), as well as defining and implementing ethical requirements as features and/or characteristics of the solution during the R&D work (the implementation of ethical requirements –arrow).

It is only by taking seriously into account these requirements during the R&D work that ethically sustainable solutions can be developed (the rightmost circle in the Figure 1).

Figure 1: Dimensions of Ethics



The ANDROMEDA trials are multifaceted from the viewpoint of ethics since they concern both the research integrity, validation of the ethical features of ANDROMEDA, and finally the use of ANDROMEDA in (close to) real time settings. During the trials (three altogether), a validation process of the solution will be conducted. This validation includes also validation of the ethical issues, i.e. how they are taken into account and whether the solution fulfils the minimum legal requirements defined (e.g. GDPR). This is pictured in the Figure 1 in the overlap of the two circles, *ANDROMEDA R&D work* and *The use of the developed solution in the future*, labelled as *ANDROMEDA trials*, and the turned arrow labelled *Ethical trial & validation*.

To address the ethical issues presented above, the ANDROMEDA consortium has set up dedicated tasks within the project. While ethical and social aspects will be taken into account in implementing each of the project’s work packages and tasks, attention will be especially paid in tasks: *T1.4 Legal, Policy, Social and Ethical Management* (WP1), and *T2.3 Legal and Ethical Context Analysis* (WP2).

Task 2.3 has been already delivered (in month 4) *D2.4: Legal, Ethical and Societal Aspects* and has provided a set of guidelines to the technological partners for ANDROMEDA components implementation. Task 1.4 provides guidance and steering on legal, ethical and societal issues of the proposed solution, as well as guidance, steering and reporting on traditional research ethics in the ANDROMEDA project. They materialise e.g. as *D1.5* (i.e. this deliverable) and *D1.6 Legal, Societal, Ethical Final Report*.

The WP8, entitled as *WP8: Ethics requirements*, needs also to be mentioned here, since it is a whole WP dedicated to specifically ensure that the ethical issues are taken into account.

The deliverables of WP8 are presented in the table below:

Table 1: WP8 Deliverables and their Content

Deliverable	Content
D8.1 H - Requirement No. 1 (M6)	The informed consent procedures for the participation of humans, together with the related templates and information sheets
D8.2 H - Requirement No. 2 (M6)	Details on incidental findings policy
D8.3 H - Requirement No. 3 (M6)	Copies of opinions/approvals by ethics committees and/or competent authorities for the research with humans
D8.4 POPD - Requirement No. 4 (M6)	A report containing explanation for the beneficiary about how the data subjects are informed in cases of profiling of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded
D8.5 POPD - Requirement No. 5 (M6)	Detailed information on the informed consent procedures with regard to data processing, together with the templates of the informed consent forms and information sheets with regard to data processing (in language and terms intelligible to the participants)
D8.6 POPD - Requirement No. 6 (M6)	Description of the anonymisation/pseudonymisation techniques that will be implemented
D8.7 POPD - Requirement No.7 (M6)	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 to safeguard the rights of the data subjects
D8.8 POPD - Requirement No. 8 (M4)	Confirmation of appointed Data Protection Officer (DPO) and the contact details of the DPO made available to all data subjects involved in the research or detailed data protection policy for the project
D8.9 POPD - Requirement No. 9 (M4)	A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants
D8.10 POPD - Requirement No. 10 (M6)	In case personal data are transferred from the EU to a non-EU country or international organisation, confirmation that such transfers are in accordance with Chapter V of the General Data Protection Regulation 2016/679. Also, in case personal data are transferred from a non-EU country to the EU (or another third state), confirmation that such transfers comply with the laws of the country in which the data was collected must
D8.11 EPQ - Requirement No. 11 (M9)	Appropriate health and safety procedures conforming to relevant local/national guidelines/legislation are followed for staff involved in this project.
D8.12 DU - Requirement No. 12 (M12)	The Regulation 428/2009 on dual-use requires export licenses and relevant authorisations compliant, thus those need to be obtained prior to using/transferring this technology
D8.13 M - Requirement No. 13 (M9)	Risk assessment and details on measures to prevent misuse of research findings

The detailed information is available on the above-mentioned deliverables of WP8, thus they are not thoroughly dealt in this report. For example, the methodology and results, together with the necessary templates and information sheets can all be found in those deliverables. All except D8.12 (due M12) either

have been submitted to ECAS or are to be submitted by M9 (May 2020). The deliverables can also be found in ANDROMEDA's SharePoint, so that the consortium members have access to them.

In general, the methodology followed a similar pattern: the principal authors of the deliverables formulated questions to be asked from the consortium member organisations, requested the information, described the background and analysis, i.e. wrote the meaning of the information. Then, the deliverables were peer reviewed by members of the WP8. Thus, in a way, these were collaborative works that could not have been done alone.

The Ethics Manager of the ANDROMEDA is Mr. Tuomas Tammilehto (M.Soc.Sci and MA Crim.). He has an extensive expertise for the ethics work at LAUREA within the several H2020 projects including MARISA and RANGER projects. The Ethics Manager will:

- monitor the ethical concerns in the project;
- ensure that the project will comply with the Research Ethics taking all relevant international ethical aspects into consideration, prior to the execution of the operational trials;
- translate and implement the ethical requirements to the various deliverables in the project;
- provide advice on assessments on ethics in the ethical progress reports as part of the yearly project progress report;
- facilitate collaboration with all the project actors.

3. Ensuring Research Integrity with Ethical Standards

Every ANDROMEDA project partners are committed into upholding ethical research standards, including the European Code of Conduct for research integrity. They are also committed to deliver high quality scientific outputs and to be transparent in order to enable to ensure the reliability and impact of the research. (See e.g. Grant Agreement – ARTICLE 34). These are validated as part of the quality management procedures.

In order to follow the principles of maximizing benefit and minimizing harm, social responsibility, dignity of persons, fundamental human rights and other such issues mentioned, for example, in the H2020 ethical self-assessment, in ANDROMEDA R&D work, an ethical self-assessment procedure is introduced in to the ANDROMEDA governance structure.

The emphasis is on the ethical R&D process, and it includes the use of consent forms for the participants taking part in project, for example in interviews, trials etc. The process is as follows:

1. Ethics Manager (EM) provides templates for the ethical self-assessment and ethical compliance check (see Annexes B and D).
2. Each WP leader provides ethical self-assessment of her/his WP and delivers it to EM (please note that the EU-RESTRICTED and the ethics deliverables are excluded of the self-assessment).
3. If problems occur, they are to be discussed with EM and the Executive Board.
4. EM will update the documents in the ANDROMEDA SharePoint, record the activities in the ethics paper trail (see Annex E), and report it as part of the ethical progress report (i.e. this deliverable and the D1.6).

The aforementioned process is illustrated in the Figure 2 here below:

Follow: 2 ⇒ 6 ⇒ 7 ⇒ 8 ⇒ 9 ⇒ 12 ⇒ 13.

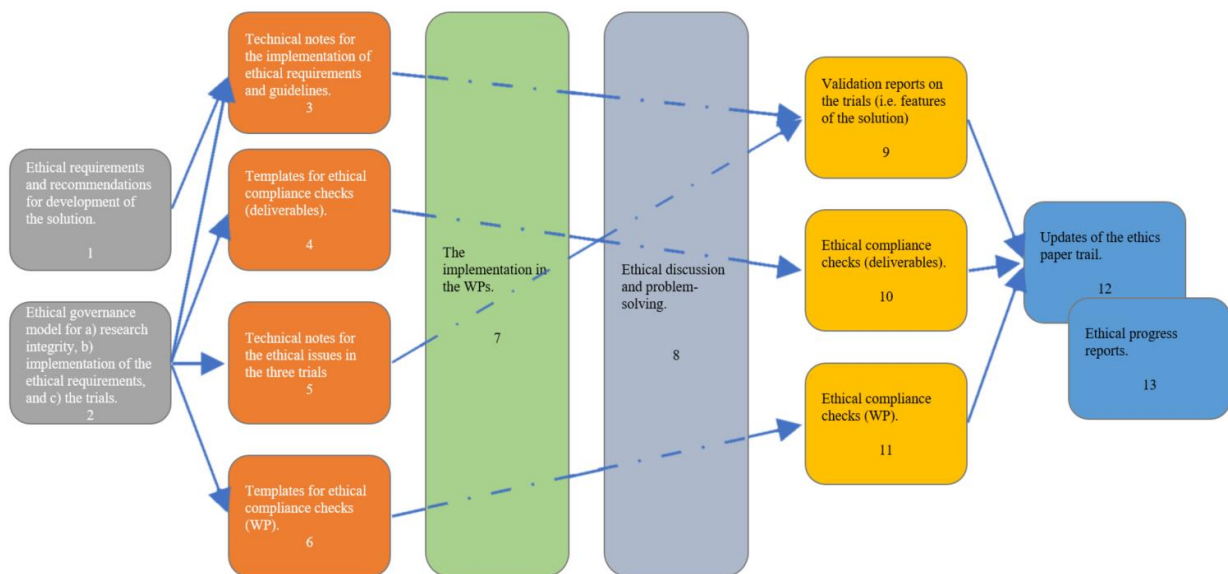


Figure 2: Ethics Governance Model

4. Converting Ethical Requirement into Ethical Features of the ANDROMEDA solution

4.1 Legal, Ethical and Societal Aspects

The purpose of the deliverable *D2.4: Legal, Ethical and Societal Aspects* submitted on M4 was to help ANDROMEDA developers, end users, and business/adoption modelers take into consideration legal, ethical and societal dimensions of the proposed ANDROMEDA solution.

When the aim of ANDROMEDA is to unlock the full capabilities of the CISE Model by enhancing it and by extending its scope to the Land Surveillance Information Exchange. This allows maritime and land security authorities to have the same information exchange system for improved information exchange, situational awareness, decision making and reaction capabilities.

Ethical, Legal and Societal aspects of the ANDROMEDA solution are, however, not limited to information Exchange. The moral aspects relating to how surveillance is performed, the various data sources, as well as services are key issues to be discussed as part of both the ANDROMEDA technology, organisational arrangements, and business models. By integrating ethics into the solution from the beginning we are seeking not only to prevent and minimize any ethical risks, but also to maximize the benefits of the solution to society.

The ethical analysis of the CISE-compliance of the MARISA project was extended to land border control environment and the ANDROMEDA solution. The use of ANDROMEDA solution utilizing both Maritime Surveillance data and Land Border surveillance data has new ethical implications both to Maritime Surveillance and Land Border environments. The extension of current CISE model scope to the Land Surveillance Information Exchange brings new ethical challenges, e.g. the use of UAVs and legacy systems providing information and focusing the surveillance also on the level of single persons instead of putting focus only on the phenomena level of anomalies.

Based on the activities described above, the ethical requirements for the ANDROMEDA have been defined. Some of the ethical requirements defined in the D2.4 are either too detailed to be converted into specific Ethical Features. Further, many of them stay on a very general level because they are interconnected with the evolving end-user requirements, technical solutions and business modelling.

The ethical requirements in D2.4 are categorised (also in this deliverable as Annex A) as *General Requirements for ANDROMEDA Development and Ethical Awareness (EG)*, *Specific Requirements for ANDROMEDA Technology Development & its User Manuals (ET)*, *Specific Requirements for User Processes and Training Material (EP)*, and *Adoption/Governance/Business Models (EB)*. Among the EG requirements there are requirements which may concern both ET, EP, and EB requirements, based on the way it was seen reasonable to implement in ANDROMEDA.

The different ethical layers are illustrated in Figure 3.

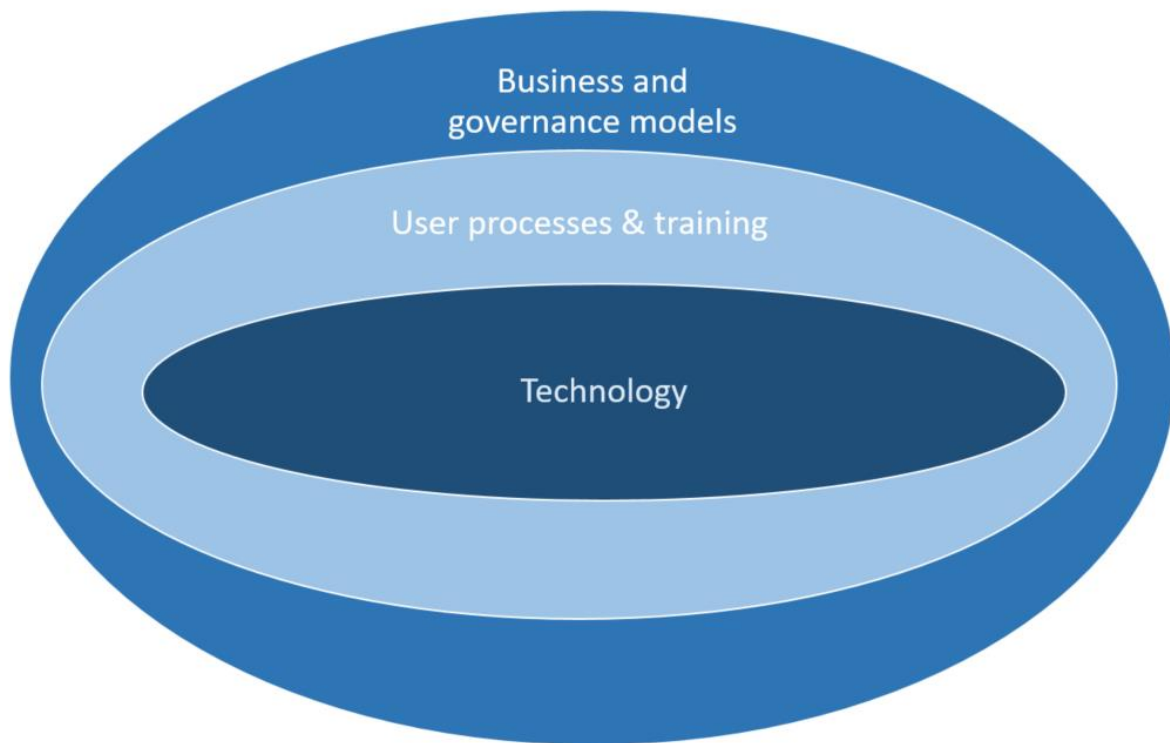


Figure 3: The Ethical Layers

4.2 Implementing Ethical Requirements into Features

Ethical awareness is of course pertinent, but in order to guarantee that the ethical requirements presented in D2.4 are also mutually understood, prioritised, and successfully implemented, specific activities are needed. Thus, the following action is planned:

First, the WP and task leaders will get familiar with the requirements by going through the Ethical Requirements presented in D2.4, i.e.

- *General Requirements for ANDROMEDA Development and Ethical Awareness (EG),*
- *Specific Requirements for ANDROMEDA Technology Development & its User Manuals (ET),*
- *Specific Requirements for User Processes and Training Material (EP), and*
- *Adoption/Governance/Business Models (EB).*

Second, it is vital to understand that there can be differences between the implementation of the requirements for the trials and with the final ANDROMEDA solution. If and when any clarification is required, it is the Ethics Managers work to provide assistance for the translation and implementation of the ethical requirements, to ensure that all can be taken into account. In practice, this is carried out by providing needed documents and specifications and/or organising teleconferences and other collaboration activities on request.

Third, the Ethics Manager shall provide a template for ethical compliance check for deliverables (the EU-RESTRICTED deliverables as well as the WP8 deliverables on ethics are excluded¹). The task leaders and/or

¹ See, the Andromeda Grant Agreement, part B, p. 156.

the principal authors of the deliverables are expected to conduct an ethical compliance check on their deliverables. If clarification is needed, the Ethics Manager shall provide assistance.

The ethical compliance checks are further reported in the ethics paper trail and ethical progress reports by the Ethics Manager.

See the process in Figure 4 here below (same as Figure 2).

Follow: 1 ⇒ 2 ⇒ 3 ⇒ 4 ⇒ 7 ⇒ 8 ⇒ 10 ⇒ 12 ⇒ 13

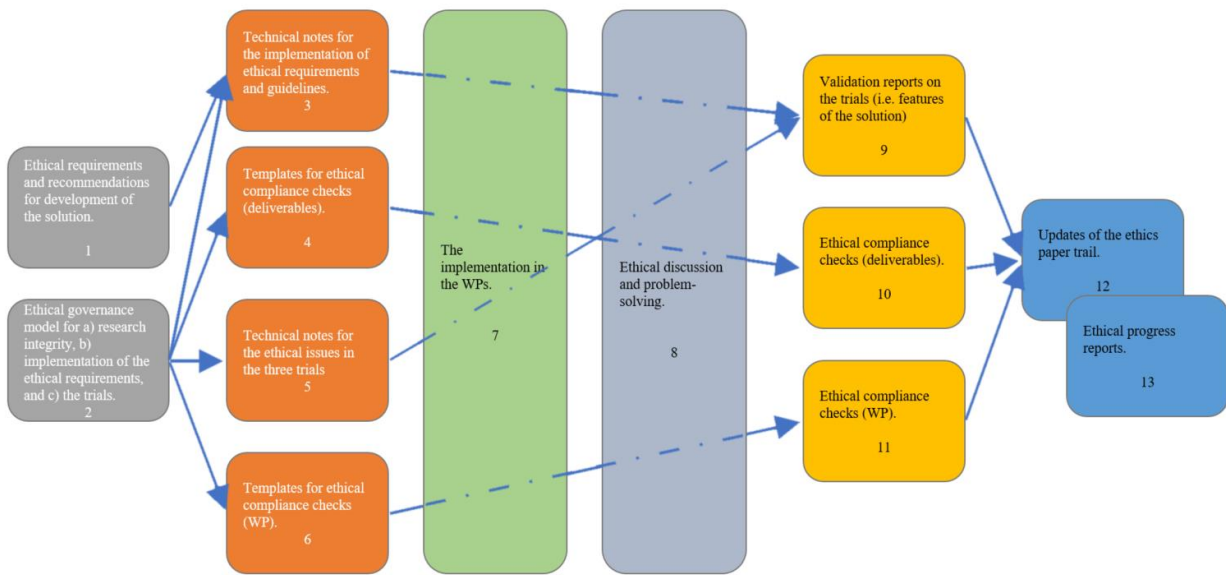


Figure 4: Ethics Governance Model

5. The Trials

The ANDROMEDA trials (three altogether) are very important from an ethics point-of-view. First, the research integrity must be secured, second the ethical features should be validated, and third, the solution itself has to fulfil the required ethical requirements.

Therefore, the following subsections describe the necessary processes to cover these issues.

5.1 Research Integrity and Action Plan

The process is explained in Chapter 3 of this deliverable.

5.2 The Validation of the Ethical Features

The ethical features will be validated as part of the general validation process of the three trials. This includes the technology, user processes, and business model. The Ethics Manager will supervise the creation of the technical notes for the validation. The notes are filled with the partners and others participating to the trials. Then, the analysis of feedback concerning ethics is to be performed by the Ethics Manager and linked to the general validation process.

5.3 Ensuring Ethical Use of ANDROMEDA Solution during the trials

The minimum ethical requirements to be met by the trial version of ANDROMEDA itself concern the legislation, namely data protection (GDPR), IPRs, and data information sharing regulation.

The minimum legal requirements concerning data protection during the trials can be defined after the data sources to be used are defined (in WP6), and when the privacy impact assessment of the trials (WP1 and WP6) and data protection risk analysis (WP1) are completed. The GDPR compliance will be checked using the CNIL PIA software, for more details, see Annex C.

1. Final decision how the data protection will be performed during the trials is to be decided by the Executive Board. The Ethics Manager will introduce the alternatives for the decision makers.
2. Other legal regulations will be figured out while the system integration for each trial (WP6) is on progress. This will be done by the Ethics Manager with the collaboration of local end-users of the trial. Technical notes will be provided for the work by the Ethics Manager.

See the process in Figure 5, here below.

Follow: 1 ⇒ 2 ⇒ (4) ⇒ 5 ⇒ 7 ⇒ 8 ⇒ (9) ⇒ 11 ⇒ 12 ⇒ 13

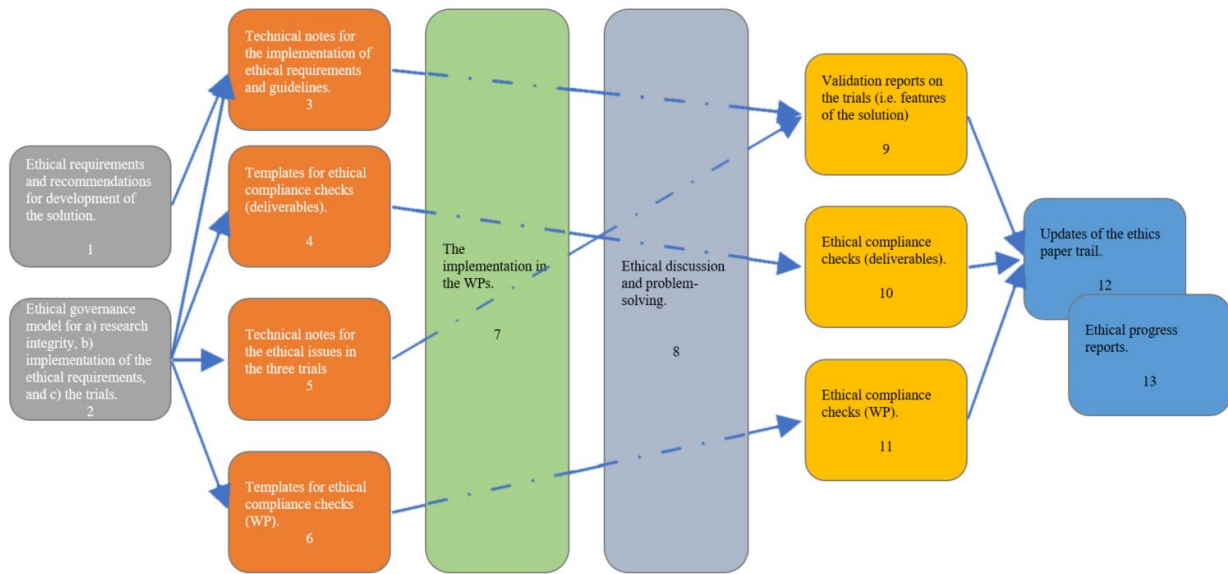


Figure 5: Ethics Governance Model

6. Conclusions

This initial report, D1.5, describes the guidelines and principles according to which the ANDROMEDA project's ethics work is done (and the work too). Together with the WP8 deliverables and D2.4 they are the tangible part of ethics work, that will be materialised also as features in the ANDROMEDA solution and related research findings.

It is very important that the research and other activities is done ethically correctly since it is a guarantee of quality. However, ethics is pivotal for another reason too. Only ethically sustainable and societally acceptable solutions can enter successfully to the market. Thus, ethics is imperative for long term market success.

Further, it is needless to say, that when doing anything based on public resources, there is an obligation to respect both the payers i.e. European taxpayers and the EC as the funder, and ethically solid work is one way to show appreciation and gratitude.

We believe that with these tools and by implementing the processes we have followed ANDROMEDA can be a success story from an ethics point of view.

7. Annex A: The Ethical Requirements

GENERAL REQUIREMENTS FOR ANDROMEDA DEVELOPMENT AND ETHICAL AWARENESS²	TYPE
EG1: Take ethics and societal challenges seriously; concerning both technology, user processes, and business/governance model, including information management.	<i>Essential Awareness</i>
EG2: Be aware of the requirements defined in the data protection reform – the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). This includes both general issues, new rights of persons, responsibilities for controllers and processors, as well as transfers of data to third countries.	<i>Essential Awareness</i>
EG3: The GDPR requires effective and clear governance model. This should be created for both the development phase and the final ANDROMEDA solution, and be integrated into the ANDROMEDA business/adoption model(s). A Data Protection Officer shall be nominated.	<i>Essential Activity and Governance/Business Model Feature</i>
EG4: Define the flows of personal in the ANDROMEDA solution both for the pilot versions and for the final version. Logical routes are the key – the physical infrastructure is important only from the information security point of view. The view should contain a description of how the data is processed along the way, who uses it, and why. After that a risk analysis and a DPIA are to be conducted to determine which level of liability is acceptable for data protection infringements (e.g. for processing sensitive data)	<i>Essential Activity and Adoption/governance Business Model Feature</i>
EG5: Consider that the GDPR applies already during the pilot. Communicate openly about data protection issues, challenges and needs already during the pilot. One alternative is to use fake data. If using real-life data is necessary, the reasons for this must be elaborated. Any personal data should be anonymised or irreversibly pseudonymised as soon as it is recognised as personal data. If this cannot be done (e.g. with photographs and indirectly identifying personal characteristics), the data should be stored only for as long as strictly necessary for testing the prototype. Avoid the processing such photos and videos due to the sensitive nature of such data.	<i>Essential Awareness and Activity</i>
EG6: Create a data/ information management plan where the following are discussed: 1) Social media strategies, policies and accounts 2) Relationship with the existing public security services 3) Internal collaboration and information sharing 4) The anchoring of data processing in legislation. This concerns both pilot versions and the final version of ANDROMEDA and its future use	<i>Essential Activity and Essential Adoption / Governance Model Feature</i>
EG7: Follow up on the legal framework for information sharing, management and data protection, as well as local restrictions related to the use of drones already during the ANDROMEDA project and after it.	<i>Essential Activity and Governance Model Feature</i>
EG8: Adopt common data management processes, taxonomies, and ontologies to enable efficient sharing of knowledge. This includes the implementation of European best	<i>Essential Activity</i>

² The requirements are based on the work done in MARISA-project, however, they are modified to serve better the ANDROMEDA context. In addition, this table includes some requirements that were not present in MARISA. Further, this list is not complete, since the full list of the data sources to be used in ANDROMEDA was not completed by the time this deliverable was due to submit. Thus, there will be additions and clarifications to these requirements during the lifecycle of the project.

practices for data management across all law enforcement and security services. >(availability, confidentiality and integrity)	
EG9: Be aware of national differences in copyright exemptions and the application of implicit licenses. Activities can best take place in countries with a copyright and database-right regime that is favourable for the project. Conduct a risk analysis to determine the acceptable level of liability for IPR infringements considering uncertainties about e.g. implicit licenses and the applicable law with respect to statutory exceptions. Integrate the perceived data protection risks into project risk management procedures. (for the pilots and afterwards)	<i>Important Activity and Essential in Exploitation.</i>
EG10: Harmonization of the legislation in data sharing and collaboration is needed. Lobby/influence also political organizations on data protection issues and other legislation that is essential for ANDROMEDA as well as on data availability across countries. (>As part of the User Community work in WP2 there is already an intention to promote EU-level collaboration in EU-legislation for legal frameworks of data exchange.)	<i>Important Activity</i>
EG11: Specify different actors' responsibilities and the moral division of labour to avoid free riding. This can include e.g. a bigger role for Frontex in situations where responsibilities and/or the scales of input are not in balance. (>duty to render assistance issues)	<i>Desirable Activity</i>
EG12: Include SAR people in the user community: their needs are as important for ANDROMEDA as everyone else's.	<i>Essential Activity</i>
EG13: Recognize third countries in the sea as both end-users of ANDROMEDA, and as partners in solving shared problems with the help of new technology.	<i>Important Activity and Essential Exploitation</i>
EG14: Make a clear division between the roles and responsibilities of the platform and software developers, content providers, end users and decision makers, as well as even ordinary people whose data may be used in the processes. (during the project and after)	<i>Important Activity and essential Business Model Feature</i>
EG15: Prioritise the development of software to avoid and solve data-related challenges (including data protection issues). Be mindful of the difference between software and hardware.	<i>Important Activity</i>
EG16: Practice transparency about ANDROMEDA on its publicly accessible website, including information about the need, purpose, proportionality, and subsidiarity of the project, and about the actions to apply privacy/security by design.	<i>Essential Activity</i>
EG17: Utilizing open standards and open source software as far as suitable is encouraged, as obtaining patents or patent licences may hinder an efficient development. (National license that can be deployed locally by the national authorities? The use of permissive SW licenses?)	<i>Important Feature</i>
EG18: Update current societal/surveillance impact assessment (SIA) to secure that ANDROMEDA is compliant with ethics and legislation.	<i>Essential Activity and</i>

	<i>Governance/Business model Feature</i>
EG19: Develop end-user specific Codes of Conducts where the ethical principles for the use of ANDROMEDA are defined (includes the pilots).	Essential Activity and Business/Adoption Model Feature
EG20: Perform an explicit legal Duty of Care before utilizing any Big Data or Artificial Intelligence (AI) (pilot version + future versions of ANDROMEDA). This requirement is overlapping with requirements found in the GDPR concerning personal data but concerns also other data. (Ensure that the data is up to date & legitimately obtained, that the algorithms meet the scientific criteria & are transparent). This can be partly linked to the duties of the Data Protection Officer. Provide also an oversight for transparency and juridical review concerning big data.	Desirable Activity and Essential Business Model Feature
EG21: The opportunity to practice and test large scale system, in a multi-agency and international setting, is a unique chance to assess and understand how the technology affects and drives the operators and decision-makers' behaviours.	Essential Activity during the trials and after
SPECIFIC REQUIREMENTS FOR ANDROMEDA TECHNOLOGY DEVELOPMENT & ITS USER MANUALS	
ET1: Apply Privacy/Security by Design (PbD) by restricting the end users' access to personal data as much as possible without compromising the intended purpose of enhancing public security. Put extra effort in the development and deployment of privacy enhancing technologies (>data minimization, storage limitation, anonymization/ pseudonymisation, access control services, information security). When applicable, deploy even additional technical solutions to cope with the data protection legislation and other requirements. e.g. the right of the data subjects in case such information will be stored on ANDROMEDA platform.	Essential Technical feature
ET2: Provide transparency and proper functionalities to help estimate the quality, reliability and validity of various data to be used. Code this information for the end-user to help her in the decision making.	Essential Technical feature
ET3: Transparency is mandatory for both the ANDROMEDA system and the processing of data, as it serves the interests of accountability. > GDPR & LED	Essential Technical Feature
ET4: Automated decision making on the actions to be performed is not allowed. The existing ban on automated decision-making should be strictly enforced, and government agencies should be more alert with semi-automated also.	Essential Technical Feature
ET5: Different frameworks for ethics (including data protection) are to be deployed depending on the activities at hand (e.g. terrorism detection and border control, fisheries control, oil spills, SAR etc.).	Essential Technical Feature
ET6: Modularity of the ANDROMEDA solution, as well as the possibility to customization and parallelization, are essential because of the differing operational needs in the user communities and because of the variations in legislation in different countries.	Important Technical Feature
ET7: To avoid both false positive and false negative results, the triangulation of data, and the transparency of data fusion and the data used in it are essential. In addition, the use of dark web is important.	Essential Technical Feature

ET8: Logs are to be used as part of the system (required in both GDPR and LED). The purpose is to avoid human information leakage and other human misuse of the system. In addition, any information put into the system and shared through it should be traceable, so that sources and their reliability can be verified when necessary.	<i>Essential Technical Feature</i>
ET9: Specific security standards are to be followed up to the EU restricted level.	<i>Essential Technical Feature</i>
ET10: A vast array of analytic techniques to identify and resolve biases, (e.g. assumption surfacing, red teaming, post-mortem analysis, etc) is encouraged.	<i>Interesting Technical Feature</i>
ET11: The quality of data is to be investigated both automatically and manually when first transferring it as well as in each use case.	<i>Essential Technical and User Process Feature</i>
ET12: Trustworthy Artificial Intelligence requires that algorithms are secure, reliable as well as robust enough to deal with errors or inconsistencies. The design of the solutions addresses the four pillar of resilience: <ul style="list-style-type: none"> • Learning from past events • Respond to regular and irregular events • Monitor the developments and assess the risks • Anticipate the future states (risk and opportunities) The conceptual model fo the system must, therefore, depict these core capabilities, recalling that the system comprises the technological components and human operators.	<i>Essential Technical Feature</i>
ET13: From the viewpoint of good governance it is recommendable that users can store/print various situational pictures and data fusions results which have been essential from the viewpoint of their decision making	<i>Interesting Technical Feature</i>
SPECIFIC REQUIREMENTS FOR USER PROCESSES AND TRAINING MATERIAL	
EP1: The quality of data is to be investigated both automatically and manually when first transferring it as well as in each use case.	<i>Essential User Process and Technical Feature</i>
EP2: Operational decisions shall never be made by a computer, not even the most efficient one: it must always be a human who makes the final decisions. ANDROMEDA can only assist in operational decision making, by providing information to the end-user/decision makers. The end-users must be informed regarding these liability issues in the training material. As we provide new decision support systems, must also acknowledge the need to revise the role of the human operator.	<i>Essential User Process Feature</i>
EP3: Adopt the check and balance approach to avoid data leakages and mis-use of it.	<i>Essential User Process Feature</i>
EP4: Proper user training on ethical decision making is needed because of 1) ethics and legislation are case/country dependent even in our pilot countries (e.g. use of the drones	<i>Essential User Process Feature</i>

<p>& privacy) 2) OSINT and the dual roles of the users are ethically challenging. 3) the inherent biases in cognitive processing are relevant to recognize</p>	
<p>EP5: Increasing training/course programs on data security are essentials, including the following aspects: Generalised access to private cloud computing accounts requires close monitor. The indiscriminate use of USB storage devices can be a potential source of security breaches. The mobile devices are a potential source of data theft and a mean of recording unauthorised and sensitive information.</p>	<p><i>Essential User Process Feature</i></p>
<p>ADOPTION/GOVERNANCE/BUSINESS MODELS (in the future)</p>	
<p>EB1: The continuous development of the ANDROMEDA services together with the end-users and stakeholders shall be embedded in the business model from the beginning to ensure that ANDROMEDA is up to date regarding ethical and legal requirements also in the future.</p>	<p><i>Essential Governance/Business Model Feature</i></p>
<p>EB2: Ethical (economic, social, environmental) sustainability is a part of the ANDROMEDA value proposition. Therefore, the continuous monitoring of legal & ethical frameworks and societal impacts as well as the use of sunset provisions is included the business/adoption model of ANDROMEDA.</p>	<p><i>Essential Governance/Business Model Feature</i></p>
<p>EB3: Considering Service Logic (SD) in designing alternative business models for ANDROMEDA and its various component is highly recommended, as it supports the holistic approach to ANDROMEDA where not only technology, but also services are included. Furthermore, it lowers the investment costs for users.</p>	<p><i>Important Business Model Feature</i></p>
<p>EB4: If ANDROMEDA technologies are used for purposes other than maritime surveillance and security, a special guidelines book including ethical restrictions of use must be provided. Furthermore, the consortium partners must, together with the EU, ensure that adequate control and licensing is in place for any system or its component developed before it can be sold or exported.</p>	<p><i>Essential Business Model Feature</i></p>
<p>EB5: Market research, which is an essential part of the business model, must be conducted early on to enable the successful adaptation of ANDROMEDA in each local context. This includes conducting a Societal Impact Assessment (SIA) as well as an evaluation of the legal and ethical frameworks for ANDROMEDA in each operating environment.</p>	<p><i>Essential Business Model Feature</i></p>
<p>EB6: Organizational activities concerning Data Protection must be applied as part of the governance model for each new implementation of ADROMEDA. Conducting a light PIA before the implementation is essential.</p>	<p><i>Essential Adoption Model Activity</i></p>
<p>EB7: It is essential for ethical compliance that the following activities are performed in each ANDROMEDA environment:</p> <ul style="list-style-type: none"> - Defining a Social Media Strategy - Defining an explicit legal Duty of Care, including external reviews - Audits of Big Data and AI components 	<p><i>Essential Adoption/Business Model Feature</i></p>
<p>EB8: Ethics management and training concerning the use of ANDROMEDA in decision making must always be included in the business model. (training during each new implementation)</p>	<p><i>Essential Business Model Feature</i></p>

8. Annex B: Template for Ethical Self-Assessment

Ethical Self-Evaluation Form for Single R&D Activities and Technology in the ANDROMEDA Project

This evaluation form is based on the ethics self-assessment of Horizon 2020 projects.³

Ethics self-assessment should be completed for all research/development tasks.

Work package leaders should make sure that it will be done.

Work package	
Research/development project name	
Form completed by (name & partner)	
Date	

1. HUMAN EMBRYOS/FOETUSES	
Does your research involve Human Embryonic Stem Cells (HESCs)?	No___ Yes ___
If yes, please specify. (And wait for further instructions from the ethics committee before starting the R&D work).	
2. HUMANS	
Does your research involve Human Participants?	No___ Yes ___
Activities to be taken (if yes): The researchers should provide Informed consent forms with an information sheet specifying the nature of the research. Furthermore, a normal approval from the University Research Ethics Committee or from the relevant Member State authority for non-academic institutions should be mandatory if the human participants come from outside the project consortium organisations.	
3. HUMAN CELLS / TISSUES	
Does your research involve human cells or tissues (other than from Human Embryos/ Foetuses, i.e. section 1)?	No___ Yes ___
If yes, please specify. (And wait for further instructions from the ethics committee before starting the R&D work).	
4. PERSONAL DATA	
Does your research involve personal data collection and/or processing?	No___ Yes ___
Does it involve tracking or observation of participants?	No___ Yes ___
Does your research involve further processing of previously collected personal data (secondary use)?	No___ Yes ___
Activities to be taken (if yes): 1. Informed consent forms collected from the participants are the general prerequisite for this data processing. (See D8.1)	

³ https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

<p>2. The researchers should provide the details of the procedures regarding the collection, storage, protection, retention, transfer and destruction or re-use of the data, as well as those regarding data safety procedures, data transfers to third countries and tracking and observing methods. (See D8.5, D8.7 and D8.10)</p>	
<p>5. ANIMALS</p>	
<p>Does your research involve animals?</p>	<p>No___ Yes ___</p>
<p>Activities to be taken (if yes): The researchers should obtain the necessary authorisations and provide a detailed analysis of the procedures, justifications and legal compliance.</p>	
<p>6. THIRD COUNTRIES</p>	
<p>Does your research involve non-EU countries?</p>	<p>No___ Yes ___</p>
<p>Do you plan to import any material from non-EU countries into the EU?</p>	<p>No___ Yes ___</p>
<p>Do you plan to export any material from the EU to non-EU countries?</p>	<p>No___ Yes ___</p>
<p>Activities to be taken (if yes): The researchers should provide a risk-benefit analysis, the details of the activities and compliance checks with the EU and local legislations. (See D8.10)</p>	
<p>7. ENVIRONMENT & HEALTH and SAFETY</p>	
<p>Does your research involve the use of elements that may cause harm to the environment, to animals or plants?</p>	<p>No___ Yes ___</p>
<p>Does your research involve the use of elements that may cause harm to humans, including research staff?</p>	<p>No___ Yes ___</p>
<p>Activities to be taken (if yes): The researchers should obtain the necessary environmental authorizations and provide a risk-benefit analysis and compliance checks regarding legislation. and/or The researchers should obtain the necessary health and safety authorizations and provide the details of safety procedures and legal compliance.</p>	
<p>8. DUAL USE</p>	
<p>Does your research have the potential for military applications?</p>	<p>No___ Yes ___</p>
<p>Activities to be taken (if yes): The researchers should provide an explanation on the exclusive civilian focus of the research, a justification of military technologies, the details of the needed export licenses, explanation on how the research might affect current standards in military ethics, and measures to apply to avoid negative implications on military ethics standards.</p>	
<p>9. MISUSE</p>	

Does your research have the potential for malevolent/criminal/terrorist abuse?	No___ Yes ___
<p>Activities to be taken (if yes):</p> <p>The researchers should provide a risk assessment and impact on human rights, the details on the applicable legal requirements and the measures to be taken to prevent abuse.</p>	
10. OTHER ETHICS ISSUES	
Are there any other ethics issues that should be taken into consideration?	No___ Yes ___
<p>Activities to be taken (if yes):</p> <p>If yes, please specify. (And wait for further instructions from the ethics committee before starting the R&D work).</p>	

9. Annex C: CNIL Software - Privacy Impact Assessment

Privacy Impact Assessment (PIA) may be defined as a *systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme and finding ways to mitigate or avoid any adverse effects*.

PIA has been in use for over 50 years worldwide even though not widely developed in the EU context. Currently, both General Data Protection Regulation (GDPR) and the previous Data Protection Directive (DPD) present conducting DPIA (Data Protection Impact Assessment) as obligatory in certain circumstances of personal data processing. PIA and DPIA are not exactly the same process. The first one is more concerned on privacy issues overall while the latter focuses on protecting the personal data. The latter might still be broader since it includes all processing of personal data whether or not such processes would cause any effects on data subjects' privacy. However, the DPIA process still needs to have sufficient analysis on privacy risks and personal data processing due to regulation's accountability principle. Therefore, PIA is a recognised and commonly used tool to begin the DPIA, including the data protection methods.

This Annex presents a simple tool to conduct a PIA. The open source PIA software is created by the National Commission on Informatics and Liberty of France (Commission nationale de l'informatique et des libertés – CNIL). CNIL is an independent French administrative regulatory body whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data, and it is also the national data protection authority for France.

The PIA software aims to help data controllers build and demonstrate compliance to the GDPR and facilitates carrying out a data protection impact assessment. The tool is available in French and in English for free.

The process to carry out the D/PIA is to enter the necessary descriptions of various elements of PIA into the software in a predefined order.

The CNIL's PIA tool has been designed around three principles:

- A didactic interface to carry out PIAs: the tool relies on a user-friendly interface to allow for a simple management of your PIAs. It clearly unfolds the privacy impact assessment methodology step by step. Several visualisation tools offer ways to quickly understand the risks.
- A legal and technical knowledge base: the tool includes the legal points ensuring the lawfulness of processing and the rights of the data subjects. It also has a contextual knowledge base, available along all the steps of the PIA, adapting the contents displayed. The data are extracted from the GDPR, the PIA guides and the Security Guide from the CNIL, to the aspect of the processing studied.
- A modular tool: designed to help you build your compliance, you can customise the tool contents to your specific needs or business sector, for example by creating a PIA model that you can duplicate and use for a set of similar processing operations. Published under a free licence, it is possible to modify the source code of the tool in order to add features or include it into tools used in your organisation.

The CNIL PIA tool consists of Sections, parts in which specific questions are to be answered. They are presented here below:

ANDROMEDA CNIL-PIA

Author's name

Tammilehto, Tuomas

Assessor's name

tba

Validator's name

tba

Creation date

xx/xx/202x

CONTEXT

(This section gives a clear view of the treatment(s) of personal data in question)

Overview

(This part allows to identify and present the ANDROMEDA solution)

Q: Which is the processing under consideration?

Q: What are the responsibilities linked to the processing?

Q: Are there standards applicable to the processing?

Data, processes and supporting assets

(This part allows to define and describe the scope of the processing in detail)

Q: What are the data processed?

- Set out a detailed list of the data processed, by category, and persons with access thereto.

Q: How does the life cycle of data and processes work?

- Present a detailed description of the processes carried out.

Q: What are the data supporting assets?

- List the data supporting assets for the entire life cycle.

FUNDAMENTAL PRINCIPLES

(This section allows to build the compliance framework for privacy principles)

Proportionality and necessity

(This part allows to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights)

Q: Are the processing purposes specified, explicit and legitimate?

- Set out in detail the data processing purposes and justify their legitimacy.

Q: What are the legal basis making the processing lawful?

- Describe the legal basis for the lawfulness of the processing.

Q: Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

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

Q: Are the data accurate and kept up to date?

- Set out in detail the data quality compliance controls, carried out on the device, the mobile app and the personal account, as well as a justification on the arrangements for or impossibility of implementing them.

Q: What are the storage duration of the data?

- Set out in detail, for each data type (common data, archived data, functional traces, technical logs): the storage durations, the justification of the storage durations, the purge mechanisms at the end of the storage.

Controls to protect the personal rights of data subjects

(This part allows you to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights)

Q: How are the data subjects informed on the processing?

- Describe the controls intended to provide information to users alongside the justification of the arrangements for, or the impossibility of, or the exemption from implementing them on the device, mobile app and personal account.

Q: If applicable, how is the consent of data subjects obtained?

- Where the lawfulness of the processing is based on consent, describe the controls intended to ensure that users' consent has been obtained, that there has been a reminder and confirmation of their consent, and the settings associated with the latter have been maintained, alongside the justification of the arrangements for, or the impossibility of, implementing them on the device, mobile app and personal account. The consent is obtained via a written form.

Q: How can data subjects exercise their rights of access and to data portability?

- Describe the controls intended to ensure users' right of access to all personal data concerning them, alongside the justification of the arrangements for, or the impossibility of, or the exemption from implementing them on the device, mobile app and personal account.

Q: How can data subjects exercise their rights to rectification and erasure?

- Describe the controls intended to ensure the right to rectification or erasure of data of users who request this, alongside the justification of the arrangements for, or the impossibility of, or the exemption from implementing them on the device, mobile app and personal account.

Q: How can data subjects exercise their rights to restriction and to object?

- Describe the controls intended to ensure the right to object and to restriction either concerning the different purposes or the whole of a processing operation, alongside the justification of the arrangements for, or the impossibility of, or the exemption from implementing them on the device, mobile app and personal account.

Q: Are the obligations of the processors clearly identified and governed by a contract?

- A processing contract must be signed with each processor, setting out all of the aspects stipulated in Art. 28 of the GDPR (duration, scope, purpose, documented processing instructions, prior authorization where a processor is engaged, provision of any documentation providing evidence of compliance with the GDPR, prompt notification of any data breach, etc.).

Q: In the case of data transfer outside the European Union, are the data adequately protected?

- Set out in detail the geographic storage location of the device, mobile app and personal account data in the cloud, alongside justification of the choice of remote hosting and indication of the legal supervision arrangements implemented in order to ensure adequate protection of the data:

Country: France /European Union /Country recognized as providing adequate protection by the EU /Other country

Justification and supervision in case of a cross-border transfer: standard contractual clauses /internal corporate regulations

RISKS

(This section allows to assess the privacy risks, taking into account existing or planned controls)

Planned or existing measures

(This section allows to identify controls [existing or planned] that contribute to data security)

Q: Illegitimate access to data

- What could be the main impacts on the data subjects if the risk were to occur?
- What are the main threats that could lead to the risk?
- What are the risk sources?
- Which of the identified planned controls contribute to addressing the risk?
- How do you estimate the risk severity, especially according to potential impacts and planned controls?
- How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Q: Unwanted modification of data

- What could be the main impacts on the data subjects if the risk were to occur?
- What are the main threats that could lead to the risk?
- What are the risk sources?
- Which of the identified controls contribute to addressing the risk?
- How do you estimate the risk severity, especially according to potential impacts and planned controls?
- How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Q: Data disappearance

- What could be the main impacts on the data subjects if the risk were to occur?
- What are the main threats that could lead to the risk?
- What are the risk sources?

Q: Risk overview

- Which of the identified controls contribute to addressing the risk?
- How do you estimate the risk severity, especially according to potential impacts and planned controls?
- How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

VALIDATION

Risk mapping

Action plan

DPO and data subjects' opinions

A visualisation of the tool is presented here below. On the left side (circled with blue colour) is the table of contents showing the sections that are to be addressed. In the middle (circled with red colour) is the main part in which the information is typed in. It gives guidance in the form of questions and also gives examples what to consider when answering. However, there is a third functionality (a menu) on the right hand side (circled with green colour), so-called *Knowledge base*, which contains more information and guidance, for example principles according which PIA runs, together with legal and other relevant definitions. These can be opened by clicking with the mouse.

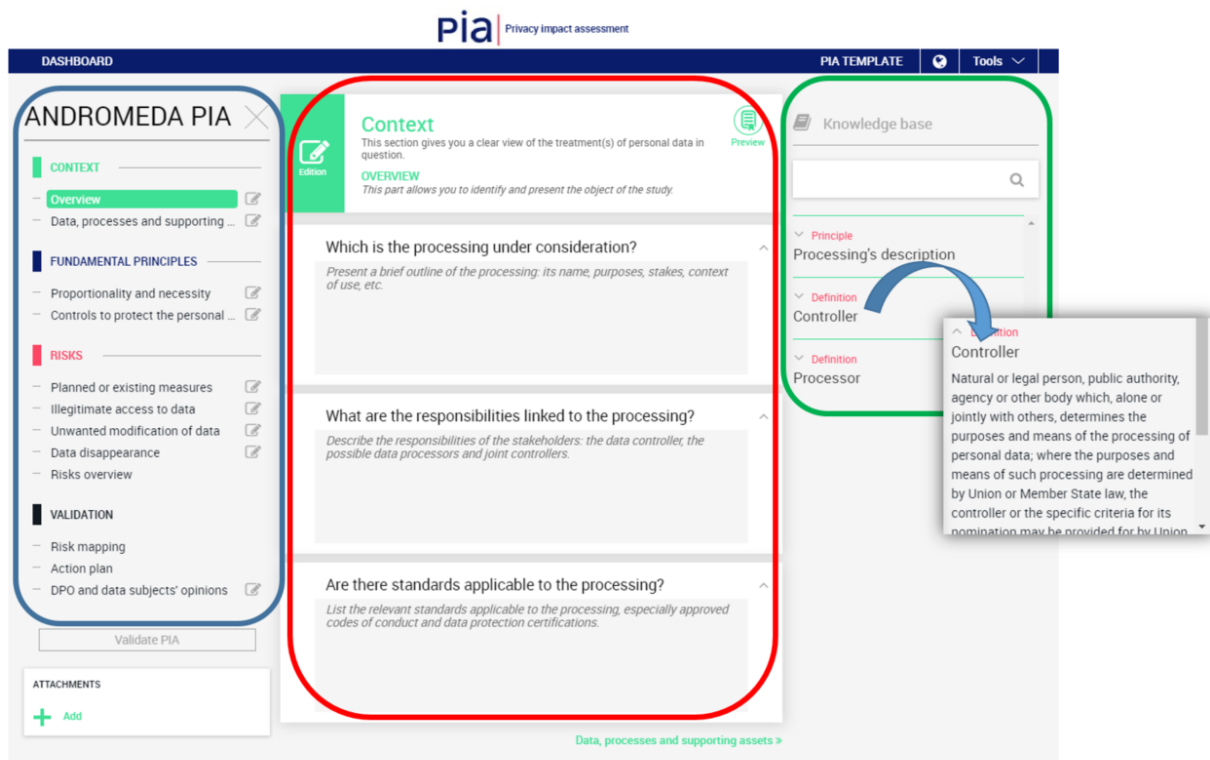


Figure 6: Visualisation of the CNIL PIA software

The filling up of this CNIL’s PIA software will be a collaborative work together with the partners responsible of the trials, the Technical Manager and the Ethics Manager.

The software enables to ensure the correct way to handle data (in compliance with GDPR), as well as identify and mitigate risks. PIA is a very important part of ensuring the ethicalness of ANDROMEDA and is recommended to be done in D2.4.

10. Annex D: Ethics Compliance Check

In this table there are summarized the ethical and societal guidelines for the ANDROMEDA solution. The table is originally defined in the *D2.4 Legal, Ethical and Societal Aspects*.

With the help of this table, an ethical compliance check will be done for each ANDROMEDA deliverable. These are to be completed by the WP leaders and/or principle authors of the deliverables and returned to the Ethics Manager for ethics supervising purposes.

The first column sets the question that can be answered by ticking No, Yes or n/a (not applicable) in the second column. In case that the answer is affirmative or negative, additional information is needed.

1. Can this deliverable/WP be justified on ethical grounds, i.e. does it respect fundamental rights and other applicable legislations, regulations and values?	No___ Yes ___ n/a___
Please specify (unless not applicable).	
2. Can the information that ANDROMEDA collects, based on this WP's/deliverable's research activities, be used for discrimination or other unethical purposes?	No___ Yes ___ n/a___
Please specify (unless not applicable).	
3. Since, any use of technology in third states' coastal waters should be carried out in the framework of explicit cooperation agreements with these states as well as in conformity with international law and regulations, third countries in the Mediterranean and land borders shall be seen as ANDROMEDA end users and as true partners in solving shared problems with new technology. Thus, based on this WP's/deliverable's research activities, are any third countries been involved?	No___ Yes ___ n/a___
Please specify (unless not applicable).	
4. ANDROMEDA is likely to result in changes in the daily work routines of different end-user groups (e.g. coast guards and SAR teams). Thus, it is important that end user communities are involved in the development. Therefore, have any end users being involved in this WP's/deliverable's research activities?	No___ Yes ___ n/a___
Please specify (unless not applicable).	

<p>5. Both the data and the system shall be transparent when developing ANDROMEDA. Moreover, AI systems and their decisions shall be explained in a manner adapted to the stakeholder concerned. Humans must be aware that they are interacting with an AI system, and shall be informed of the system's capabilities and limitations. Have these been taken into account in the research activities of this WP/deliverable?</p>	<p>No ___ Yes ___ n/a ___</p>
<p>Please specify (unless not applicable).</p>	
<p>6. Any decisions on Maritime and Land Border Surveillance and SAR must always be made by the competent human decision makers - computer systems can only have an assisting role in operational decision making. Based on the research activities of this WP/deliverable, is this the case?</p>	<p>No ___ Yes ___ n/a ___</p>
<p>Please specify (unless not applicable).</p>	
<p>7. The principles relating to processing of personal data, such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality as well as data controller's accountability must be embedded in the ANDROMEDA technology. Based on the research activities of this WP/deliverable, is this the case?</p>	<p>No ___ Yes ___ n/a ___</p>
<p>Please specify (unless not applicable).</p>	
<p>8. Are a) Social media strategies, policies and accounts, b) Relationship with the existing public security services, c) Internal collaboration and information sharing, and/or c) the anchoring of data processing in legislation relevant in this WP/deliverable?</p>	<p>No ___ Yes ___ n/a ___</p>
<p>Please specify (unless not applicable).</p>	
<p>9. AI systems must be resilient, secure accurate, reliable and reproducible. A fall-back plan must be in place to ensure safety in</p>	<p>No ___ Yes ___ n/a ___</p>

<p>case something goes wrong. Also, mechanisms to ensure responsibility and accountability for ANDROMEDA AI systems and their outcomes must be established. Auditability, which enables the assessment of algorithms, data, and design processes, plays a key role therein, especially in critical applications. Are these relevant in this WP/deliverable, and are they taken into account?</p>	
<p>Please specify (unless not applicable).</p>	
<p>10. ANDROMEDA is not used to identify individuals but phenomena. However, individuals could be identified, nevertheless. Thus, have the respective privacy and data protection rights and freedoms of people been addressed?</p>	<p>No___ Yes ___ n/a___</p>
<p>Please specify (unless not applicable).</p>	
<p>11. ANDROMEDA will use during the pilot demonstrations tools and technologies (e.g. radar, drone) that could potentially pose health and safety risks to the involved participants. Have the risks and the mitigation actions been properly addressed?</p>	<p>No___ Yes___ n/a___</p>
<p>Please specify (unless not applicable).</p>	

11. Annex E: The Ethics Paper Trail

This paper trail is to be filled in and kept up to date by Ethics Manager.

#	Activity	Document	Date	Actor	Data Storage	Comments
1	Presentation on ethical issues in KoM, Athens, Greece	PP-slides	Sep 17–18, 2019	EM All	ANDROMEDA SharePoint	
2	Presentation on ethical issues at the End Users meeting + Technical meeting, Rome, Italy	PP-slides	Nov 05–06, 2019	EM, All	ANDROMEDA SharePoint	Together with KEMEA
3	Investigation of ethical, legal and societal aspects.	D2.4 Legal, Ethical and Societal Aspects	Dec 30, 2019	EM, PC, All	ECAS, ANDROMEDA SharePoint	
4	Confirmation of appointed Data Protection Officer (DPO) and the contact details of the DPO made available to all data subjects involved in the research or detailed data protection policy for the project	D8.8 POPD - Requirement No. 8	Dec 30, 2019	KEMEA, EM, LAUREA, MMAIP	ECAS, ANDROMEDA SharePoint	
5	A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants	D8.9 POPD - Requirement No. 9	Jan 2, 2020	EM, PC, LAUREA, KEMEA, All	ECAS, ANDROMEDA SharePoint	
6	Presentation on ethical issues at the 2nd Project Meeting (Plenary, Technical, Innovation, Advisory), Alfeite, Almada, Portugal	PP-slides	February 11–12, 2020	EM All	ANDROMEDA SharePoint	Together with KEMEA
7	The informed consent procedures for the participation of humans, together with the related templates and information sheets	D8.1 H - Requirement No. 1	Feb 28, 2020	KEMEA PC EM	ECAS, ANDROMEDA SharePoint	
8	Details on incidental findings policy	D8.2 H - Requirement No. 2	Feb 28, 2020	KEMEA, PC, EM, SAB, MMAIP	ECAS, ANDROMEDA SharePoint	
9	A report containing explanation for the beneficiary about how the data subjects are informed in cases of profiling of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded	D8.4 POPD - Requirement No. 4	March 5, 2020	EM, PC, All	ECAS, ANDROMEDA SharePoint	

#	Activity	Document	Date	Actor	Data Storage	Comments
10	Detailed information on the informed consent procedures with regard to data processing, together with the templates of the informed consent forms and information sheets with regard to data processing (in language and terms intelligible to the participants)	D8.5 POPD - Requirement No. 5	March 6, 2020	EM, PC, KEMEA, MMAIP	ECAS, ANDROMEDA SharePoint	
11	In case personal data are transferred from the EU to a non-EU country or international organisation, confirmation that such transfers are in accordance with Chapter V of the General Data Protection Regulation 2016/679. Also, in case personal data are transferred from a non-EU country to the EU (or another third state), confirmation that such transfers comply with the laws of the country in which the data was collected must	D8.10 POPD - Requirement No. 10	March 23, 2020	EM, PC, LAUREA, KEMEA, All	ECAS, ANDROMEDA SharePoint	
12	Description of the anonymisation/ pseudonymisation techniques that will be implemented	D8.6 POPD - Requirement No. 6	March 23, 2020	EM, PC, LAUREA, KEMEA, SAB, MST, MMAIP, All	ECAS, ANDROMEDA SharePoint	
13	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 to safeguard the rights of the data subjects	D8.7 POPD - Requirement No.7	March 23, 2020	EM, PC, LAUREA, KEMEA, SAB, MST, MMAIP, All	ECAS, ANDROMEDA SharePoint	
14	Copies of opinions/approvals by ethics committees and/or competent authorities for the research with humans	D8.3 H - Requirement No. 3	March 26, 2020	KEMEA, PC, EM, All	ECAS, ANDROMEDA SharePoint	
15	3 rd Project Meeting (remotely)	PP-slides	May 13-14, 2020	EM, PC, LAUREA, KEMEA	ANDROMEDA SharePoint	Together with KEMEA

12. Annex F: Quality Review Report

The ANDROMEDA Consortium uses the Quality Review Report process for its internal quality assurance for deliverables to assure consistency and high standard for documented project results.

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

12.1 Reviewers

Project Coordinator	Athina Foka (MMAIP)
Management Support Team Member	Alkis Astyakopoulos (KEMEA)
Internal Peer Reviewer	Georgia Melenikou (KEMEA)

12.2 Overall Peer Review Result

The Deliverable is:

- Fully accepted
 Accepted with minor corrections, as suggested by the reviewers
 Rejected unless major corrections are applied, as suggested by the reviewers

12.3 Consolidated Comments of Quality Reviewers

General Comments	
Deliverable contents thoroughness	Reviewers comment: Yes. Just one addition is proposed in Annex D ‘Ethics Compliance Check’ with respect to the health and safety requirements (risks and mitigation actions). Author’s reply: Added question No. 11.
Innovation level	Reviewers comment: n/a Author’s reply:
Correspondence to project and programme objectives	Reviewers comment: Yes, it corresponds to the need of constant ethical monitoring of the ANDROMEDA research activities. Author’s reply:
Specific Comments	
Relevance with the objectives of the deliverable	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partially <input type="checkbox"/> Not applicable Reviewers comment: Author’s reply:
Completeness of the document according to the its objectives	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partially <input type="checkbox"/> Not applicable

	Reviewers comment: Author's reply:	
Methodological framework soundness	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partially <input type="checkbox"/> Not applicable Reviewers comment: Author's reply:	
Quality of the results achieved	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partially <input type="checkbox"/> Not applicable Reviewers comment: Author's reply:	
Structure of the deliverable with clear objectives, methodology, implementation, results and conclusions	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partially <input type="checkbox"/> Not applicable Reviewers comment: Author's reply:	
Clarity and quality of presentation, language and format	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partially <input type="checkbox"/> Not applicable Reviewers comment: Author's reply:	
Detailed Comments (please add rows as appropriate)		
No.	Reference	Remark
1		
2		
3		
4		
5		