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

Grant Agreement Number: 833881

D.2.4 Legal, Ethical and Societal Aspects

Deliverable Identifier:	D.2.4
Deliverable Due Date:	2019/12/31
Deliverable Submission Date:	2019/12/30
Deliverable Version:	v.2.5
Author(s) and Organisation:	Sari Sarlio-Siintola and Tuomas Tammilehto (LAUREA)
Work Package:	WP2 Operational Analysis, User Requirements and Technical Specifications
Task:	Task 2.3 Legal and Ethical Context Analysis
Dissemination Level:	PU: Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833881.

Document Control Page

Deliverable Number:	D.2.4	
Deliverable Title:	Legal, Ethical and Societal Aspects	
Deliverable Version:	v.2.5	
Work Package Number:	WP2	
Work Package Title:	Operational Analysis, User Requirements and Technical Specifications	
Submission Date:	2019/12/30	
Dissemination Level:	☒ PU: Public ☐ CO: Confidential, only for members of the Consortium (including the Commission Services) ☐ RE: RESTREINT UE (Commission Decision 2015/444/EC)	
Status:	☒ Draft ☒ Consortium reviewed ☒ Peer reviewed ☒ Management Support Team reviewed ☒ Project Coordinator accepted	
Author(s):	Sari Sarlio-Siintola	LAUREA
	Saara Siintola	LAUREA
	Karoliina Nikula	LAUREA
	Jyri Rajamäki	LAUREA
	Tuomas Tammilehto	LAUREA
Contributor(s):	Alkis Astyakopoulos	KEMEA
	Vasiliki Zomenou	KEMEA
	Zdravko Paladin	MSD
	Vítor Fernando Plácido da Conceição	Defesa
Peer Reviewer(s):	Giovanni Barone	ENG
	Georgia Melenikou	KEMEA
Security Assessment:	☒ Passed ☐ 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	2019/09/15	Sari Sarlio-Siintola	Table of Content
v.0.2	2019/10/14	"	Chapters 3,5,6 first drafts
v.0.3	2019/10/29	"	First SIA + Code of Conduct for comments
v.0.4	2019/11/20	"	First full version for T2.3 team
v.0.5	2019/12/05	Sari Sarlio-Siintola Tuomas Tammilehto	Editing for peer-review
v.0.6	2019/12/05	Saara Siintola	Editing for peer-review
v.1.0	2019/12/06	Tuomas Tammilehto	Final editing, Executive summary and Conclusion
v.2.0	2019/12/18	Tuomas Tammilehto	Making minor changes according to comments from consortium
v.2.1	2019/12/19	Tuomas Tammilehto	Changing illustration to newer
v.2.2	2019/12/22	Tuomas Tammilehto	Upadating table of contents
v.2.3	2019/12/23	Tuomas Tammilehto	Taking into account the feedback of the reviewers, e.g. a chapter on smuggling is added.
v.2.4	2019/12/23	SAB	Review by the SAB
v.2.4	2019/12/23	MMAIP, KEMEA	Internal approval review by the PM
v.2.5	2019/12/27	MMAIP	Final version submitted

Executive Summary

This deliverable is an important part of ANDROMEDA work. It outlines the legal, ethical and societal aspects related to the research and project work of ANDROMEDA, but more so, to the solutions, and to the future use of solutions (incl. practices and new governance and business models) developed and researched during the project. This document sets the specific ethical requirements that must be taken into account when designing and realising the ANDROMEDA solutions, as well as when using those solutions.

This document first justifies itself, i.e. the necessity of legalities and ethics, then briefly introduce the project (and links to related projects) before introducing the norms in the ANDROMEDA domain, i.e. maritime and border security. Then after, concerns of privacy, data protections and OSINT[1] and AI are dealt, before introducing the ethical challenges in maritime and land border security. This is followed by the results of the Societal Impact Assessment (SIA) carried out in the beginning of the project. Then the focus is turned to perhaps the most pivotal section of this document: the ethical requirements. There are 21 general ethical requirements, 13 requirements specifically for the technology, five for user processes and training material, and eight for adaptation and business/governance models. However, this list lives during the projects as more detailed information, for example, on the data sources, sensors and legacy systems is collected and analysed. Ethics never ends, nor does technical advancement, so there might be changes or adjusts in the presented requirements, too. Maybe, above is also the justification for the last part of this document: the initial Code of Conduct of ANDROMEDA. These are the nine ethical and moral principles according which ANDROMEDA, both the project and the results, is done.

Disclaimer

Copyright message

[1] Although, the use of OSINT is not anticipated during the ANDROMEDA trials, OSINT is embedded in current CISE implementation, for example in MARISA project, thus we are touching this here too.

Table of Contents

Table of Figures

Table of Tables

1. Introduction

1.1 Purpose of the Document

The purpose of this deliverable is to help ANDROMEDA developers, end users, and business/adoption modelers take into consideration legal, ethical and societal dimensions of the proposed ANDROMEDA solution.

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 contents of this deliverable are partly overlapping with the analysis of Ethical, Legal and Societal Aspects of the MARISA project in the deliverable D.2.13 The ethical analysis of the CISE- compliancy of MARISA is 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 bring new ethical challenges, e.g. the use of UAV 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.

This deliverable has been created in the early beginning of the ANDROMEDA project in M4. Therefore, the above outputs (SIA, Ethical requirements, Code of Conduct) will be developed further during the ANDROMEDA project and reported as part of ANDROMEDA ethical progress reports. In addition, as part of the User Community work in WP2 there is an intention to promote EU-level collaboration in EU-legislation for legal frameworks of data exchange.

1.2 Reference Documents

Project Reports

ANDROMEDA GA (2019).

PARIS PROJECT (2015). Available from: https://paris.projexct.org/. (Accessed November 2018).

Political Papers and Legislation

AI ETHICS (2019). Ethics Guidelines for Trustworthy AI. High Level Expert Group on Artificial Intelligence. EU Commission 04/2019.

CFR (2010). European Charter of Fundamental Rights. Official Journal of the European Communities.

CISE (2013). The Development of CISE of the Surveillance of the EU Maritime Domain and their related impact assessment. European Commission DG Mare. Draft Interim Report. Cowi.

COM (2014). European Commission: Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain. 451 final.

ECHR (2010). European Convention on Human Rights. Council of Europe. Retrieved from: http://www.echr.coe.int/Documents/Convention_ENG.pdf.

EU (2007). Treaty of Lisbon amending the treaty on European Union and the Treaty establishing the European Community.

EU (2019) Regulation of the European Parliament and of the Council on the European Border and Coast Guard and repealing Regulations (EU) No1052/2013 and (EU)2016/1624.

EU (399/2016). Regulation No. 399/2016 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)

EU (656/2014). Regulation No 656/2014 of the Parliament and of the Council of 15 May 2014 establishing rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union.

European Group on Ethics in science and new technologies (2014). Ethics of Security and surveillance Technologies. Opinion 28. European Commission, Brussels.

GDPR (2016). Regulation 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).

IMO (2005). Role of the Human Element—Assessment of the impact and effectiveness of implementation of the ISM Code, International Maritime Organization, MSC 81/17.

LED (2016). Directive 2016/680 of the European Parliament and of the Council of 24 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 of the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

SAR Convention (1979). International Convention on Maritime Search and Rescue. Available from: https://treaties.un.org/doc/Publication/UNTS/Volume%201405/volume-1405-I-23489-English.pdf. (Accessed 22. April 2019).

SOLAS (1974). The 1974 International Convention for the Safety of Life at Sea. Available from: https://treaties.un.org/doc/Publication/UNTS/Volume%201184/volume-1184-I-18961-English.pdf. (Accessed 20. April 2019).

TEU (2009). Consolidated Version of The Treaty on European Union. Available from: http://data.europa.eu/eli/treaty/teu_2012/oj. (Accessed 17. May 2019).

TFEU (2009). Consolidated Version of the Treaty on the Functioning of the European Union. Available from: http://data.europa.eu/eli/treaty/tfeu_2012/oj. (Accessed 17. May 2019).

UN (1951). Refugee Convention 1951. Available from: https://www.unhcr.org/4ca34be29.pdf. (Accessed 25. April 2019).

UNCLOS (1994). 1982/1994 United Nations Convention on the Law of the Sea. Available from: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf. (Accessed 26. April 2019).

Articles, Reports, and Books

Amsterlaw, Jennifer & Zikmund-Fisher, Brian & Fagerlin, Angela & Ubel, Peter. (2006). Can avoidance of complications lead to biased healthcare decisions? Judgment and Decision Making. 1. 64-75.

Andersson (2015). Why border controls are now a global game. Available from http://blogs.lse.ac.uk/internationaldevelopment/2015/06/29/why-border-controls-are-now-a-global-game. (Accessed 5/12/2019).

Coles,J, S. Faily & D. Ki-Aries (2018). 'Tool-Supporting Data Protection Impact Assessments with CAIRIS,' 2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE), pp. 21-27, 2018.

Crepeau (2013). Report of the Special Rapporteur on the human rights of migrants, François Crépeau - Regional study: management of the external borders of the European Union and its impact on the human rights of migrants, UN Human Rights Council 24 April 2013, A/HRC/23/46.

Denes-Raj V & Epstein S (1994). Conflict between intuitive and rational processing: when people behave against their better judgement. Journal of Personality and Social Psychology.

Edelman, G. & Tononi, G. (2001). Consciousness. How Matter Becomes Imagination.

European Union Agency for Fundamental Rights (FRA) (2013). Fundamental rights at Europe's southern sea borders. Luxembourg: Publications Office of the European Union.

Fischer-Lescano Andreas, Tillmann Löhr & Timo Tohidipur (2009). Border Controls at Sea: Requirements under International Human Rights and Refugee Law. Oxford University Press. Available from: http://ijrl.oxfordjournals.org/content/21/2/256.abstract.

Gilovich, T. Griffin, D. Kahneman, D. (edit.) (2002). Heuristics and Biases – The Psychology of Intuitive Judgement. Cambridge University Press. New York.

Hayes, Ben, & Vermeulen, Mathias (2012*). Borderline: EU Border Surveillance Initiatives - An Assessment of the Costs and Its Impact on Fundamental Rights*. Berlin: Heinrich-Böll-Stiftung.

Helkama, K., Uutela, A., Pohjanheimo, E., Saliminen, S., Koponen, A. and Rantanen, V.R. (2003). Moral reasoning and values in medical school: a longitudinal study in Finland. Scandinavian Journal of Educational Research, 47:4, 399–411.

Human Rights Watch (HWR) (2009). Pushed Back, Pushed Around. Italy's Forced Return of Boat Migrants and Asylum Seekers, Libya's Mistreatment of Migrants and Asylum Seekers. Online. Available at: https://www.hrw.org/report/2009/09/21/pushed-back-pushed-around/italys-forced-return-boat-migrants-and-asylum-seekers Accessed: 5/12/2019.

Järvenpää, S. L. & Majchrzak, A. (2008). Knowledge collaboration among professionals protecting national security: Role of transactive memories in ego-centered knowledge networks. Organization Science. Vol 19 (2).

Jeandesboz J. (2011). Beyond the Tartar steppe: EUROSUR and the ethics of European border control practices. In Burgess J and Gutwiths S. (eds.) Migration and Integration. Institute for European Studies Series.

Kahneman, D. & Frederick, S. (2002). Representativeness Revised: Attribute Substitution in Intuitive Judgement. In: Gilovich, T. Griffin, D. Kahneman, D. (edit.). 2002. Heuristics and Biases – The Psychology of Intuitive Judgement. pp. 49-81. Cambridge University Press. New York.

Klabbers, J. (2013). International Law. Cambridge university press.

Koops, B-J. (2013). Police investigations in Internet open sources: Procedural law issues. Computer Law & Security Review (6) 654-665.

Krempel, E. & Beyerer, J. (2014). 'TAM-VS: A Technology Acceptance Model for Video Surveillance' In Privacy Technologies and Policy. Springer, 2014, pp. 86-100.

Lichtenstein, Sarah; Slovic, Paul; Fischhoff, Baruch; Layman, Mark & Combs, Barbara (1978). Judged Frequency of Lethal Events, 4. Journal of Experimental Psychology: Human Learning and Memory.

Marin, L. (2013). Protecting the EU's borders from …fundamental rights? In R Holzhacker & P Luif (eds). Springer. New York.

Matvejeff, P. (2009). Luottamuksen Pula-Aika – tarina kunnanjohtajan luottamuspulasta ja sen seurauksista. ['A story about the lack of confidence in a mayor and its consequences'] Master's Thesis. University of Lapland.

Meijers Committee (2012). Note of the Meijers committee on the proposal for a regulation establishing the European border surveillance system.

Rajamäki, J & Knuuttila, J. (2013). 'Law enforcement authorities' legal digital evidence gathering: Legal, integrity and chain-of-custody requirement,' in Intelligence and Security Informatics Conference (EISIC), 2013 European, 2013, pp. 198-203.

Rajamäki, J. Tervahartiala, S. Tervola, S. Johansson, L. Ovaska & Rathod, P. (2012). 'How transparency improves the control of law enforcement authorities' activities?' in Intelligence and Security Informatics Conference (EISIC), 2012 European, 2012, pp. 14-21.

Rijpma, J & Vermeulen, M. (2015) EUROSUR: saving lives or building borders?, *European Security*, 24:3, 454-472.

Tammilehto, T. (2011). *Information Sharing in Human Trafficking Cases in the United Kingdom Law Enforcement.* MA in Criminology –thesis. City University London, UK.

Tversky, A. & Kahneman, D. (1974). Judgemnt under uncertainty: Heuristics and biases. Science.

Vanclay, F. & Esteves, A.M. (Eds.) (2011). New directions in Social Impact Assessment. Conceptual and Methodological Advances. Chelternam. UK.

Wells, D. & Gibson, H. (2017). 'OSINT from a UK perspective: Considerations from the law enforcement and military domains', in H. Maasing, From research to security union. Tallinn: Sisekaitseakadeemia, pp 83-114.

Xie, F. (2011). The Research on Information Sharing Behavior in Digital Age: Enabling Collaboration for Innovation. Proceedings of the 8th International Conference in Innovation & Management, pp. 888-891.

Zikmund-Fisher B. J., Sarr B., Fagerlin A. & Ubel, P. A. (2006). A matter of perspective: choosing for others differs from choosing for yourself when making treatment decisions. Journal of General Internal Medicine.

1.3 Structure of the Document

After the short introduction of ANDROMEDA solution, an overview of the legal framework of ANDROMEDA is provided, beginning with a big picture description of the relevant principles and norms, and ending with more detailed descriptions of the legislation (including also data protection). After that the main ethical and legal challenges of the use of ANDROMEDA are discussed based on literature review. The rest of the deliverable in chapters 7-9 elaborates the final outputs of this deliverable based on the analysis of the previous chapters as well as co-creation with project partners:1) initial Societal Impact Assessment (SIA) 2) initial ANDROMEDA Ethical Requirements 3) Initial ANDROMEDA Code of Conduct.

1.4 List of Acronyms

List of Acronyms	
AI	Artificial Intelligence
AIS	Automatic Identification System
ANDROMEDA	An Enhanced Common Information Sharing Environment for Border Command, Control and Coordination Systems
CISE	Common Information Sharing Environment
DPIA	Data Privacy Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ETIAS	European Travel Information and Authorisation System
EU	European Union
EUCISE	European test bed for the maritime Common Information Sharing Environment
EUROSUR	The European Border Surveillance system
E/O	Electro-Optical
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
HCI	Human Computer Interaction
IBM	Integrated Border Management
IMO	International Maritime Organization
LED	Law Enforcement Directive
LRIT	Long Range Tracking and Identification
MARISA	Maritime Integrated Surveillance Awareness
ML	Machine Learning
MS	Maritime Surveillance
OSINT	Open Source Intelligent
PbD	Privacy by Design/Privacy by Default

List of Acronyms	
PET	Privacy Enhancing Technologies
SAR	Search and Rescue
SBC	Schengen Border Control
SD/SDL	Service Logic/Service Dominant Logic
SIA	Social Impact Assessment
SOCMINT	Social Media Intelligence
SOLAS	The 1974 International Convention for the Safety of the Life at Sea
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UAV	Unmanned Aerial Vehicle
UN	United Nations
UNCLOS	United Nations (UN) Convention on the law of the Sea

2. ANDROMEDA in a Nutshell

ANDROMEDA 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 Guard 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 by adapting state-of-the-art command & control systems for full compliancy with the enhanced model and CISE message exchange patterns (ANDROMEDA GA 2019).

Specifically, ANDROMEDA aims to introduce applied solutions to enhance border and external security by:

- Defining Maritime CISE Model Enhancements and contributing on the CISE 2020 roadmap in coherence with the European Maritime Security Strategy Action Plan[2]
- Extending the scope of the CISE Model to support Land Border Operational Information Exchange
- Adapting state-of-the-art Command, Control and Coordination systems for full compatibility with the enhanced CISE Models
- Demonstrating advanced functions as well as Data Fusion, Analytics, Situational Awareness and Decision Support Services as parts of the C2 systems and the CISE advanced services
- Analysing the legal, ethical and cultural barriers of CISE
- Validating in an adequate period of time and three trials the CISE Compliant C2s and associated services by several Civil and Military Maritime and Land Border Agencies

2.1 The ANDROMEDA Architecture and Services

The proposed ANDROMEDA solution is a distributed set of systems and services interconnected according to the CISE principles that aim to foster faster detection of new events, better-informed decision-making and the achievement of joint understanding and undertaking of situations across borders. It includes CISE compliant Command and Control systems by means of total support of the CISE Service Model and project extended CISE Data Model, a suite of services to correlate and fuse various heterogeneous and homogeneous data and information from different sources, decision support tools, end-user legacy systems and components for the CISE network integration. Figure 1 shows the architecture of the ANDROMEDA solution. The various layers and components are (ANDROMEDA GA 2019):

A. ***The ANDROMEDA Command and Control Layer:*** This layer will provide the Command, Control and Coordination capabilities (Collection, Fusion, Analysis, Dissemination, Decision/Action) and will be integrated with all other layers. Three Command and Control systems will be adapted to the enhanced CISE models and configured according to the user requirements and needs:

- Socrates Operational Centre by GMV is one of the Socrates suite tools that is currently part of the Advanced Services deployed in EUCISE. The idea would be to use Socrates OC as a C2 system that would provide the capability of a total integration with CISE data model, allowing users to consume all the information provided by the CISE network and to provide information to it.
- ENGAGE C3i BME by STWS is one of the Command, Control and Coordination Systems demonstrated at the PERSEUS project (West and East campaigns) and a basis of various large-scale deployments (Incident Logging System of the International Maritime Surveillance Bureau of MMAIP, National Command System of the Hellenic Fire Brigade etc.)

[2] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf

- GeoC2 by INW is the basis for a series of national and international large-scale projects in both military and civilian clients (Portuguese Navy, Portuguese Directorate General for Maritime Policy, European Maritime Safety Agency)

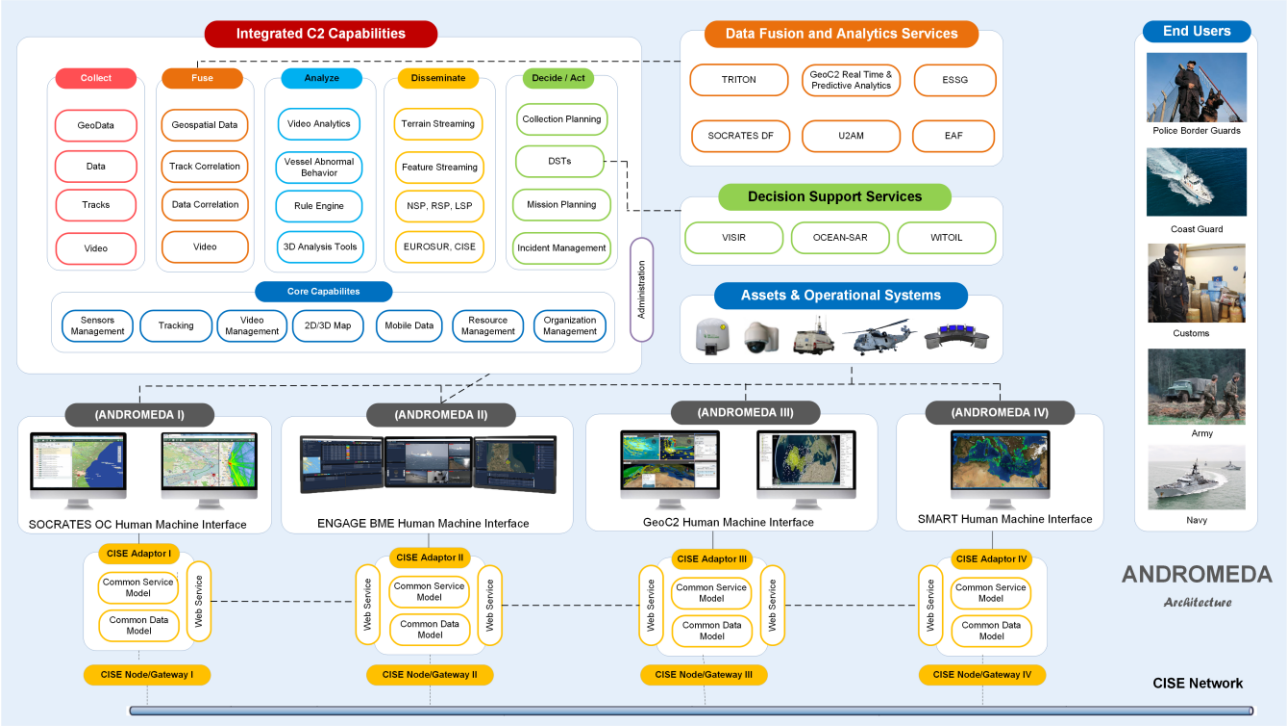

Figure 1: ANDROMEDA Architecture

B. ***The Data Fusion, Analytics & Situational Awareness Layer:*** ANDROMEDA consortium anticipates having the best possible set of data fusion algorithms that will lead to improved situational awareness. The following JDL models will be followed: Level 1 - "Observation of elements in the environment", Level 2: "Comprehension of the current situation", Level 3 - "Projection of Future States". The components comprising this layer are:

- ESSG Real Time Maritime Analytics, is a maritime surveillance solution based on the ESSG (Enterprise Security Service Grid) software framework developed by CDN.
- TRITON Analytics Engine by STWS, is a Vessel Abnormal Behaviour Detection Engine that identifies and analyses motion patterns of vessels that indicate an unwanted ongoing situation.
- Socrates DF Services by GMV consists of a JDL Level 1 fusion as a first step is converting large amount of received data into useful information, allowing further processing by next levels. The JDL Level 2 is the Behaviour Analysis Service designed to be tailored by the operator through a set of rules that can be configured and customized.
- GeoC2 Real Time Analytics by INW is a mixed heuristics / statistic analytics engine that continuously monitors a sensor stream, allowing for correlation events and alert events to be generated from the observations arriving from a system's sensor network.
- GeoC2 Predictive Analytics by INW uses state of the art Machine Learning techniques to correlate and forecast geospatial events and their recurrence, generating domain-neutral predictions for occurrence and location of events of interest – such as crowd movements, incident probabilities, thus allowing for pre-emptive mission planning and better goal-setting.
- EXUS Analytics Framework which main role is to take all the available measurements at a particular time "step t", that could be measurements from different sensors (like data sources,

radars, existing legacy systems, AIS data) and fuse them in order to obtain a set of more accurate results and in general to produce intelligence.

- U2AM: UAVs can provide enhanced situation awareness to border and customs authorities. The ICCS UAV systems for Land Border Surveillance will be used for identification and tracking of suspicious vehicles/objects, equipped with day and night vision sensors and/or spectral sensors. Two UAV systems (one fixed-wing and one octocopter) will be adapted to cover the following functionalities: Mission based object detection and tracking upon prior knowledge of suspicious targets, and surveillance-based object detection and tracking based on dynamic knowledge of possible suspicious routes and/or change of routes of illicit movement of illegal goods.

C. ***The Decision Support Layer:*** Consist of the following 3 services provided by CMCC.

- WITOIL (Where Is the Oil) creates a forecast of oil spill events, evaluate uncertainty of the predictions, and calculates hazards based on historical meteo-oceanographic datasets.
- VISIR is decision support system for ship routing. The model employs meteo-oceanographic forecast products to optimize nautical routes.
- OCEAN-SAR is a decision support tool for search-and-rescue (SAR) at sea. It simulates drifting objects at sea, using as input ocean currents and wind data.

D. ***The CISE Level:*** Consists of the CISE Adaptors that will comply with the enhanced and extended Data Model which will translate the C2's internal data model (when different) and provide the inbound and outbound Web Services that will wire to the CISE Nodes/Gateways. Given that ANDROMEDA will extend the CISE Data Model, the adaptors will not be compatible with the existing CISE test bed that is available to the premises of several ANDROMEDA end users. For this reason, the Adaptors will support also direct wiring of the Web Services and will also support (ANDROMEDA hybrid architecture) connection with future enhancements of the CISE Nodes/Gateways based on the project results and standardization actions.

E. ***The Assets and Legacy Operational Systems Level:*** Consists of the various end user surveillance systems (Land and Maritime radars, E/O, AIS, LRIT), assets and software applications but also assets (Land Border Radar, UAV, E/O) from technical partners (KEM, ICCS).

2.2 ANDROMEDA End-Users and Target Audience

The ANDOMEDA Consortium includes a trans-disciplinary group of experts that cover the range of activities from applied science to commercial high technology product development/supply. As key success factor, eight Border or Coast Guard End Users are involved as full partners (from six different countries) providing all the coordination and the expertise on the Land & Maritime Integrated Surveillance Awareness (MMAIP, HPL, ITN, PTN, INP, EAMA, HMOD, MSD), in order to deliver bottom-up user requirements and data models, scenario-based requirement and use-cases of the ANDROMEDA project (ANDROMEDA GA 2019).

In addition, ANDROMEDA will form a User Community that covers not only project partners, but also additional organisations, both users and providers of data and services, not directly involved in the project. The community will support and advise project partners with experience and know-how throughout the project duration. A key element driving this community is the collaborative involvement not only of users but also of all stakeholders, bringing together their expertise in Command & Control systems, DF technologies and SA information solutions, during and beyond the lifetime of the project. Therefore, the design of ANDROMEDA solution will integrate the user community experience in design and development as well as needs, operational scenarios, existing gaps, acceptability issues and societal impacts. Links with European projects

Key stakeholders of the ANDROMEDA target audience have been grouped into several categories, as depicted in Table 1.

Table 1: ANDROMEDA target audiences

Related Industry	End users/ Technology consumers	Facilitators
• Technology Providers • Scientific Communities • Defence Industry	• Government authorities (Border control – Defence sector – Coast Guards etc.) • FRONTEX • System Operators • SaR Operators • Commercial Customers • Authorities at Pilot Sites • The General Public	• EU Institutions (EC, European Science Foundation) • National Public Authorities (Industrial committees, national regulation authorities, ministry and regional councils) • Standardisation Bodies • Related EU-funded Projects • European Technology Platforms and Respective Clusters • Public Bodies & Environmental Organisations • European Policy Makers (MEPs) • Professional Associations • Immigration-related NGOs

2.3 Linkages with European Projects

In the current environment where governments in the EU face existing and continuing budget pressures, the need for cost effective solutions is of paramount importance. ANDROMEDA's aims to make use of the capabilities and results of other European programs, while introducing state-of-the-art technologies whenever appropriate and compatible with the proposed enhanced CISE (e-CISE) data models; the main EU Industry and Practitioners involved in the central Security European programs (e.g. EUCISE2020[3], Perseus[4], CLOSEYE, MARISA[5], RANGER[6], EWISA[7], CoopP[8] etc.) are present in the consortium composition. Moreover, several partners have been also involved in National Procurement projects of CISE Nodes and Adaptors and on the CISE infrastructure of the participating End-Users (ANDROMEDA GA 2019). Additionally, the ANDROMEDA consortium brings experience from European and National Activities related to Border and External Security, building also on the results of these projects. The broad knowledge of previous projects will allow to move from the current achievements and introduce improvements and further innovation.

2.4 Contribution to European Standards for Interoperable Systems and EUROSUR

Cross-sectorial and cross-border interoperability is one of the CISE principles. That is why the standardization process within ETSI was initiated already in the frame of the EUCISE2020 project. EUCISE2020 aimed to standardise the technical components of CISE, including the protocol stack, the semantic and data model specifications, the Core and Common Services as well as the operational components, including the

[3] EUropean test bed for the maritime Common Information Sharing Environment in the 2020 perspective, http://www.eucise2020.eu
[4] Protection of European seas and borders through the intelligent use of surveillance, https://www.perseus-fp7.eu
[5] Maritime Integrated Surveillance Awareness, https://www.marisaproject.eu
[6] RAdars for loNG distance maritime surveillancE and Search and Rescue opeRations, https://ranger-project.eu
[7] Early Warning for Increased Situational Awareness, http://www.ewisa-project.eu.
[8] Test project on cooperation in Execution of various maritime functionalities at sub-regional or sea-basin level in the field of integrated maritime surveillance (CoopP).

harmonized procedure for shared maritime situational awareness representation implementation, the alerts sharing protocols, etc. In addition, new regulatory procedures for the implementation of a "responsibility to share" information sharing policies within the existing regulatory framework at national and sectorial level is under investigation. No ETSI working group currently dealing with information sharing in the maritime domain and thus EUCISE2020 created a new Industry Specifications Group (ISG) with main objectives to develop the technical specifications to enable multiple organisations to develop an interoperable software to be used in a Common Information Sharing Environment for exchanging data and services. ANDROMEDA will further support this standardisation process in collaboration with EUCISE2020 Consortium and will try to introduce the extended CISE framework that will be developed (ANDROMEDA GA 2019).

ANDROMEDA produces the required information at all situational awareness levels and this concept is one of the key enablers to the successful further development and operational use of EUROSUR. The architecture, openness and flexibility of ANDROMEDA system also contributes to the further development of EUROSUR in allowing not only ANDROMEDA partners to contribute, but ensuring that innovations from other solutions, information and service providers to be easily integrated. Similarly, the approach of creating knowledge from identified data sources, but also allowing for evolutions in the number, type, format and origin of data is well adapted to the evolutions of EUROSUR and of the incredible amount and diversity of data that is constantly increasing. Thus, it is expected that ANDROMEDA will have a significant impact in the development of the EUROSUR network, since according to its regulation, the need for a proper situational awareness through the collection, evaluation, collation, analysis, interpretation, generation, visualisation and dissemination of information is defined in Article 8, where Article 9.9 is related to sharing information among national coordination centres neighbouring member states, directly and in near real-time in relation to incidents and tactical risk analysis.

3. The Norms of Maritime Security - The Big Picture

In this chapter we shed light on the big picture of the values and norms behind maritime surveillance and search and rescue (SAR) at sea, as well as on Land Border security. Both international law and a broad overall view of EU law will be discussed. More specific and detailed legislation will be discussed in the following chapters.

3.1 International Law

3.1.1 Overview

International Law, also called Public International Law or the Law of Nations, is a network of legal rules, principles and practices generally regarded and accepted as binding among states. The lack of a single, overarching authority from which the law emanates is perhaps the most noticeable characteristic of international law: its sources consist of bilateral or multilateral treaties that sovereign states voluntarily bind themselves to (the dominant source of international law), as well as customary law (general, established practice accepted as law). International law can thus be said to be a largely consent-based system. International agreements are often developed and negotiated within the framework of international organizations such as the United Nations[9] or the Council of Europe[10].

3.1.2 The European Convention on Human Rights

The birth of modern human rights thinking can be placed after WW2, with the Universal Declaration of Human Rights in 1948 by the UN marking a kind of a breakthrough. The declaration contains a collection of rights, with their underlying philosophy being that all individuals, by virtue of human dignity, enjoy certain rights and should be protected against their governments. Though not a legally binding document, the declaration's influence has been huge and at least some of the provisions can be argued to form a part of international customary law (Klabbers 2013).

It is, however, one thing to say that there is such a thing as universal human rights, and quite another to actually put them into practice. The Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights (ECHR), came into force in 1953 and is likely the most successful system for human rights protection. The convention offers protection for rights such as the right to life, the right to liberty and safety and the right to a fair trial. One thing that makes the convention so effective is that joining it, as almost 50 European states (including all EU member states) have done, entails acceptance of the jurisdiction of the European Court of Human Rights (ECtHR), a supranational court established by the convention. The ECtHR rules on complaints by individuals, organizations or states alleging on violations of rights set out in the convention and its protocols. It is worth noting that the applicant does not have to be a citizen of a contracting state. The judgements are binding and have led states to alter their legislation and administrative practice in a wide range of areas (ECHR 2010).

Since its adoption in 1950 the Convention has been amended several times and supplemented with many rights in addition to those set forth in the original text. The EU Charter of Fundamental Rights, which will be described later, is consistent with the ECHR: when the Charter contains rights that stem from this Convention, their meaning and scope are the same[11].

[9] http://www.un.org/en/sections/what-we-do/uphold-international-law/index.html
[10] http://www.coe.int/en
[11] http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm

3.1.3 The Convention Relating to the Status of Refugees

The Convention Relating to the Status of Refugees, (the Refugee Convention), is a United Nations multilateral treaty grounded in article 14 of the UN Declaration of Human Rights, which recognises the right of person to seek asylum from persecution in other countries (UN 1951).

Ratified by 145 states, the Refugee Convention defines the concept of a refugee, sets out the rights of the displaced, and the legal responsibilities of states to protect them. The convention is built upon a number of fundamental principles, the most notable of which are the principles of non-discrimination, non-penalization and non-refoulement. It is thus recognised that asylum seekers may be required to breach immigration rules and should not be penalised for their illegal entry or stay. The treaty prohibits that refugees or asylum-seekers be expelled or returned in any way to the frontiers of territories where his or her life or freedom would be threatened (UN 1951).

3.1.4 United Nations Convention on the Law of the Sea

A great deal of the general international law of the sea is found in the United Nations Convention on the Law of the SEA (UNCLOS). The treaty defines the rights and responsibilities of states in their use of the world's oceans and establishes a framework for the conduct of maritime commerce, the environment, and the management of marine natural resources. UNCLOS sets the geographical limits of maritime zones (e.g. the territorial seas over which each state has sovereignty) and establishes rights and discretionary and non-discretionary responsibilities of coastal States (UNCLOS 1994).

For the purposes of maritime surveillance and security, the most important provision in the UNCLOS is the article 98 on duty to render assistance. It obliges for every master of a ship flying the flag of a contracting state, so long as this does not put their own ship in danger: 1)To render assistance to any person found at the sea in danger of being lost 2) To proceed with all possible speed to the rescue of persons in distress 3)After a collision, to render assistance to the other ship.

Additionally, every coastal state shall promote the establishment, operation and maintenance of an adequate and effective search and rescue service regarding safety on and over the sea and, where circumstances so require, by way of mutual regional arrangements cooperate with neighbouring states for this purpose. (UNCLOS 1994).

3.1.5 International Convention for the Safety of Life at Sea

The International Convention for the Safety of Life at Sea (SOLAS Convention) is the most important treaty concerning the safety of merchant ships. The chapter 5 on Safety of Navigation, however, applies to all ships, on all voyages. From the perspective of maritime surveillance and security, two provisions stand out: the duty of any master of a ship to render assistance (similar to that in UNCLOS), and the duty of states to establish SAR services.

The duty to provide assistance applies **regardless of the nationality or status of the persons in distress** or the circumstances in which they are found. Once rescued, they shall be treated humanely and delivered **to a place of safety** (IMO WB). The provision on SAR services obliges each government to make all necessary arrangements for distress communication and coordination for the rescue of persons in distress at sea around its costs. These arrangements shall include the establishment, operation and maintenance of SAR facilities that are necessary and practicable with regard to the density of the seagoing traffic and the navigational dangers. Adequate means of locating and rescuing shall be provided (SOLAS 1974).

3.1.6 The international Convention on Maritime Search and Rescue

The 1979 International Convention on Maritime Search and Rescue (SAR Convention) establishes an international system for SAR operations. Its objective is to uphold an international SAR plan so that no matter where an accident occurs, their rescue would be coordinated by a SAR organization or several SAR organizations in cooperation.

Following the adoption of the SAR Convention, IMO's Maritime Safety Committee divided the world's oceans into 13 search and rescue areas, in each of which the countries concerned have delimited search and rescue regions for which they are responsible (IMO 2005).

The participating states to the SAR Convention are obliged to establish certain basic elements of a SAR service: a legal framework, assignment of a responsible authority, organization of available resources, communication facilities, coordination and operational functions, and processes to improve the service (including planning, domestic and international cooperative relationships and training). The Convention also regulates the establishment of preparatory measures, including SAR coordination centres and sub-centres. The convention outlines operating procedures to be followed in the event of emergencies or alerts and during SAR operations (SAR Convention 1979).

SAR Convention **includes several provisions providing guidance for SAR organisations on how information management and system design shall be performed in order to manage SAR situations**. These instructions can be taken into account in the ANDROMEDA services, so that they are well suited for rescue purposes:

- Each rescue co-ordination centre and rescue sub-centre shall have available up-to-date information relevant to search and rescue operations in its area. (SAR Convention 1979, chapter 4.1.1.).
- 'Each rescue co-ordination centre and rescue sub-centre should have *ready access to information* regarding the position, course, and speed of vessels within its area which may be able to provide assistance to persons, vessels or other craft in distress at sea, and regarding how to contact them. This information should either be kept in the rescue co-ordination centre or be readily obtainable when necessary' (SAR Convention 1979, chapter 4.1.2.).

3.2 EU Law

3.2.1 The European Council

The European Council is an EU institution that comprises the heads of government/state of the EU member states together with its President and the President of the Commission. Its task is to define the overall political directions and priorities of the Union. In June 2019, the European Council agreed on **a new strategic agenda for the EU for the next five years**. This agenda provides an overall framework and direction to respond to any challenges and opportunities that the Union faces, to promote the interests of EU citizens and to guide the work of union institutions in the next five years.

The Agenda comprises four priority areas: protecting citizens and freedoms; developing a strong and vibrant economic base; building a climate-neutral, green, fair, and social Europe; and promoting European interests and values on the global scale. From the viewpoint of Maritime and Land border surveillance, two priority areas are particularly important: 'protecting citizens and freedoms', and 'promoting European interests and values on the global scale'. In the following part, we will take a closer look at them both.

'Protecting citizens and freedoms' deals with the freedom, security and prosperity of the EU itself. The agenda underlines the integrity of the EU territory and the effective control of external borders is an absolute

prerequisite for upholding security, law, and order, and for ensuring that EU policies function properly. However, this cannot happen at the expense of European values and principles, such as fundamental and human rights. Most of the specific objectives under this priority area are directly relevant for border security. It is also noteworthy that these objectives look different from those of the previous, 2014 strategic agenda: a heavy emphasis has been put on effective border control and migration policies and practices, and the issues relating to SaR are named specifically.

Table 2: EC priority areas and ANDROMEDA

Priority area **Protecting Citizens and Freedoms**	**Contents**	**Relevance for ANDROMEDA and its Maritime and Land Border Surveillance**
'*Europe must be a place where people feel free and safe. The EU shall* ***defend the fundamental rights and freedoms*** *of its citizens, as recognised in the Treaties,* ***and protect them against existing and emerging threats.'*** *'We must ensure the* ***integrity of our territory****. We need to know and be the ones to decide who enters the EU.* ***Effective control of the external borders*** *is an absolute prerequisite for* ***guaranteeing security, upholding law and order, and ensuring properly functioning EU policies,*** *in line with our principles and values.'*	Developing a comprehensive migration policy. Deepening cooperation with countries of origin and transit. Fighting illegal migration and human trafficking and ensuring effective returns. An effective internal migration and asylum policy; a reform of the Dublin Regulation based on a balance of responsibility and solidarity, taking into account the persons disembarked following Search and Rescue operations. Enhancing the proper functioning of Schengen. Increasing EU's resilience against natural and man-made disasters through active solidarity and pooling of resources. Protecting the EU from malicious cyber activities, hybrid threats and disinformation.	Increased control and security measures are justified with the need to protect Europe against cross-border crime. The European maritime and land border is however not only a security issue for the EU, but also for those seeking to enter Europe. Deepening the cooperation with countries of origin and transit are relevant issues for ANRDOMEDA project and future business/adoption models. Protecting the European seas and borders should be aimed at both creating a secure maritime and land border environment, but also protecting the lives and physical and moral integrity of those at the sea and on land borders. The lack of accountability and clear lines of responsibility between EU member states and their different actors has been a persistent problem. Also, the diverging interpretations of international law hindered the cooperation between Member States in maritime surveillance and SAR.
Priority area **Promoting European interests and values on the global scale**	**Contents**	**Relevance for ANDROMEDA and its Maritime surveillance and Land Border Surveillance**
'In a world of increasing uncertainty, complexity and change, the EU needs to pursue a strategic course of action ***and increase its capacity to act autonomously to safeguard its interests,***	Leading the response to global challenges in the fight against climate change, promoting sustainable development, implementing the 2030 Agenda, cooperating with partner countries on migration.	Third countries must be taken seriously as stakeholders, partners, and potential users of information when developing ANDROMEDA and it future business/adoption models. The solution, in all of its dimensions, must be designed in such a way the

uphold its values and way of life, and help shape the global future.' *'The EU will* ***remain a driving force behind multilateralism and the global rules-based international order****, ensuring openness and fairness and the necessary reforms. It will support the UN and key multilateral organisations.'*	Pursuing an ambitious neighbourhood policy and developing a comprehensive partnership with Africa. Working towards global peace and stability, promoting democracy and human rights. Taking greater responsibility for EU's own security and defence; enhancing defence investment, capability development, and operational readiness; cooperating closely with NATO. More synergies between the EU and the bilateral levels; the EU needs to present a united front and avoid a piecemeal approach in order to have a robust foreign policy.	specific needs of each implementation context can be taken into account. The tensions between different rights, freedoms, and interests, such as those between European security interests and the humanitarian values is to be taken seriously when developing ANDROMEDA and its future adoption/business models. In addition to border control, both SAR, fisheries control and environment control are relevant aspects of maritime surveillance in the context of ANDROMEDA development and future use.

3.2.2 ANDROMEDA and EU Fundamental Rights

The earlier EU treaties were more or less purely economic and did not include references to fundamental rights. Therefore, the doctrine about EU law's precedence over national law eventually led to worries about the protection of fundamental rights granted in the national constitutions. In 1970, The Court of Justice of the European Union argued that, inspired by the common constitutional traditions of the member states, respect for fundamental rights forms an integral part of the general principles of EU law. The EU's Charter of Fundamental Rights is a document established in 2000 to bring consistency and clarity to the fundamental rights protected in the EU. The Charter became legally binding in 2009 when the Treaty of Lisbon was ratified and has the same legal weight as the EU treaties (EU 2007).

In addition to the EU Charter of Fundamental Rights, fundamental rights safeguards relating to border checks are also spelled out in secondary EU Law, particularly the Schengen Borders Code, as well as in the EU asylum acquis and in other regulations and directives. Thus, the fundamental rights are necessary requirements that set limits to what is and what is not acceptable in EC funded security research initiatives (CISE 2013).

In the context of maritime and land border surveillance activities, it is important to perceive that EU fundamental rights and/or Human Rights concern not only Europeans, but all the people, including those attempting to reach Europe**.** Important is also to note the positive value ethics can bring to the development. There are various fundamental rights, which ANDROMEDA can promote, both in the area of border control and maritime security. Thus, Ethics implication should not be viewed as a burden; on the contrary, it offers possibilities to create value in society – and to justify the existence of ANDROMEDA despite the challenges.

Table 3: EU Fundamental Rights

Dignity 1 Human dignity 2 Right to life 3 Right to the integrity of the person 4 Prohibition of torture and inhuman or degrading treatment or punishment 5 Prohibition of slavery and forced labour Freedoms 6 Right to liberty and security 7 Respect for private and family life 8 Protection of personal data 9 Right to marry and right to found a family 10 Freedom of thought, conscience and religion 11 Freedom of expression and information 12 Freedom of assembly and of association 13 Freedom of the arts and sciences 14 Right to education 15 Freedom to choose an occupation and right to engage in work 16 Freedom to conduct a business 17 Right to property 18 Right to asylum 19 Protection in the event of removal, expulsion or extradition Equality 20 Equality before the law 21 Non-Discrimination 22 Cultural, religious and linguistic diversity 23 Equality between women and men 24 The rights of the child 25 The rights of the elderly 26 Integration of persons with disabilities	Solidarity 27 Workers' right to information and consultation within the undertaking 28 Right of collective bargaining and action 29 Right of access to placement services 30 Protection in the event of unjustified dismissal 31 Fair and just working conditions 32 Prohibition of child labour and protection of young people at work 33 Family and professional life 34 Social security and social assistance 35 Health care 36 Access to services of general economic interest 37 Environmental protection 38 Consumer protection Citizen's Rights 39 Right to vote and to stand as a candidate at elections to the European Parliament 40 Right to vote and to stand as a candidate at municipal elections 41 Right to good administration 42 Right of access to documents 43 Right to refer to the European Ombudsman 44 Right to petition 45 Freedom of movement and of residence 46 Diplomatic and consular protection Justice 47 Right to an effective remedy and to a fair trial 48 Presumption of innocence and right of defence 49 Principles of legality and proportionality of criminal offences and penalties 50 Right not to be tried or punished twice in criminal proceedings for the same criminal offence

To clarify the links between fundamental rights and surveillance operations on the table below there are identified relevant EU fundamental rights from the viewpoint of EU citizens and migrants. The left column tells first the domain of surveillance from which viewpoint the rights are analysed, the central column identifies the rights ANDROMEDA can promote, and finally the right column reveals the rights which may be violated by the use of ANDROMEDA if it is not designed and used ethically.

Table 4: EU Fundamental Rights and Maritime and Land Border Surveillance

Aspect of maritime surveillance	**Rights which ANDROMEDA can actively promote**	**Rights to be protected/not to be violated**
Search and Rescue	**(2) Right to life** > Providing vital aid to people who are in distress or imminent danger, by rescuing them either in land or at the sea.	**(7) Privacy** **(8) Protection of personal data** **(21) Non-discrimination**

Aspect of maritime surveillance	Rights which ANDROMEDA can actively promote	Rights to be protected/not to be violated
	(6) Right to liberty and security >More efficient SAR operations. Responsibility for search and rescue remains valid no matter how one receives information about a vessel in distress. **(31) Fair and just working conditions** >Better information about the circumstances also from SAR personnel point of view.	
Border control	**(18) Right to seek asylum from persecution** >Border control operations should not prevent asylum seekers from having their demands examined. **(2 and 6) Right to life, liberty, and security.** >Border control operations should not prevent individuals from the right to leave their country. **(19) Protection in the event of removal, expulsion or extradition** > Border control must take into account the potential serious risk (e.g. death penalty, torture, other inhuman or degrading treatment or punishment) that refugees and migrants could be subjected to, if sent back. **(24) The rights of the child** >Border control must respect the best interests of any child, and specifically the child's right to maintain a personal relationship and direct contact with both of their parents (when parent(s) are already in the hosting country). Moreover, attention should be paid during border checks in order to identify children at risk of, for example, being trafficked. **(41) Right to good administration** > Border control operations should not prevent individuals from being heard, before any individual measure which would affect them is taken (e.g. approve or not their entry) and administration's obligation to give reasons for its decisions and be impartial and fair is of outmost importance. **(47) Right to an effective remedy and to a fair trial** >Border guards should also safeguard that everyone whose rights and freedoms guaranteed by the law of the Union are violated has the present right In addition, the following rights can be of relevance when dealing with asylum seekers, as these rights are often violated in their country of origin. **(1) Respect for Human dignity** **(4) Prohibition of torture and inhuman treatment** **(5) Prohibition of slavery and force labour** **(10) Freedom of thought, conscience, religion** **(21) Non-discrimination**	**(7) Privacy and family life** **(8) Data protection** The rights which can be promoted (in the left column) could also be violated if refugees and migrants are sent back to their country of origin.

Aspect of maritime surveillance	Rights which ANDROMEDA can actively promote	Rights to be protected/not to be violated
	(45) Freedom of movement	
Customs	**(16) Freedom to conduct a business** > Avoidance of pirate goods in the market. **(38) Consumer protection** >Improved maritime surveillance technology can help customs to protect EU citizens from illegal and pirate goods.	**(7) Privacy** **(8) Protection of personal data**
Environment	**(37) Environmental protection** >Improved surveillance system can help to fight environmental pollution e.g. by offering a better control over the vessels and their where about.	**(7) Privacy** **(8) Protection of personal data**

4. Legal Framework for Collaboration and Information Sharing in Maritime and Land Surveillance

The migratory crisis and the terrorist attacks in several member states have highlighted the need to reinforce the EU's external borders. The EU is working on concrete measures to safeguard Europe's security. These include among other things the following: new European Border and Coast Guard agency, an upgraded Schengen information system, systematic checks against relevant databases on all persons crossing the external borders, a new entry-exit system for non-EU nationals, the European travel information and authorisation system (ETIAS), new rules to make EU databases more interoperable. In this chapter we will shed light on the most relevant issues of this framework for ANDROMEDA.

4.1 European Border and Coast Guard Agency

The **European Border and Coast Guard Agency** (Frontex) was launched in October 2016 following the EU leaders' call to strengthen controls at external borders in September 2015. The agency **closely monitors the EU's external borders**. It also works together with member states to quickly identify and address any **security threats** to external borders. The European Border and Coast Guard helps to manage migration more effectively, improve the EU's internal security and protect the principle of free movement of people. In June 2018, EU leaders at the European Council meeting agreed to **reinforce the role** of the European Border and Coast Guard. Finally, the Council adopted 8th November 2019 the new regulation on the European Border and Coast Guard, an important element of the EU's comprehensive approach to migration and border management. (EU 2019)

According to the new regulation "the Agency relies on the cooperation of Member States to be able to perform its tasks effectively. In that respect, it is important for the Agency and the Member States to act in good faith and to exchange accurate information in a timely manner. No Member State should be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security. Member States should also, in their own interest and in the interest of the other Member States, contribute relevant data necessary for the activities carried out by the Agency, including for the purposes of situational awareness, risk analysis, vulnerability assessments and integrated planning. Equally, they should ensure that the data are accurate and up-to-date and are obtained and entered lawfully. Where those data include personal data, Union law on data protection should apply in full". (EU 2019, preambles 25-26)

In the implementation of the Regulation, the Agency and the Member States should make the best possible use of existing capabilities in terms of human resources as well as technical equipment, both at Union and national level. (EU 2019, preamble 72)

The new rules will allow Frontex also to strengthen cooperation with third countries. The agency will have a wider scope for action, and it will be able to extend cooperation beyond neighbouring countries. The agency will be able to conclude status agreements between the EU and third countries (limited to neighbouring countries under current rules). Frontex will therefore be able to deploy border management teams and liaison officers in such third countries. Status agreements have so far been negotiated with the following countries and are currently in force or pending signature: Albania, Bosnia and Herzegovina, North Macedonia, Montenegro and Serbia. (EU 2019)

4.2 Improved Schengen Information System

The Schengen information system helps preserve **international security** in the Schengen countries in the absence of internal border controls.

Authorities across the EU use the Schengen information system to enter or consult alerts for wanted or missing people and objects. It contains over 80 million alerts and was consulted over 5 billion times by authorities in 2017. In December 2016, the Commission proposed to strengthen the Schengen information system. The proposed regulations **address potential gaps and introduce new categories of alerts.**

In November 2018, the Council formally adopted the Commission's proposals. The upgraded Schengen information system is expected to be fully implemented by **2021**.

4.3 Systematic Checks

The Schengen borders code sets out the rules for checking people crossing the external borders of EU member states. On 7 March 2017, the Council adopted a regulation amending the Schengen borders code to reinforce checks at external borders.

Member states will be required to systematically check all people against relevant databases when crossing the EU's external borders. They will be able to ensure that those people are not threatening public policy, internal security or public health.

This obligation will apply at all external borders (air, sea and land borders), both at entry and exit. Certain derogations regarding sea and land borders may apply under very strict conditions and without risk for the public policy, internal security or public health

4.4 Entry-exit System

The Council adopted the regulation for an entry-exit system in November 2017. This system will **register entry, exit and refusal of entry information of non-EU nationals crossing the external borders** of the Schengen area. The entry-exit system will help:

- **reduce border check delays** and improve the quality of border checks by automatically calculating the authorised stay of each traveller
- ensure systematic and reliable **identification of overstayers**
- **strengthen internal security and the fight against terrorism and other serious crime** by allowing law enforcement authorities access to travel history records

The new system will be built by eu-LISA, together with member states, and is expected to be **operational by 2020**.

4.5 A New Online Travel Authorisation System

The EU lacks information on **non-EU nationals who do not need a visa** to enter the Schengen area.

EU leaders in September 2016 agreed to set up a European travel information and authorisation system (ETIAS) to enhance Europe's security. This system will carry **advance checks on visa-exempt travellers** and deny them travel authorisation if necessary. It will be similar to existing systems in place in the US, Canada and Australia, among others. The Council adopted the regulation establishing ETIAS on 5 September 2018.

ETIAS will bring several **benefits** such as:

- improved internal security
- better prevention of illegal immigration
- reduced public health risks

- reduced delays at the borders

ETIAS will be developed by **eu-LISA**. This is the EU agency that manages large-scale IT systems in the area of freedom, security and justice. The objective is to have ETIAS operational by **2021**.

4.6 More Interoperable Databases

Authorities across the EU use several databases[12] to fight crime, control borders, and manage migration flows. However, these IT systems have been fragmented and have not been interlinked with each other, resulting in a risk for information gaps.

In June 2017, EU leaders invited the Commission to prepare legislative proposals **to improve the interoperability of EU databases.** This launched a process that resulted in the regulations (EU) 2019/817 and (EU) 2019/818 being given by the Parliament and the Commission in May 2019. The regulations establish a framework for interoperability between EU information systems in the field of borders and visa, and in the field of police and justice cooperation, asylum and migration, respectively.

The objectives of the regulations on interoperability are:

a) to improve **the effectiveness and efficiency of border checks** at external borders;
b) to contribute to the prevention and the **combating of illegal immigration**;
c) to contribute to **a high level of security** within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and safeguarding security in the territories of the Member States;
d) to improve the implementation of **the common visa policy**;
e) to assist in the examination of applications for **international protection**;
f) to contribute to the prevention, detection and investigation of **terrorist offences** and of **other serious criminal offences**;
g) to facilitate **the identification of unknown persons** who are unable to identify themselves or unidentified human remains in case of a natural disaster, accident or terrorist attack.

Key to achieving these objectives are the correct identification of persons / combating of identity fraud, improving data quality and harmonising the quality requirements, facilitating and supporting technical and operational implementation of the systems, and streamlining access conditions and making the data protection conditions that govern the respective information systems more uniform. In order to achieve results specified in the regulations, four new tools in particular are established to improve information flows:

1) a **European search portal** (ESP) to search simultaneously in multiple EU information systems
2) a **shared biometric matching service** (Shared BMS) to search and cross-check biometric data in relevant EU information systems
3) a **common identity repository** (CIR) containing biographical and biometric data of non-EU citizens available in several EU information systems
4) a **multiple identity detector** (MID) to detect multiple identities linked to the same set of biometric data

[12] the Entry/Exit System (EES), the Visa Information System (VIS), the European Travel Information and Authorisation System (ETIAS), Eurodac, the Schengen Information System (SIS), and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).

4.7 Temporary Internal Border Controls

a) In Case of Exceptional Circumstances

The Schengen borders code (article 29) allows member states to reintroduce controls at certain internal borders in exceptional circumstances threatening the functioning of the Schengen area. In such situations the Council can recommend that one or more member states reintroduce border controls, based on a Commission proposal.

The reintroduction of internal checks should only take place as a **last-resort option,** and must fulfill the following conditions:

- controls can be reintroduced for **up to six months**
- controls can only be **extended three times**
- controls can last a **maximum of two years**

On 4 May 2016, the Commission recommended the reintroduction of border controls in the context of the then ongoing **migratory crisis**.

Massive irregular arrivals hindered some member states' ability to control parts of the EU's external borders. As a result of this irregular migrants moved around the EU putting the functioning of the entire Schengen area at risk.

b) In Foreseeable Cases

The Schengen borders code (article 25 and 26) establishes that member states can introduce temporary border controls in the case of foreseeable events.

The following conditions must be met:

- controls can be reintroduced for **up to 30 days** or for the foreseeable duration of the threat
- controls can last for a **maximum of 6 months**

The member state concerned must notify the Commission and the other member states at least four weeks before checks are introduced.

Internal checks in foreseeable cases under Articles 25-26 do not require the Council's approval, unlike checks introduced in the case of exceptional circumstances under Article 29.

4.8 Maritime CISE and EUCISE 2020 Project

CISE (Common Information Sharing Environment) is a voluntary collaborative **process** in the European Union to enhance and promote information sharing between authorities involved in maritime surveillance, within and across sectors. It does not replace or duplicate old information exchange systems and platforms, but rather builds upon them. The objective is to improve situational awareness and to ensure that information collected by one authority can automatically be shared to others, making data collection a less time and resource intensive exercise and to ensure that the relevant authorities will always have at their disposal the best available information (CISE 2014). The information being shared could be either unprocessed or processed, basic or rich. Maritime surveillance information data covers for example ship positions and routing, cargo data, sensor data, charts and maps, meteo-oceanic data and so forth.

The Commission emphasises that it is the responsibility of Member States to ensure the effective surveillance of waters under its sovereignty and jurisdiction, and on the high seas, if relevant. Ensuring the operational exchange of maritime surveillance information services between these authorities is the responsibility of

Member States, in some instances EU agencies can facilitate and support this process. Therefore, the operational aspects of such information exchange need to be decentralised to a large extent to national authorities in line with the principle of subsidiarity (COM 2014).

The EUCISE2020 Project

The interim report '*The Development of CISE of the Surveillance of the EU Maritime Domain and their related impact* assessment' addresses the mapping of the user communities of EUCISE2020 based on legal barriers, access rights and responsibility to share information. Secondly, it addresses the EU Right to Act and relevant opt-in opt-out clauses.

EU Maritime policy does not fall under a single sector-based policy but is based on a number of legislative acts with legal bases in different provisions of both the Treaty on the European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). If all user communities were to be included under a single framework of rules, it could, in theory, to seek recourse to multiple legal bases. However, the existing legal framework limits the possibilities to do so: TFEU and TEU competences may not be combined to provide a multiple legal basis for a single measure, as they have substantially different general characteristics, provide for divergent legal instruments and envisage different decision-making procedures.

According to the interim report, given that the defence user community has legal basis in the TEU and the other communities in the TFEU, it would be necessary to analyse the extent to which CISE seeks to implement objectives of the common foreign and security policy, as governed in the TEU, and to what extent similar objectives may be implemented under TFEU policies. The following conclusions with respect to the implementation of CISE can, thus, be made:

Firstly, the measure may be split in parts so that one part covers the user communities governed by TFEU, while another deals with the defence community (CISE 2013).

Secondly, it may nonetheless be possible to embrace all user communities under one TFEU measure, but only to the extent the objectives sought by the defence user community in CISE *can be implemented under the TFEU*. For example, the policies under title V of the TFEU (Area of Freedom, Security and Justice) developed to cover not only the Union's internal security but have external dimensions as well (e.g. fight against organised crime and terrorism). Monitoring in support of general defence tasks, as defined in Arts. 42 and 43 TEU would, however, normally fall outside the TFEU competencies (CISE 2013).

The EUCISE2020 Policy Options

EUCISE2020 interim report also presents the policy options drafted accordingly to the need that CISE corresponds to EU trend on information sharing and the identified legal barriers that should be overcame in order to implement CISE.

First policy option would focus on the positive CISE momentum already established and illustrated in the previous projects such as MARSUNO and BluemassMed. As a benefit, the above-mentioned approach does not attempt any changes to existing legislation. *First policy option* allows the full exploration of the significant initiatives in the area, such as EUROSUR. It is an approach that applies the current legal framework at national, EU and international levels: legal barriers prevail and the CISE development would be based on its own evolution adjusting to the legal reality (CISE 2013). According to interim report, this evolution may over time encourage and motivate the stakeholders to eliminate cultural, legal and technical barriers on their own will and pace.

Second policy option could be to seek to utilise the current information sharing potential to the maximum, by stimulating enhanced information sharing among user communities by means of recommendations. Policy option 2 could be seen as optimizing the status quo by streamlining the current situation and removing

inexpediencies that arise from cultural barriers (CISE 2013). According to interim report, it would intensify the current CISE stage as it continues the soft approach by facilitating the process as well as adds more specific recommendations on overcoming obstacles. Such recommendations should encourage pro-sharing interpretation of legislation at national and EU levels and encourage adjustments to national legislation. (CISE 2013).

A third policy option has similarities with the second policy option. However, the difference is that the policy option 4 would remove such barriers by applying legally binding provisions. According to interim report, specific legal barriers include for instance:

1) Limited responsibility to share/access rights - i.e. the act provides that a particular type of data shall be shared with specified MS and/or competent authorities thereof and/or for specified purposes;

2) Optional sharing of data, but no obligation to share;

3) The responsibility to share only with respect to some of the data collected within the framework of the act;

4) Specific user communities are excluded from the scope of the act;

5) No specific access rights provided and

6) Lacking institutional framework for data sharing (CISE 2013).

The fourth policy option combines the removal of barriers by legislative acts (option 3) with a voluntary approach encouraging cross-sectoral cooperation and data exchange in policy option 2.

Policy option 5 provides for a horizontal and cross-sectoral EU CISE legal framework flexible to utilise specific instruments addressing the specific categories of users and functions. In addition, a common legal framework will provide the CISE process with the cross-sectoral coordination and the political and legal weight. Policy option 5 provides also for the legal mandate to address binding and non-binding cross-sectoral initiatives for the CISE development (CISE 2013). The fifth policy option presents legal cross-sectoral mandate which will provide the legal mandate to ensure the horizontal coordination amongst the equally important sectoral legislation. In this case, the CISE legal framework adds the cross-sectoral and coordinated mandate to the already existing sectoral legislation. Together, the CISE legal framework and the sectoral legislation constitute the comprehensive EU regulatory framework for integrated maritime policy (CISE 2013). This framework would aim at embracing all user communities under one measure.

5. Privacy, Data Protection, OSINT and AI

5.1 Privacy and Data Protection

5.1.1 Background

To ensure a consistently high level of data protection, while simultaneously facilitating the exchange of data between competent authorities and promoting the digital economy, a comprehensive data protection package was adopted in the EU in 2016. This package comprises two main instruments:

1) Regulation (EU) 2016/679 (**The General Data Protection Regulation / GDPR**)
2) Directive (EU) 2016/680 (**The Data Protection Law Enforcement Directive / LED**)

The LED sets out rules for the processing for personal data by criminal law enforcement authorities (including private actors entrusted with the right to exercise public authority and powers for law enforcement purposes). The GDPR concerns largely all other processing of personal data by actors that are a) located within the EU, b) holding/processing the data of EU subjects, or c) offering goods/services to or monitoring the behaviour of EU data subjects. Content-wise there are some differences between the GDPR and the LED, especially regarding the principles and lawfulness of personal data processing and to the rights of the data subject, but the responsibilities of register owners and data processors are very similar.

'*Personal Data*' means any information relating to an identified or identifiable natural person ('data subject').[13] '*Controller*' means the (natural or legal) person, public authority, agency or other body, which determines the purposes and means of the processing of personal data. It does not make a difference if this is done alone or jointly with others. '*Processor*' means a (natural or legal) person, public authority, agency or another body, which processes personal data on behalf of the controller.

Only processors that provide sufficient guarantees to implement appropriate technical and organisational measures may be used; the use of a processor may not lead to worse protection for personal data. The processing activities must be governed by a contract or a comparable binding legal act.

Accountability

Accountability is a key approach in the new era of data protection. Controllers/processors are not only required to implement specified measures, but also to demonstrate compliance whenever requested. Protective measures must be undertaken before, during, and after processing personal data, as well as in the event of a breach. If a breach takes place, a controller must demonstrate the level of compliance prior to the violation, not just the acquired compliance level they reached afterwards. All measures shall be sufficient with regards to the risks involved.

The practical measures to reach accountability include, but are not limited to,

a) documentation on the objects, manner, time period and purposes of processing of personal data;
b) the establishment of procedures to tackle data protection issues, both when designing information systems and in the event of a data breach;
c) risk assessments regarding technologies, their development, use processes and business models
d) in many cases, the appointment of a Data Protection Officer

[13] 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

Accountability is an ongoing process that must be continually reviewed and updated. The development of new technologies or codes of conduct, or the appearance of new risks could mean that what is compliant today is no longer compliant tomorrow. Well-established accountability procedures can help to build trust with authorities and the public, to mitigate enforcement action, and may even become a competitive advantage.

The Risk-based Approach

Under both the LED and the GDPR, a controller is responsible for implementing "*appropriate technical and organisational measures*" to ensure lawfulness and compliance. In determining what counts as appropriate, at least *the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons* shall be considered. Data processors are, thus, instructed **to scale their protective measures to correspond to the risk levels in their activities**.

Identifying and evaluating risks in personal data processing requires a walk-through of the whole processing chain: going through every process, information system, personnel group, task and facility that are part of the personal data processing chain. The means to achieve adequate protection can look different in environments and for different types of actors. This risk-based approach represents a shift from detailed "tick-box" bureaucratic requirements towards a more flexible 'compliance in practice' - enabling a high level of protection, while also avoiding to over-regulate low-risk processing.

Data Protection by Design and by Default

Compliance requires that safeguards are integrated into the processing by default and by design, both at the time of the determination of the means for processing and at the time of the processing itself. The default settings, processes and procedures in any solution must be chosen so that they provide the highest level of data protection that is possible in the situation. Both technical and organisational measures that are appropriate (based on the risk analysis) must be implemented in an effective manner to ensure a high level of protection. A concrete example of a privacy by design and default-approach could be to use pseudonymisation whenever there are no specific reasons to the contrary¨

5.1.2 Principles

5.1.2.1 The Principles for Processing Personal Data

Processing of personal data refers to 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'. **The GDPR and LED apply, thus, even if personal data is not stored.**

The principles of personal data processing are essentially identical in the GDPR and the LED:

1) **Lawfulness, Fairness and Transparency**: personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subjects
2) **Purpose Limitation**: personal data shall be collected for specified, explicit and legitimate purposes, and not be processed in a manner that is incompatible with those purposes.
3) **Data Minimisation**: the data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4) **Accuracy**: the data shall be accurate and kept up to date: every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay.

5) **Storage Limitation**: the data must be kept in a form that permits the identification of data subjects only for as long as is necessary.
6) **Integrity and Confidentiality**: the data must be processed in a manner that ensures appropriate security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7) **Accountability**: The controller shall be responsible for and be able to demonstrate compliance with the legislation.

5.1.2.2 Lawfulness of Processing

Processing of personal data under the GDPR is lawful only when at least one justifying condition is met. Due to the heterogeneity of data sources and the purposes behind data processing in ANDROMEDA, the relevant justification can vary from case to case. All possible justifying conditions are listed below.

1) The data subject has given **consent** to the processing of her personal data for one or more specific purposes;
2) Processing is **necessary for the performance of a contract** to which the data subject is party;
3) Processing is carried out because of the **controller's legal obligation** under either EU law or national law;
4) Processing is done to protect the **vital interests of the data subject or of another natural person;**
5) Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller. Either EU law or national law must lay down the basis for the processing in these cases; or
6) Processing is necessary for the purposes of the **legitimate interest** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. This in particular if where the data subject is a child.

When it comes to the LED, member states are required to provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes of crime prevention, investigation, detection or prosecution, or the execution of criminal penalties (LED, article 8). The personal data shall not be processed for other purposes, unless such processing is specifically authorised by EU law or member state law.

5.1.2.3 Special Categories of Personal Data

Certain types of sensitive data are given a special status in the GDPR and LED. All processing of such data is prohibited, with some exceptions (the data subject themselves has manifestly made the data public, the processing is necessary to protect the vital interests of the data subject or of another natural person...). **Even in these cases, the data may only be processed if it is strictly necessary and appropriate safeguards have been ensured**. Sensitive personal data is:

a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership
b) genetic or biometric data processed for the purpose of uniquely identifying a natural person
c) data concerning health
d) data concerning a person's sex life or sexual orientation

5.1.3 Obligations for Controllers and Processors

5.1.3.1 Rights of the Data Subject

The legislation grants the data subjects numerous rights, for example the right to access to their data, and the right to rectification or erasure of personal data and restriction of processing. Controllers and processors are required to take appropriate measures to ensure the fulfilment of the rights the data subjects, and to facilitate the exercise of these rights.

5.1.3.2 Records of Processing Activities and of Data Breaches

Controllers and processors have an obligation to maintain records of processing activities. This entails a written overview and documentation, to be made available to the supervisory authority upon request. A list of minimum requirements is found in the legislation, including e.g.

a) information about the controller/processor
b) the purposes of the processing,
c) a description of the categories of data subjects and personal data,
d) the categories of recipients of the personal data (including planned future ones)
e) information about transfers to third countries or international organizations
f) time limits for storage
g) general descriptions of technical and organizational measures referred to in the section 'security of personal data' (below).

In order to be able to comply with the accountability principle, and specifically to be able to demonstrate compliance to the supervisory authorities, a register of any breaches of personal data must be kept by the controller. This documentation shall comprise the facts relating to the personal data breach, its effects and the remedial action taken.

Logging

For processing of personal data under the LED, keeping logs if compulsory:

a) the collection, alteration, consultation, disclosure including transfers, combination and erasure of personal data in automated processing systems must be logged
b) it must be possible to establish the justification, date and time of any consultation or disclosure operations based on the logs
c) the identification of people who consulted or disclosed personal data, and the identities of the recipients of such personal data, shall be facilitated as far as possible
d) the logs may only be used for the purposes of the verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.
e) the controller and the processor shall make the logs available to the supervisory authority upon request.

5.1.3.3 The Security of Personal Data

Security of Processing

The GDPR article concerning the security of processing does not provide any descriptions of general minimum measures for data protection but instructs controllers and processors to scale their protective measures to the likelihood and severity of the risks involved (the risk-based approach). Some suggestions for appropriate measures are, however, provided:

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regular testing, assessing and evaluating the effectiveness of technical and organisational security for ensuring the security of processing

A similar risk-based requirement is found also in the LED, but instead of mere suggestions there are concrete obligations. Following and evaluation of the risks involved, controllers and processors are to implement measures designed to:

a) control access to equipment
b) prevent unauthorised reading, copying, modification or removal of data media
c) prevent the unauthorised input, inspection, modification or deletion of stored personal data
d) prevent the use of automated processing systems by unauthorised persons using data communication equipment
e) ensure that authorised users to automated processing systems have access only to the personal data covered by their access authorization
f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment
g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input
h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media
i) ensure that installed systems may, in the case of interruption, be restored
j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported and that the stored personal data cannot be corrupted by means of a malfunctioning of the system

In order to know what constitutes ‘appropriate measures’, a controller/processor needs to **assess the risks involved**. The preamble to the GDPR gives some guidelines as to how data security risks can look: they might result e.g. from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (preamble point 83).

All actors who process personal data should have **the organizational and technological capability to notice and document breaches** (including ones caused by unauthorised/unlawful processing) - a regular firewall or encryption as a preventive instrument is not sufficient.

It is also important that **system data flows are documented** and that **trainings (and possibly tests) are given for personnel** with access to personal data. Without a periodically reported personnel education plan, it is hard

to demonstrate accountability and the lawfulness of processing. **Demonstrating accountability in all data processing will need strong and carefully planned governance structure**.

Notifications of Personal Data Breaches

'Personal data breach' refers to any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This definition is very broad, encompassing both instances of e.g. hacked data, but also of lost, stolen or improperly disposed hardware or paper records, or information mistakenly disclosed to unauthorised actors by staff members.

Controllers are generally obliged to **notify the appropriate supervisory authority about a breach** without undue delay (max 72 hours after having become aware of it) and to provide them with documentation about it. The exception is when the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Processors, in turn, have an obligation to, without undue delay, inform the controller after becoming aware of a breach. The information to be included in the notification is regulated in the articles 33 (GDPR) and 30 (LED).

Data subjects have a right to be **informed** without undue delay of a personal data breach that is likely to cause a high risk for their rights or freedoms. This notification should include the nature of the data breach and its possible consequences as well as the contact information of controller and measures taken by the controller.

5.1.3.4 Data Protection Impact Assessment and Prior Consultation

Data Protection Impact Assessment

When a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, both the GDPR and the LED oblige the controller to carry out a Data Protection Impact Assessment prior to the processing.

The DPIA according to GDPR shall contain at least:

a) A systematic description of the envisaged processing and its purposes, including the possible legitimate interests pursued by the controller
b) An assessment of the necessity and proportionality of the processing operations in relation to the purposes
c) An assessment of the risks to the rights and freedoms of the data subjects
d) The measures envisaged to address the risks. This includes safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance, taking into account the rights and legitimate interests of data subjects and other persons concerned.

The purpose is to describe the processing, assess its necessity and proportionality, and to identify and minimise risks as the initial step of any new project. DPIAs are important tools for accountability, as they help controllers to demonstrate that appropriate measures have been taken to ensure compliance.

Coles, Fairy and Ki-Aries (2018) have studied existing Privacy Requirements Engineering approaches and tools to support carrying out DPIAs. Their main contributions are:

a) existing requirements for engineering techniques associated with integrating requirements and information security process framework can be effective when supporting the different steps needed

when carrying out a DPIA. However, there is no one-to-one mapping between requirements and techniques, and several techniques might be needed to support a single step;

b) demonstration how an exemplar for Security Requirements Engineering tools supports and helps reason about potential GDPR compliance issues as a design evolves; and
c) they present a real example where their approach assessed the conceptual design of a medical application without an initial specification, and only the most preliminary of known functionality. They show that the use of this approach and the Requirements Engineering techniques in general, are effective in discovering additional functionality, and envisaging different forms of intended and unintended device use.

Prior consultation

The result of DPIA must be considered when planning control measures. If a controller is unable to mitigate the risks or if the DPIA indicates that the processing involves high risks, they must consult the supervisory authority before starting the processing activities (*'prior consultation'*).

5.1.3.5 Data Protection Officer

Designation of a Data Protection Officer

The designation of a Data Protection Officer (DPO) is compulsory for processing of personal data under the LED, and for processing under the GDPR in the following three cases, all of which hold true for ANDROMEDA:

a) if the processing is carried out by a public authority or body
b) if the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or
c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

The DPO may be a staff member of the controller or processor, but the designation has to be made based on professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks that the position involves. The possible additional task and duties cannot be ones that could result in a conflict of interest.

The Position and Tasks of the Data Protection Officer

The controller shall ensure that the DPO is properly involved in all data protection-related issues and shall support the DPO by providing her with the necessary resources, access to personal data and processing operations, and the maintenance of her expertise. The DPO may not be given instructions regarding the exercise of her tasks, and she shall not be dismissed or penalised for performing them. The DPO's tasks include at least:

a) **informing and advising** the controller or the processor and the employees who carry out processing of their legal obligations regarding data protection
b) **monitoring compliance** with the legislation and the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
c) providing **advice** where requested **regarding the DPIA** and monitoring its performance
d) **cooperation with the supervisory authority**;

e) acting as **the contact point for the supervisory authority** on issues relating to processing, including the prior consultation mentioned earlier, and to consult, where appropriate, with regard to any other matter.

It is important to note that the DPO is not personally responsible for compliance; the controllers and processor are. The DPO's role and responsibilities should be defined and documented in the business model and it must be included in it. The DPO will also influence the governance model where the roles and responsibilities of controllers/processors are defined in detail.

5.1.3.6 Codes of Conduct and Certification

The GDPR includes provisions regarding the devising of Codes of Conduct by associations representing data subjects/processors and the accreditation of data protection certifications, seals and marks. The purpose of these tools is to **facilitate compliance within specific industries and sectors, but the mere adherence to or obtaining of a Code of Conduct, seal, or mark does not in itself constitute proof for compliance**. National supervisory authorities or the European Data Protection Board can approve and register Codes of Conduct, and the Commission may decide that they have general validity within the union. The European Data Protection Board maintains a publicly available register of the certification mechanisms, seals and marks.

5.1.3.7 Transfers to Third Countries or to International Organizations

No special permission is needed for the transfer of personal data to countries outside the EU and to international organizations if the Commission has decided the target country or organizations has guaranteed the adequate level of personal data protection. The Commission maintains lists of countries and organizations that do or do not meet the requirements of the adequate level of personal data protection. In these cases, the controller or processor should enforce adequate measures of securing the personal data and to help the data subjects to use their rights. The transferring of personal data to third countries or to international organisations must always be based on binding contracts.

5.2 OSINT

OSINT is intelligence collected from publicly available sources, including the internet, newspapers, radio, television, government reports and professional and academic literature. OSINT binds through a systematic analysis process as a tight and informative thematic entity, the scattered information to be obtained from open sources. During the last few years, the internet and especially social media channels have revolutionized the ones that had significantly increased the amount of OSINT and information to be analysed. OSINT requires knowledge of the network environment with a good performer, a comprehensive means selection and problem-solving skills. Ethical questions apply to the handling of the collected information. When collecting data from people, one must remember that the creation of person registers is strictly regulated.

On the market, there are numerous efficient network analysis tools, some of which are also used by the public safety operators. Wells and Gibson (2017) have studied OSINT from a UK perspective and considered the law enforcement and military domains. Their conclusion was that the UK police and military open source investigations have a great number of similarities. However, there are several observable differences: (1) the handling of a chain of evidence; police forces prioritize and integrate a chain of custody for any intelligence that may lead to prosecution in a court of law and therefore the police tend to have a more structured and detailed approach to evidence gathering; (2) the use of third party software and developers; the military prioritizes the use of bespoke software tools and in-house training solutions, where the police have rationally used a variety of commercial and private sector solutions, some of which are specifically designed for police OSIN; and (3) the approach towards the dark web; the military has a far more cautious approach to operating

on the dark web, whereas the police have faced both pressure and a necessity to operate in this domain due to policing-specific concerns, such as online child sexual exploitation.

The International and EU regulation of OSINT includes the regulations and conventions. However, even though international regulatory guidelines are available, specific allowances, prohibitions and exceptions mainly stem from national legislation. Koops (2013) concerns procedural issues of OSINT in police investigations and investigates criminal-procedure law in relation to open source data gathering by the police. He studies the international legal context for gathering data from openly accessible and semi-open sources, including the issue of cross-border gathering of data. This analysis is used to determine if investigating open sources by the police in the Netherlands is allowed on the basis of the general task description of the police, or whether a specific legal basis and appropriate authorization is required for such systematic observation or intelligence. Hu (2016) identifies five key concerns relating to OSINT. These key concerns are gathered in the table below (left column) together with corresponding regulation (right column).

Table 5: Legal and ethical framework for OSINT

Key concerns for OSINT	**International and EU regulation for OSINT**
Origin and intent of sources Unclassified but sensitive Mosaic effect Reliance on automated analysis Publicity and visibility	European Fundamental Rights European Convention on Human Rights Cybercrime Convention EU Data Protection Regulation IPR legislation Liability Regulation of investigative agencies

Also, the line between espionage and OSINT can be very thin, therefore caution and double-checking are advised before conducting OSINT activities (Hribar, Podbregar & Ivanusa 2014). Koops (2013) also concerns the need for OSINT tools to meet non-manipulability and auditing requirements associated with digital forensic quality assurance.

MEDI@4SEC project identifies legal and ethical issues of using social media intelligence both from the viewpoint of the police use of social media, and from the viewpoint of involvement of citizens in the provision of public security. These viewpoints are summarized in the table below [6; 7]:

Table 6: Ethical and legal challenges of SOCMINT

Police Use of Social Media	**Citizens as Providers of Public Security (DIY Policing)**
Legal issues 1) The double role of public security agents as enforcers of the law and, data controllers) 2) Fundamental rights of the citizens 3) Involvement of citizens in the provision of the public security	Difficulty to ensure transparency, accountability and non-discrimination. Citizens are driven by their own interpretations of the law and morality without democratically legitimized authority and without sharing the required education, training or expertise.
Ethical issues 1) Disproportionate interference with the privacy of innocent individuals or groups 2) Risk of outright discrimination 3) Unfair access of some vulnerable or disadvantaged groups to criminal justice of public security 4) Police officer's rights to a private life and to freedom of expression	Key challenges (concerning especially dark web): - How to distinct between illegal and merely offensive or otherwise unethical behaviour - How to determine the line between justified covert interactions with criminals and unjustified entrapment

	- What are the national legal limitations in citizen's interference.

5.3 Big Data Analytics

Next table presents big data life cycles (left column) as well as special ethical and privacy questions (right column) of them.

Table 7: Big data life cycles and their special ethical and privacy questions

BD life cycle	**Ethical and privacy questions**
Capture	*Active*: data owner will give the data to a third party *Passive*: data are produced by data owner's online actions (e.g., browsing) and the data owner may not know about that the data are being gathered by a third party
Store	*Clouds*: cloud customer doing anything more than storing encrypted data must trust the cloud provider
Analysis	*Machine learning* techniques including neural networks run in two phases: training phase and prediction phase • quality of predictions is absolutely dependent on examples used for the training phase • ML systems are only as good as the data sets that the systems trained and worked with However, analysis does not directly touch the individual and may have no external visibility.
Use	Ethical issue comes especially with *automated policing*.
Destroy	How be sure that has destroyed all data in all redundant data storages in multiple physical locations?

With regard to ANDROMEDA technologies, data protection impacts should be assessed from four different dimensions of Big Data: 1) capture and storage, 2) data analysis, 3) use and destroying of data, and 4) technology and infrastructure behind data.

Big data may be analysed by Artificial Intelligence (AI). Machine learning (ML), a branch of AI, can provide detailed, personalized characteristics of an individual and prediction of his or her future behaviour. The High-Level Expert Group on Artificial Intelligence (AI HLEG) provided the AI Ethics Guidelines[14] to the

[14] https://ec.europa.eu/digital-single-market/en/news/have-your-say-european-expert-group-seeks-feedback-draft-ethics-guidelines-trustworthy

Commission in March 2019. The AI Ethics Guidelines form part of a vision embracing a human-centric approach to AI, which will enable Europe to become a globally leading innovator in ethical, secure and cutting-edge AI. It strives to facilitate and enable **"Trustworthy AI made in Europe"** which will enhance the well-being of European citizens. Trustworthy AI has three components which should be met throughout the system's entire life cycle:

- It should be lawful, complying with all applicable laws and regulations
- It should be ethical, ensuring adherence to ethical principles and values
- It should be robust, both from technical and societal perspective since even with good intentions, AI systems can cause unintentional harm

The framework does not explicitly deal with first component (lawful AI). Instead, it offers guidance for fostering and securing ethical and robust AI. Guidelines seek to go beyond a list of ethical principles, by providing guidance on how such principles can be operationalised in sociotechnical systems. The guidelines can be summarised from ANDROMEDA's viewpoint as follows:

1) Develop, deploy and use AI systems in a way that adheres to the ethical principles of: respect for human autonomy, prevention of harm, fairness and explicability.

   Acknowledge and address the potential tensions between these principles. Acknowledge that, while bringing substantial benefits to individuals and society, AI systems also pose certain risks and may have a negative impact, including impacts which may be difficult to anticipate, identify or measure. Adopt adequate measures to mitigate these risks when appropriate, and proportionately to the magnitude of the risk.

2) Ensure that the development, deployment and use of AI systems meets the seven key requirements for Trustworthy AI: (1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination and fairness, (6) environmental and societal well-being and (7) accountability.

   Consider technical and non-technical methods to ensure the implementation of those requirements. Communicate information to stakeholders about the AI system's capabilities and limitations. Facilitate the traceability and auditability. Involve stakeholders throughout the system's life cycle. Foster training and education to stakeholders. Be mindful that there might be fundamental tensions between different principles and requirements. Continuously identify, evaluate, document and communicate these trade-offs and their solutions.

3) Adopt a Trustworthy AI assessment list when designing, developing, deploying, implementing or using the systems, and adapt it to the specific use case in which the system is being applied. Keep in mind that such an assessment list will never be exhaustive. Ensuring Trustworthy AI is not about ticking boxes, but about continuously identifying and implementing requirements, evaluating solutions, ensuring improved outcomes throughout the AI system's lifecycle, and involving stakeholders in this.

Table 8: Trustworthy AI assessment list

Trustworthy AI assessment list
1. Human Agency and Oversight **Fundamental rights:** • Did you carry out prior to the AI system's development a fundamental rights impact assessment where there could be a negative impact on fundamental rights? Did you identify and document potential trade-offs made between the different principles and rights? • Does the AI system interact with decisions by human (end) users (e.g. recommended actions or decisions to take, presenting of options)? • Could the AI system affect human autonomy by interfering with the (end) user's decision-making process in an unintended way? • Did you consider whether the AI system should communicate to (end) users that a decision, content, advice or outcome is the result of an algorithmic decision? • In case of a chat bot or other conversational system, are the human end users made aware that they are interacting with a non-human agent? **Human agency:** • Is the AI system implemented in work and labour process? If so, did you consider the task allocation between the AI system and humans for meaningful interactions and appropriate human oversight and control? Do you secure the end user's right not to be subject to a decision based solely on automated processing? • Does the AI system enhance or augment human capabilities? • Did you take safeguards to prevent overconfidence in or overreliance on the AI system for work processes? **Human oversight:** • Did you consider the appropriate level of human control for the particular AI system and use case? • Can you describe the level of human control or involvement? • Who is the "human in control" and what are the moments or tools for human intervention? • Did you put in place mechanisms and measures to ensure human control or oversight? • Did you take any measures to enable audit and to remedy issues related to governing AI autonomy? • Is there is a self-learning or autonomous AI system or use case? If so, did you put in place more specific mechanisms of control and oversight? • Which detection and response mechanisms did you establish to assess whether something could go wrong? • Did you ensure a stop button or procedure to safely abort an operation where needed? Does this procedure abort the process entirely, in part, or delegate control to a human?
2. Technical Robustness and Safety **Resilience to attack and security:** • Did you assess potential forms of attacks to which the AI system could be vulnerable? • Did you consider different types and natures of vulnerabilities, such as data pollution, physical infrastructure, cyber-attacks? • Did you put measures or systems in place to ensure the integrity and resilience of the AI system against potential attacks? • Did you verify how your system behaves in unexpected situations and environments? • Did you consider to what degree your system could be dual-use? If so, did you take suitable preventative measures against this case (including for instance not publishing the research or deploying the system)? **Fallback plan and general safety:**

- Did you ensure that your system has a sufficient fallback plan if it encounters adversarial attacks or other unexpected situations (for example technical switching procedures or asking for a human operator before proceeding)?
- Did you consider the level of risk raised by the AI system in this specific use case?
- Did you put any process in place to measure and assess risks and safety?
- Did you provide the necessary information in case of a risk for human physical integrity?
- Did you consider an insurance policy to deal with potential damage from the AI system?
- Did you identify potential safety risks of (other) foreseeable uses of the technology, including accidental or malicious misuse? Is there a plan to mitigate or manage these risks?
- Did you assess whether there is a probable chance that the AI system may cause damage or harm to users or third parties? Did you assess the likelihood, potential damage, impacted audience and severity?
- Did you consider the liability and consumer protection rules, and take them into account?
- Did you consider the potential impact or safety risk to the environment or to animals?
- Did your risk analysis include whether security or network problems such as cybersecurity hazards could pose safety risks or damage due to unintentional behaviour of the AI system?
- Did you estimate the likely impact of a failure of your AI system when it provides wrong results, becomes unavailable, or provides societally unacceptable results (for example discrimination)?
- Did you define thresholds, and did you put governance procedures in place to trigger alternative/fallback plans?
- Did you define and test fallback plans?

Accuracy

- Did you assess what level and definition of accuracy would be required in the context of the AI system and use case?
- Did you assess how accuracy is measured and assured?
- Did you put in place measures to ensure that the data used is comprehensive and up to date?
- Did you put in place measures in place to assess whether there is a need for additional data, for example to improve accuracy or to eliminate bias?
- Did you verify what harm would be caused if the AI system makes inaccurate predictions?
- Did you put in place ways to measure whether your system is making an unacceptable amount of inaccurate predictions?
- Did you put in place a series of steps to increase the system's accuracy?

Reliability and reproducibility

- Did you put in place a strategy to monitor and test if the AI system is meeting the goals, purposes and intended applications?
- Did you test whether specific contexts or particular conditions need to be taken into account to ensure reproducibility?
- Did you put in place verification methods to measure and ensure different aspects of the system's reliability and reproducibility?
- Did you put in place processes to describe when an AI system fails in certain types of settings?
- Did you clearly document and operationalise these processes for the testing and verification of the reliability of AI systems?
- Did you establish mechanisms of communication to assure (end-)users of the system’s reliability?

3. Privacy and Data Governance

Respect for privacy and data Protection

- Depending on the use case, did you establish a mechanism allowing others to flag issues related to privacy or data protection in the AI system’s processes of data collection (for training and operation) and data processing?

- Did you assess the type and scope of data in your data sets (for example whether they contain personal data)?
- Did you consider ways to develop the AI system or train the model without or with minimal use of potentially sensitive or personal data?
- Did you build in mechanisms for notice and control over personal data depending on the use case (such as valid consent and possibility to revoke, when applicable)?
- Did you take measures to enhance privacy, such as via encryption, anonymisation and aggregation?
- Where a Data Protection Officer (DPO) exists, did you involve this person at an early stage in the process?

Quality and integrity of data

- Did you align your system with relevant standards (for example ISO, IEEE) or widely adopted protocols for daily data management and governance?
- Did you establish oversight mechanisms for data collection, storage, processing and use?
- Did you assess the extent to which you are in control of the quality of the external data sources used?
- Did you put in place processes to ensure the quality and integrity of your data? Did you consider other processes? How are you verifying that your data sets have not been compromised or hacked?

Access to data

- What protocols, processes and procedures did you follow to manage and ensure proper data governance?
- Did you assess who can access users' data, and under what circumstances?
- Did you ensure that these persons are qualified and required to access the data, and that they have the necessary competences to understand the details of data protection policy?
- Did you ensure an oversight mechanism to log when, where, how, by whom and for what purpose data was accessed?

4. Transparency

Traceability

- Did you establish measures that can ensure traceability? This could entail documenting the following methods:
- Methods used for designing and developing the algorithmic system:
  - Rule-based AI systems: the method of programming or how the model was built;
  - Learning-based AI systems; the method of training the algorithm, including which input data was gathered and selected, and how this occurred.
- Methods used to test and validate the algorithmic system:
  - Rule-based AI systems; the scenarios or cases used in order to test and validate;
  - Learning-based model: information about the data used to test and validate.
- Outcomes of the algorithmic system:
  - The outcomes of or decisions taken by the algorithm, as well as potential other decisions that would result from different cases (for example, for other subgroups of users).

Explainability

- Did you assess:
  - to what extent the decisions and hence the outcome made by the AI system can be understood?
  - to what degree the system's decision influences the organisation's decision-making processes?
  - why this particular system was deployed in this specific area?
  - what the system's business model is (for example, how does it create value for the organisation)?
- Did you ensure an explanation as to why the system took a certain choice resulting in a certain outcome that all users can understand?
- Did you design the AI system with interpretability in mind from the start?
- Did you research and try to use the simplest and most interpretable model possible for the application in question?

- Did you assess whether you can analyse your training and testing data? Can you change and update this over time?
- Did you assess whether you can examine interpretability after the model's training and development, or whether you have access to the internal workflow of the model?

Communication

- Did you communicate to (end-)users – through a disclaimer or any other means – that they are interacting with an AI system and not with another human? Did you label your AI system as such?
- Did you establish mechanisms to inform (end-)users on the reasons and criteria behind the AI system's outcomes?
  - Did you communicate this clearly and intelligibly to the intended audience?
  - Did you establish processes that consider users' feedback and use this to adapt the system?
  - Did you communicate around potential or perceived risks, such as bias?
  - Depending on the use case, did you consider communication and transparency towards other audiences, third parties or the general public?
- Did you clarify the purpose of the AI system and who or what may benefit from the product/service?
  - Did you specify usage scenarios for the product and clearly communicate these to ensure that it is understandable and appropriate for the intended audience?
  - Depending on the use case, did you think about human psychology and potential limitations, such as risk of confusion, confirmation bias or cognitive fatigue?
- Did you clearly communicate characteristics, limitations and potential shortcomings of the AI system?
  - In case of the system's development: to whoever is deploying it into a product or service?
  - In case of the system's deployment: to the (end-)user or consumer?

5. Diversity, Non-discrimination and Fairness

Unfair bias avoidance

- Did you establish a strategy or a set of procedures to avoid creating or reinforcing unfair bias in the AI system, both regarding the use of input data as well as for the algorithm design?
- Did you assess and acknowledge the possible limitations stemming from the composition of the used data sets?
- Did you consider diversity and representativeness of users in the data? Did you test for specific populations or problematic use cases?
- Did you research and use available technical tools to improve your understanding of the data, model and performance?
- Did you put in place processes to test and monitor for potential biases during the development, deployment and use phase of the system?
- Depending on the use case, did you ensure a mechanism that allows others to flag issues related to bias, discrimination or poor performance of the AI system?
- Did you establish clear steps and ways of communicating on how and to whom such issues can be raised?
- Did you consider others, potentially indirectly affected by the AI system, in addition to the (end)users?
- Did you assess whether there is any possible decision variability that can occur under the same conditions?
- If so, did you consider what the possible causes of this could be?
- In case of variability, did you establish a measurement or assessment mechanism of the potential impact of such variability on fundamental rights?
- Did you ensure an adequate working definition of "fairness" that you apply in designing AI systems?
- Is your definition commonly used? Did you consider other definitions before choosing this one?
- Did you ensure a quantitative analysis or metrics to measure and test the applied definition of fairness?
- Did you establish mechanisms to ensure fairness in your AI systems? Did you consider other potential mechanisms?

Accessibility and universal design

- Did you ensure that the AI system accommodates a wide range of individual preferences and abilities?

- Did you assess whether the AI system usable by those with special needs or disabilities or those at risk of exclusion? How was this designed into the system and how is it verified?
- Did you ensure that information about the AI system is accessible also to users of assistive technologies?
- Did you involve or consult this community during the development phase of the AI system?
- Did you take the impact of your AI system on the potential user audience into account?
- Did you assess whether the team involved in building the AI system is representative of your target user audience? Is it representative of the wider population, considering also of other groups who might tangentially be impacted?
- Did you assess whether there could be persons or groups who might be disproportionately affected by negative implications?
- Did you get feedback from other teams or groups that represent different backgrounds and experiences?

Stakeholder participation

- Did you consider a mechanism to include the participation of different stakeholders in the AI system's development and use?
- Did you pave the way for the introduction of the AI system in your organisation by informing and involving impacted workers and their representatives in advance?

6. Societal and Environmental Well-being

Sustainable and environmentally friendly AI:

- Did you establish mechanisms to measure the environmental impact of the AI system's development, deployment and use (for example the type of energy used by the data centres)?
- Did you ensure measures to reduce the environmental impact of your AI system's life cycle?

Social impact:

In case the AI system interacts directly with humans:

- Did you assess whether the AI system encourages humans to develop attachment and empathy towards the system?
- Did you ensure that the AI system clearly signals that its social interaction is simulated and that ithas no capacities of "understanding" and "feeling"?
- Did you ensure that the social impacts of the AI system are well understood? For example, did you assess whether there is a risk of job loss or de-skilling of the workforce? What steps have been taken to counteract such risks?

Society and democracy:

- Did you assess the broader societal impact of the AI system's use beyond the individual (end-)user, such as potentially indirectly affected stakeholders?

7. Accountability

Auditability

- Did you establish mechanisms that facilitate the system's auditability, such as ensuring traceability and logging of the AI system's processes and outcomes?
- Did you ensure, in applications affecting fundamental rights (including safety-critical applications) that the AI system can be audited independently?

Minimising and reporting negative Impact:

- Did you carry out a risk or impact assessment of the AI system, which takes into account different stakeholders that are (in)directly affected?
- Did you provide training and education to help developing accountability practices?
- Which workers or branches of the team are involved? Does it go beyond the development phase?
- Do these trainings also teach the potential legal framework applicable to the AI system?

- Did you consider establishing an 'ethical AI review board' or a similar mechanism to discuss overall accountability and ethics practices, including potentially unclear grey areas?
- Did you foresee any kind of external guidance or put in place auditing processes to oversee ethics and accountability, in addition to internal initiatives?
- Did you establish processes for third parties (e.g. suppliers, consumers, distributors/vendors) or workers to report potential vulnerabilities, risks or biases in the AI system?

Documenting trade-offs

- Did you establish a mechanism to identify relevant interests and values implicated by the AI system and potential trade-offs between them?
- How do you decide on such trade-offs? Did you ensure that the trade-off decision was documented?

Ability to redress

- Did you establish an adequate set of mechanisms that allows for redress in case of the occurrence of any harm or adverse impact?
- Did you put mechanisms in place both to provide information to (end-)users/third parties about opportunities for redress?

6. Ethical Challenges in Maritime and Land Border Security

In this section we shed light on the ethical and societal dimensions of maritime surveillance and Land Border operations aided by solutions such as ANDROMEDA. The purpose is to give the reader an overall picture of the value base for operations from the viewpoint of fundamental and human rights, as well as other principles and norms discussed in the previous section.

6.1 Maritime Surveillance and Ethics

Surveillance can be understood as the activities of watching, monitoring, recording, and processing the behaviour of people, objects, and events in order to govern activity'. Surveillance is thus not strictly confined to passive observing but includes also the recording and processing of that which is being seen, with the objective to gain knowledge useful in governing the observed activity.

'ICT-mediated surveillance increases the speed of control practices and the differential between the legal borders of rights and of policing, which casts a doubt over the pertinence of the latter claim. Critically engaging with the notion that Europe is 'under treat' … should thus go together with asking whether the Europe that is shaped by current border control and surveillance practices, has not itself become a threat.' (Jeandesboz 2011).

' Data Mining enables large amounts of personal data from disparate sources to be organised and analysed, facilitating the discovery of previously unknown relationships amongst the data. Knowledge Discovery in Databases (KDD) is a heuristic process of data mining which has evolved from the convergence of machine learning, database systems, statistics and artificial Intelligence. KDD is a multi-step process that facilitates the conversion of large data to valid, novel, potentially useful, and ultimately understandable information.' (European Group of Ethics 2014.)

The ethics of Maritime Surveillance has been a topic for vivid discussions in both academia and various other forums, reports and statements. Especially the concerns related to the relationship between privacy on the one hand and security on the other have gained a lot of interest in the debate, with perspectives ranging from predominantly philosophical viewpoints to practically oriented arguments. The utilization of technological advancements in surveillance, as exemplified by the use of surveillance camera drones, automated border control, and the collection and analysing of big data, raises worries about privacy and data protection. This is also the case with ANDROMEDA. There is a concern that this kind of technologies can be used to infringe on fundamental or human rights, for instance the protection of personal data and the protection of private life which are both protected under the EU Charter of Fundamental Rights (articles 7 and 8). The data collected in ANDROMEDA from various sources and sensors may contain information relating to identified or identifiable individuals at least indirectly, for instance via AIS data. The utilization of social media data poses further challenges with regards to the data subjects' rights.

In addition to privacy issues, the implications of the new surveillance technologies on asylum seekers and refugees have been deliberated by several scholars (see Marin 2012, European Group of Ethics 2014, Crepeau 2013, Meijers Committee 2012). As both EU law and international law regarding i.e. human rights, the rights of refugees and SAR activities impose obligations on states to help and protect those in need, the increased situational awareness enabled by the new technologies will also lead to an increased responsibility to act. For instance, both the Refugee Convention, the EUROSUR regulation, the EU Regulation 656/2014 and customary international law contain the principle of non-refoulement (the prohibition of returning asylum seekers to countries where they might be in danger.

There is also a risk that the in itself lawful purpose of maritime surveillance and information sharing to increase maritime security could nevertheless end up having a negative impact on the already vulnerable refugees. The

Meijers Committee - the Standing Committee of Experts on International, Immigration and Refugee Law - has noted the following:

'Assessing the content of the current proposal for a Regulation establishing the European Border Sur- veillance System, the Meijers Committee not only has doubts with regard to the necessity and efficiency of the proposed measures (also considering the high permanent costs involved), but is also very concerned with regard to the effects of Eurosur for the fundamental rights of asylum seekers and refugees, including the right to privacy and data protection. In particular, the Meijers Committee warns against the risks of increased surveillance as this might also increase the human costs of undocumented migration: border surveillance indeed will have an impact on migration routes but not on the root causes of migration.' (Meijers Committee 2012.)

In a similar manner, Francois Crepeau, the UN Special Rapporteur on the Human Rights of Migrants, has raised questions in 2013 regarding the consequences of the user processes of the EUROSUR system:

'The Special Rapporteur regrets that the proposal does not, however, lay down any procedures, guidelines, or systems for ensuring that rescue at sea is implemented effectively as a paramount objective. Moreover, the proposed Regulation fails to define how exactly this will be done, nor are there any procedures laid down for what should be done with those 'rescued'. In this context, the Special Rapporteur fears that EUROSUR is destined to become just another tool that will be at the disposal of member States in order to secure borders and prevent arrivals, rather than a genuine life-saving tool. (Crepeau 2013.)

The ethical/societal challenges and opportunities of ANDROMEDA are similar to those of maritime surveillance in general. However, ANDROMEDA's more efficiency and capacity in maritime surveillance highlights the importance considering these challenges and opportunities not only when designing the ANDROMEDA technology, but also as part of its user processes and business modelling.

ANDROMEDA can be developed either as a stand-alone version, or as part of the CISE environment. In the table below, the ethical aspects of ANDROMEDA in the possible compositions are illustrated. The darker the colour, the more challenging the ethical and societal issues to be solved.

Table 9: Ethics and ANDROMEDA's various compositions

	ANDROMEDA Technology	ANDROMEDA User Processes and Training	ANDROMEDA Business/Governance/ Adoption Models
ANDROMEDA as a Stand-alone System (in Europe and/or Outside)	Sufficient Privacy Enhancing Technologies. Technical challenges of OSINT, Big Data and Artificial Intelligence.	Unethical ways of using ANDROMEDA data in decision making, Organizational challenges with OSINT, BIG Data and AI Intelligence.	Misuse, dual use, other unethical use of ANDROMEDA (especially outside Europe)
ANDROMEDA as a Part of CISE	Sufficient Privacy Enhancing Technologies. Technical challenges of OSINT, Big Data and Artificial Intelligence.	Unethical ways of using ANDROMEDA data in decision making, Organizational challenges with OSINT, BIG Data and AI	Unethical aims of using ANDORMEDA in maritime surveillance

6.2 Search and Rescue (SAR) and the Duty to Render Assistance

Search and Rescue (SAR) organizations run by either public or private actors exist to assist people in distress or danger at sea. The statutory basis for SAR services is set out in both international treaties, EU legislation and national laws and regulations as shown in previous sections of this deliverable.

The Right to Life is one of the most fundamental rights enshrined in the EU Charter of Fundamental Rights (article 2) and the European Convention on Human Rights (article 3). In the maritime context, it has been codified by the duty to render assistance to persons in distress at sea and by the duty to establish and maintain search and rescue services (European Union Agency for Fundamental Rights 2013). The use of ANDROMEDA will increase the likelihood of finding out about any ships in distress at the sea, thus playing a role in saving the lives of people on board. Additionally, ANDROMEDA can help reduce the volume of sea vessels which are not seaworthy and thus save lives of migrants at sea.

The Duty to Render Assistance to those in distress at sea is found in multiple international treaties: at least UNCLOS (1982), SOLAS (1974), and the SAR Convention (1979). The duty applies to all vessels public and private, including private yachts and other non-commercial ships. Additionally, it poses responsibilities for coastal states to promote the establishment, operation and maintenance of SAR services, also in collaboration with neighbouring states when applicable. The European Agency for Fundamental Rights has in a 2013 paper stated the following: 'When the EU and its Member States provide assets, equipment and other maritime border management facilities to neighbouring third countries, priority should be given to assets and equipment that can be used to enhance their search and rescue capacities.'

Improved technological capabilities can raise questions concerning international responsibilities. When an actor that uses ANDROMEDA identifies an event taking place in waters outside of their area of responsibility that would call for a SAR operation, what legal and moral responsibilities can be vested on said state? Currently, according to the international law, states are responsible for maritime rescue operations in their designated SAR regions. However, it is of course possible that a state is, for one reason or another, unable to detect a situation of distress or to react to it in a timely manner, even within their national waters. The recent political turbulence in certain Mediterranean countries is a good example of a situation that poses risks for effective SAR operations. In circumstances like that, what are the responsibilities of the states that, with the help of technology such as ANDROMEDA, can monitor the situation from much further away than previously? Will it be sufficient for them to inform the local authorities of the situation, or are they also required to take action themselves? How can such actions outside of the regular SAR area be organised, and how can permissions to operate on foreign waters be granted?

Another moral dilemma for SAR created by the improved awareness and control at sea is related to the potential displacement of irregular migration. This kind of migration across the Mediterranean to Europe has probably always occurred. In 2015 and 2016 the numbers increased significantly, when the deteriorating situation in certain African and Middle Eastern states led to many refugees, displaced people and other migrants to try to get to Europe to apply for asylum. Improved border control and coast surveillance is likely to influence the flows and routes of migrants such as these, but the exact effects can be hard to predict. One undesired scenario is that the technological developments intended to increase safety and security at sea will result in the opposite effect, if migrants no longer can or dare to use their old routes and thus resort to other, more dangerous routes. This creates moral challenges for the development and use of surveillance technology. EU's commitment to the fundamental and human rights call for well-balanced actions to minimise the inadvertent harm caused by the adoption of new technology.

Both the duty to render assistance and the obligations of states related to SAR have implications for the development of ANDROMEDA. At least the following issues are to be deliberated further:

- How could we deliver information provided by ANDROMEDA to third counties so that they can also improve their SAR activities, but without any unwanted negative consequences?
- What should the division of labour be in situations where information is received about distress situations outside of a country's own SAR-region? Could Frontex be active in the coordination of such situations?

6.3 Smugglings

Smuggling is a practice which has existed (especially in the Mediterranean Sea) for thousands of years. The reason for it is simple: money, although in some very rare cases, people have been smuggled for altruistic reasons, too. The logic for smuggling is simple: either there exists a price difference for a product between the country of origin and country of destination, or for other reasons someone needs or wants to cross the border between two countries. Therefore, there is a profit to be made.

One can make a profit with smuggling illegal goods, i.e. goods that are forbidden in a country but that have a market nonetheless. Given that these goods cannot enter the market legally, the smugglers can charge for their services. Typical examples of illegal goods are various narcotics. The most commonly smuggled drugs to Europe are cannabis, heroin, (meth)amphetamine(s), and cocaine. Ingredients for manufacturing drugs are smuggled too.

Legal goods are also smuggled, i.e. goods that are *per se* legal, but are smuggled to avoid taxes or other fiscal payments, and hence money can be made. A classical and still relevant example of smuggled legal good are cigarettes, but the sky is the limit regarding the variety of smuggled legal goods: alcohol, electronics, perfumes, medicines, watches, weapons, food etc.

In addition, there is the specific kind of subject of smuggling: human beings, with or without their consent. The latter case, i.e. persons smuggled against their will is more often called trafficking of human beings.

The critical thing for ANDROMEDA is to understand that borders are in the centre of the phenomena of smuggling. Whether it is sea or land border, they are a prerequisite to smuggling. This does not mean that to get rid of smuggling, we need to eradicate borders. On the contrary, from an ethical point-of-view, securing borders enables protecting citizens from harm, such as drug abuse, but also keeps business to compete on the merits by not allowing anyone to gain a competitive advantage through illegalities. Further, when it comes to trafficking human beings, it is imperative to act. Quoting a member of LEA in the field of trafficking human beings: "You can afford to lose a kilo of cocaine, but you can't afford to lose a human being." (Tammilehto 2011)

Together with enhancing SAR, also reducing harm is an excellent ethical justification of ANDROMEDA. The requirement of ethical justification in the Code of Conduct is described later in chapter 9.

6.4 Irregular Immigration and the Surveillance of National Borders

The protection of the migrants' rights as well as the EU principles of solidarity and burden-sharing are constantly tested through the arrival of new migrant boats. EU integrated maritime surveillance and border control as well as the EUROSUR and CISE initiatives have been criticised by scholars as 'Push Back' operations (see e.g. Hayes & Vermeulen 2012; Rijpma & Vermeulen (2015). In order to 'defend' its borders, EU has funded sophisticated surveillance systems, given financial support to member states such as Bulgaria and Greece to fortify their borders, and created an agency to coordinate a Europe-wide team of border guards to patrol EU frontiers. From the viewpoint of the migrants, this kind of activities can pose severe threats to the fulfilment of human rights and various rights guaranteed in international conventions such as the refugee convention. Also, the strong role of industries in the development of new surveillance technologies has evoked

criticism. Marijn Hoitink, for instance, has in her 2012 article discussed the investment of resources in civil security without asking the public about the purpose and desirability of such investments and developments. Instead, the focus has largely been on improving the financial success of the industry. (Hoitink 2012.)

One additional challenge with the border control at sea is that the distinction between refugees and (economic) migrants cannot be done yet. A **refugee** is a person who 'owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group, or political opinion, is outside the country of his nationality, and is unable to or, owing to such fear, is unwilling to avail himself of the protection of that country (UN 1951). As described in the previous sections, refugees are subject to special protection arrangements under international law and cannot for example be returned to a region where they might be subjected to persecution (the principle of non-refoulement). Furthermore, refugees have a right to same treatment and economic and social help as any foreigner who is a legal resident. **(Economic) migrants,** on the other hand, choose to move mainly to improve their lives by finding work or similar, and generally continue to receive the protection of their government, should they choose to return home. However, since the determining of a person's refugee status happens through a specific administrative process and those concerned have a right to appeal against the decisions, in practice the principle of non-refoulement has to be applied to anyone wishing to come to Europe to apply for asylum.

Non-refoulement, *as explained previously,* is a core principle of refugee law: *refugees shall never be returned to the frontiers of territories where her life or freedom would be threatened on account of her race, religion, nationality, membership of a particular social group or political opinion*. Judgments of both the European Court of Justice (CJEU) and the European Court of Human Rights (ECtHR) have consolidated the application of this principle. In cases of so called indirect refoulement or chain refoulement *(*when one country returns a refugee to an allegedly 'safe' third country, which then returns them to an unsafe country), both countries may bear responsibility. However, as countries face increasing migratory pressures, they often try to interpret their international obligations more restrictively. As countries struggle to reconcile national security with their human rights obligations, they are taking a closer look at Article 33(2) of the refugee convention, which provides that:

'The benefit of the present provision may not, however, be claimed by a refugee whom there are reasonable grounds for regarding as a danger to the security of the country in which he is, or who, having been convicted by a final judgment of a particularly serious crime, constitutes a danger to the community of that country '. (UN 1951.)

In April 2014, following a long debate, the EU adopted a regulation which provides for Frontex-coordinated sea border surveillance operations to be carried out in accordance with the principle of *non-refoulement* and international search and rescue legislation.

ANDROMEDA services enable tracking vessels not only on their own sea territories, but also in the high seas and the territorial waters of third countries. It is therefore technically possible that ANDROMEDA will be used to organise border control outside countries' own borders and to redirect intercepted migrants to the coasts of third states. Trevisanut (2014) argues that border control has been detached from the territorial borders. Her main argument is that the principle of non-refoulement is a fundamental yardstick for this 'de-territorialization of border control and applies wherever competent state authorities perform border control measures. The principle of non-refoulement protects individuals against being sent to a country where they fear torture and other inhuman or degrading treatments, persecution on the basis of the grounds listed in 1951 Refugee Convention, or serious human rights violations. Furthermore, as Fischer-Lescano et al. (2009) have pointed out, the international obligations stemming from European law prohibit European border authorities from 'turning back, escorting back, preventing the continuation of a journey, towing back or transferring vessels to non-EU coastal regions in the case of any person in potential need of protection, as long as the administrative and juridical examination of the asylum application has not been completed on European territory. This

obligation is extraterritorial in nature and applies in all sea areas. European authorities are responsible for ensuring that the non-refoulement principle is respected also by any third parties involved in European surveillance and SAR operations. Since returning refugees to African transit countries is not considered to be in line with the principle of non-refoulement, and the determining of a person's refugee status cannot be done on the spot, basically anyone wishing to be taken to the EU to apply for asylum must be taken to the territory of an EU member state, with few exceptions. (Fischer-Lescano et al. 2009.)

Despite the clarity of the legislation, in some SAR operations the vessels in distress rescued by border patrols have been brought back to their port of origin. Such operations have been criticised as concealed push-back operations that violate both the rights and the needs of migrants. Human Rights Watch (2009) has drawn attention to the issue, pointing out that the principle of non-refoulement is clearly violated in these operations[15]. Misconduct such as this will be a significant concern also in the development and use of ANDROMEDA.

In addition to the above challenges, diplomatic aspects need to be considered. The use of ANDROMEDA could be considered as intrusive if it is used to monitor third state's territorial waters without prior agreement. Any state is sovereign within its territorial waters, and surveillance that reaches these waters should be carried out in the framework of agreements with the concerned third states.

The key challenge for the development of ANDROMEDA is thus ensuring that the rights of the already vulnerable refugees and other migrants are not further compromised for the interests of the more well-off European citizens. The following issues are to be discussed in detail during the project:

- Since EUROSUR and CISE probably have already taken into account the above criticism, it is crucial that ANDROMEDA's interoperability and compliance with EUROSUR and CISE covers also these ethical issues (not only technology).
- ANDROMEDA as a stand-alone solution, especially its user processes and business/governance model, need to be designed carefully, including the user training and selling/procurement strategy. The collaboration with non-governmental organizations is essential to create a sustainable action model.

6.5 The Displacement Effect

It is to be expected that the use of ANDROMEDA in border control and customs (either as a stand-alone solution or as part of the integrated CICE/EUROSUR solution) may cause situations in which one route of unregulated immigration and/or smuggling of goods closes, while another opens. As these new routes can be even more dangerous than the old ones, an increase of threat for the fulfilment of human rights, such as right to live and security occurs.

Displacement of the above type has in the context of 'the war on drugs' been called the 'balloon effect'[16]: squeeze a balloon in one place, and it expands somewhere else. Something similar is happening with efforts to crack down on irregular migration, but there is an important difference: when the balloon consists of people, they get more desperate the harder you squeeze. The balloon effect puts the supposed success of some migration control operations in a rather different light. (Andersson 2015.)

We can take the year 2010-2011 in Greece and Bulgaria as an example. In summer 2010, a sudden increase in irregular migration, mostly from Iraq and Afghanistan, tool place along a 12km stretch of the River Evros, which marks the land border between Greece and Turkey. Diverse actions to battle this development were implemented in Greece, including measures such as erecting a 12km long fence in Orestiada, but the numbers

[15] https://www.hrw.org/report/2009/09/21/pushed-back-pushed-around/italys-forced-return-boat-migrants-and-asylum-seekers
[16] http://www.coha.org/the-balloon-effect-and-displacement-part-2-of-2

climbed again in 2011, with a total of 57 000 irregular border crossings taking place: the Greek response had produced a displacement effect to the Bulgarian land border. The choice of sea routes also became innovative. Some smugglers even took the passage from Turkey to Italy. The smuggling of migrants has developed into an important industry in for instance in Turkey, with active networks in various cities, such as Istanbul, Izmir, Edirne and Ankara. The nationalities of the smugglers vary, frequently mirroring the nationality of their customers. The relaxation of Turkey's visa rules towards many African countries has created another pull factor for migrants from this continent, who arrive in Turkey by plane before attempting entry into the EU[17]. It can be expected that businesses of smuggling humans and goods will find new routes after their current Mediterranean routes will be closed. Therefore, the following issues are important to be taken into consideration when implementing ANDROMEDA:

1) Before the implementation of ANDROMEDA, it is crucial to always make a feasibility study and a societal impact assessment for ANDROMEDA in the proposed area, and to take action to eliminate any undesirable consequences beforehand. The role of both governmental and non-governmental organizations is essential to find sustainable solutions.
2) After implementation, follow-up evaluations of the consequences of ANDROMEDA are to be carried out for the purposes of e.g. risk analyses. If ANDROMEDA is sold stand-alone system instead of as part of the CISE ecosystem, this information sharing must be designed separately.

6.6 Land Border Security

In addition to the ethical challenges in Maritime Surveillance (MS), Land Border Security (LBS) has its particularities. Many of them overlap with the maritime environment, thus this paragraph can be somewhat repetitive.

The analysis of the ethical challenges begins with identifying different sensors/sources of data used in LBS, since many of the challenges are related to the specific characteristics of the data (image, sound…).

Thus, three types of sensors can be identified. In this analysis, we have made the typology depending on the so-called sense, as the sensors were human like capabilities. The reason for this is predominantly practical. Since, we need in the analysis input from the end-users, who perhaps are not experts in ethics, it is often useful to bring the discourse on a very pragmatic level. Also, many of those who are conducting the ethical analysis lack the finesse for very technical details. Be that as it may, the sensors are divided in this chapter into ones of *vision* (e.g. optical cameras, videos, thermal cameras etc.), of *acoustic* (e.g. microphones), and of *scent* (e.g. sniffing devices). In addition, we added a fourth that comprise of sensors that does not fit in well with the typology presented above, for example, motion detection, seismic sensors, Geiger counter etc. Another separate category under the title others, was also added. This includes intelligence, i.e. data, information and knowledge gathered by others, and shared to ones. In addition, the use of Artificial Intelligence was put in this category.

In short, the typology is visualised in the illustration below.

Example Typology of Sensors Used in Land Border Security

SENSORS

1. *Vision*
    - Optical camera (day time)
    - Optical camera, high definition (day time)

[17] http://frontex.europa.eu/trends-and-routes/eastern-mediterranean-route

- Optical camera (night vision)
- Thermal image/ Infrared camera

2. *Acoustic*
   - Microphone, low quality
   - Microphone, high quality
3. *Scent*
   - Sniffing device (dangerous goods and/or persons)
4. *Other*
   - Motion detection, simple
   - Seismic sensors
   - Pyroelectric detectors
   - Laser
   - Chemical detector
   - Mobile sensing (detecting mobile phones)
   - Geiger counter (radioactive material)

OTHER

Intelligence

- Trend and pattern analysis
  - Warnings, tips etc.
  - Artificial Intelligence, algorithms, Warning Engines etc.

Once the sensors and other sources of data are being identified, the analysis can be widen into pondering the different ethical aspects and challenges of each sensor. However, first must be noted the general challenge that touch all the sensors, namely the recording and storage of the data. All the above-mentioned sensors produce data that can be recorded, and thus needs to be stored somewhere. As a result, these recordings of data, its handling, usage, possible altering, processing etc. all pose ethical various challenges starting from the problematics of ownership to the correct ways of processing data. In this preliminary analysis we do not get to every detail. Critical is to acknowledge that there are various challenges in these areas.

What comes to the challenges related with the typology, the preliminary ones are presented here below:

SENSOR TYPE	ETHICAL CHALLENGES
• Optical camera (day time) • Optical camera, high definition (day time) • Optical camera (night vision)	• Depending of the quality and the resolution, the cameras can take pictures that reveals targets faces, i.e. the identity of the targets/subjects, privacy issues can become an ethical challenge. • It must be noted that face is not the only critical area, since, for example, high definition optical cameras have the capability of detecting other personal characteristics, such as pace. • There must be a clear understanding on where the cameras can be aimed at. People are entitled to their privacy, thus the breach of that must be done in accordance of law. • Another question is the need of images altogether. Photos are realistic, i.e. picturing the landscape as it is. However, it would be ethically sustainable to consider whether the operational needs should guide the use of the sensors, and not the

SENSOR TYPE	ETHICAL CHALLENGES
	technology *per se*. For example, if the need is to know the number of individuals crossing the border, loitering in an area etc., then there is not necessarily a need to have the capacity to identify person's identity, e.g. faces. Maybe, a simpler sketch would serve the purpose. Nevertheless, there are many ethical considerations on the use of optical data (i.e. the photos, video etc.).
• Thermal image/ Infrared camera	• Thermal image can reveal not only identity but also breach privacy by showing to the operator of the camera images/video that are almost comparable to images/video of a naked person. This has already been raised as an ethical challenge in many airports.
• Microphone, low quality • Microphone, high quality	• Person's identity can be revealed from sound of one's voice. • A high-quality microphone can also reveal private conversations; thus, eavesdropping can become an ethical issue.
• Sniffing devices (dangerous goods and/or persons)	• Some devices operate with high voltage, using radiation etc., and can thus be harmful to health. In cases persons are hiding in the cargo, it must be assured that these devices do not pose any risk to their health.
• Motion detection, simple • Seismic sensors • Pyroelectric detectors • Laser • Chemical detector • Mobile sensing (detecting mobile phones) • Geiger counter (radioactive material)	• Laser beams can be harmful to health so in the use one must be careful • Detecting dangerous chemicals or other dangerous material, such as radioactive, brings the responsibility to notify all the individuals that have been possible contaminated, not forgetting to get them the necessaire medical attention. • Mobile sensing can reveal personal information including identity. Therefore, its use is not without ethical challenges either. • The placement of motion detectors can result in to a so-called balloon effect, in which for example irregular immigrants that try to cross the border illegally, will take unnecessary risks when trying to enter undetected.
• Trend and pattern analysis • Warnings, tips etc. • Artificial Intelligence, algorithms, Warning Engines etc.	• The use of anything on the continuum of data-information-knowledge-intelligence needs a thorough risk assessment. Usually, the closer you are to the data provider, or if you are indeed the actual provider, the reliable the material is for further use, analyses or operational. • Especially challenging from ethical point-of-view is information received from outside ones' organisation. The critical question is reliability: to what extent should one plan

SENSOR TYPE	ETHICAL CHALLENGES
	any border security activities, nevertheless execute ones, if and when the intelligence is questionable. • The less trusted the data provider is, the more careful one needs to be, and for example, even deliberate mis-information cannot be ruled out. • In addition to humans processing data, AI is increasingly processing not just data, but forming intelligence. This is one area, where there is a multitude of ethical challenges, starting from the programming of the AI to the very basics of the rules of AI.

Above table is a simplification of the actual border security. In real life, multisensory systems are in everyday use, for example, both sound and image in one video. Thus, the challenges presented here can be easily become more complex. Further, combining various data from different sensors, together with databases and other sources of information, challenge performing LBS in an ethically sustainable and societally acceptable way even greater.

Facing this complexity, it is perhaps comforting to know, that in ethics, questioning is often more significant, than getting to the bottom of it.

6.7 Human Collaboration, Technology and Information Sharing

To increase the Maritime and Land Border Security actor's willingness to collaborate across disciplines, several ethical aspects need to be addressed in order to enhance trust not only towards ANDROMEDA technological solution, but also towards the other organizations utilizing and providing the data. It is imperative to be mindful of the ethical dimensions of information sharing. Even when the law permits agencies to share information, they may still worry about their ethical obligations to preserve the privacy, safety, and wellbeing of those they serve. Information about a person's involvement with the criminal justice system, for instance, is highly sensitive information that when carelessly disclosed to unintended parties can lead to problematic consequences. National security agencies (e.g. border guards, the police, the military) may be reluctant to share information if there is a concern that the release might lead to violations of their jurisdiction, jeopardization of national security, or other misuse that may lead to worse outcomes for the national security.

In a similar manner, justice officials must ensure that data are used accurately, properly, and by the right people, and that the release of maritime and land border security related information does not lead to harsh or unsafe treatment of people or use of technology. These factors play a role also in ANDROMEDA, even if the data fusing and sharing solutions are approached first and foremost from a technical aspect. The ethical aspects of cross-border and cross-sectoral collaboration need to be addressed regarding both users, information systems and processes. Strategies to mitigate some of the ethical concerns in information sharing may include aspects such as;

1) Reaching an explicit understanding among the information sharing entities about which information will be shared, in what circumstances, for what purposes can it be used, and who will have access to it

2) Developing legal & technical tools that effectively limit the use of sensitive information to its intended purpose

Human–computer interaction (HCI) studies the use and design of technology, with focus on the interfaces between the technology and its users. For technological solutions to be truly successful, people should not only be able to use them properly, but also to trust and accept them

Human factors, or ergonomics, refers to the science of designing products, processes and systems so that human psychological and physiological qualities are acknowledged to optimise both human well-being and overall system performance. The field has embraced 'situation awareness' as a construct to aid our understanding about human decision making in complex dynamic systems and to help with the design of human-machine interfaces (Shorrock & Claire 2016). One of the central challenges in ergonomics lies in predicting and preventing repercussions in high-risk socio-technological systems.

Understanding human-technology interaction and human factors is central in the development and use of ANDROMEDA. Factors related to the design of ANDROMEDA are likely to influence the level of acceptance the toolkit receives: the fact that the use of certain technologies in maritime and land border surveillance is permitted or even legally required does not entail that the use of such **technology would be risk-free.** It is essential for the developers of ANDROMEDA to understand how people interact with technology in high-pressure and real-life situations. Also, the question of **autonomous decision-making** processes, especially concerning 'who controls what' is an example of an aspect in ANDROMEDA that may become an issue to some security actors and/or the general public. Opting for solutions that embed privacy into the design of business processes, technologies, operations, and information architectures in a holistic, integrative and creative way is highly encouraged. All in all, 'ethics by default' type of thinking regarding decision-making patterns, risk assessments and mitigation, governance, etc. is recommended throughout the development and use of ANDROMEDA.

Several technologies are used among the ANDROMEDA community and stakeholders to promote the information and knowledge sharing and collaborative work. Such means of collaboration may also inherent ethical considerations, namely in relation to intellectual property, processing personal data, and sharing of information across the borders. Table below will be updated throughout the first half of the ANDROMEDA project.

Table 10: Information Sharing

Information sharing		
Functional category	**Examples of Technologies**	**Ethical considerations**
Communication technologies	• E-mail • Instant messaging, • Audio and video conferencing such as Skype	• Data protection • Privacy protection
Information-sharing technologies	• Document management system such as ANDROMEDA SharePoint (managed by KEMEA) and project website • Data conferencing	• Data protection • Intellectual property
Process-support technologies	• Electronic meeting system • Collaborative working platform such as Slack	• Data protection • Intellectual property
Coordination technologies	• Workflow management system • Calendar and scheduling system	• Data protection • Intellectual property
Integrated Technologies Across Functional Categories	• Collaboration product suite • Web-based team/project room • Integrated team support technology (Slack	• Data protection • Intellectual property • Privacy protection

	• E-learning system	

The benefits of collaboration from the organisational learning perspective are widely accepted. Sharing information and knowledge can be critical in driving both individual and organizational creativity and innovation. Innovation is fostered by collaboratively work, which requires information resources, insights and experiences, and problem-solving capabilities shared by members of formal or informal group. Consequently, the relationship between information sharing and collaboration is central to innovating new technological solutions, processes or services. To provide some conceptual clarity for **information sharing behaviour**, table below provided by Xie (2011) summarises a general categorization.

Table 11: Information Sharing Behaviour in General (by Xie 2011)

Information Sharing Behaviour in General		
Definition	**Characteristic**	**Explanation**
Collaboration or Collective Behaviour	Responsibility, Obligation	Information sharing as an umbrella concept that covers a wide range of collaborative behaviour
Mutual Benefit Behaviour	Relationship and Social Capital	Pursuing economic and rational interests to seeking psychological and social benefits.
Helping Behaviour Personal	Preference or Self-realization	Information value-added as transferred and transformed between people or within organization.

6.8 Human Decision Making and Ethics

Just like other animals, humans look at the world through a lens of evolved adaptations. Our sensory organs are tuned to respond to some types of stimuli – for example certain wavelengths of light - while ignoring others, so the sensory inputs coming into our brains are selected from the beginning. Also, the mechanisms in the human brain that use this 'raw data' to produce a holistic perception of reality are affected by numerous distortions related to for instance working memory limitations, attentional biases, preconceived expectations, emotional responses, and even the language we use to conceptualise our experiences. Each individual's perception of reality is thus inherently subjective in nature, and it is these subjective perceptions that govern our behaviour in the social world.

That our perceptions and cognitive processes would be so unreliable might seem a little surprising, but from an evolutionary perspective it makes a lot of sense: we have evolved to survive, not to be great scientists. When evaluating the risks of either physical threats (predator attack, poisonous food) or social ones (disapproval, punishment, exclusion from the group), it has been much better to be safe than right. The ability to jump to quick conclusions and to generalise instead of engaging in timely evaluations of logical soundness has thus been highly adaptive. The biased nature of human perception and thinking is not inherently good or bad, but it is something we need to be aware of when designing and using new technology with potentially far-reaching implications for human decision making and society.

Cognitive (psychological) biases are, thus, systematic patterns or tendencies to deviate from rational judgement. They are sometimes confused with logical fallacies but are not the same. A logical fallacy is an error in argumentation that can generally be detected by examining the logical form of the specific argument: does the conclusion follow from the premises or not? A cognitive bias, on the other hand, is more like a subconscious predisposition towards perceiving, thinking and making judgements in a certain way or of a certain type. While cognitive biases – which are an inherent part of our cognitive machinery - easily lead to fallacious argumentation, they affect us even when no arguments are being made. In a similar manner, the

logical validity of an argument does not mean that the person making it would be unbiased (maybe the thing being argued for simply falls within the bias), or even that the argument as a whole is sound: if could be that the facts/premises of the argument are wrong.

Already in the 1970´s, Kahneman and Tversky noticed in their studies that people have a clear tendency to use various heuristics - rules of thumb that provide a 'best guess' solution to a problem - in their decision-making in order to cope with uncertainty and complexity of their lives. Even in highly professional settings, humans have a tendency to use shortcuts in thinking rather than consider their decisions thoroughly through engaging in complex and time-consuming probability or value estimations. (Gilovich, Griffin & Kahneman 2002.)

Numerous cognitive heuristics have been identified in psychological research, and they occur on all levels of cognitive processing, from simple perception to higher cognitive functions. When perceiving visual scenes, our brain automatically looks for familiar patterns, groups similar or nearby stimuli together and interprets stimulus patterns with assumptions such as that objects being overlapped by other objects continue behind the overlapping object. Our conscious expectations of what we should see and the way we direct our attention, can further reinforce these biases. This is one reason AI can be more effective than humans at e.g. interpreting medical or radar pictures.

Examples of common heuristics that are more explicitly associated with decision making are the availability heuristic and the representativeness heuristic. The former states that humans consistently judge events that are easy to remember as more probable than ones that are less easily remembered. This is probably why people have a tendency to think of tornadoes as more dangerous than asthma, even though around 20 times more people die because of asthma than because of tornadoes (Lichtenstein et al. 1978). The availability heuristic can also take the form of illusory correlations – situations where we perceive a correlation between events when there is none or it is much weaker than we think. This can be related to remembering instances of co-occurrence as well as our own expectations of finding a correlation. The representativeness heuristic states that the probability that X is a member of class Y can be determined by determining how well the characteristics of X resemble those associated with Y. This is why upon hearing that a particular person is very shy and introverted, we might be more likely to guess that she is Finnish than Italian - even though there are well over ten times more Italians in the world, and thus probably a much larger number of Italian than Finnish introverts. (Tversky & Kahneman 1974.)

One intuitive hypothesis is that people are still rational in the sense that if they have all the relevant information, they will choose the objectively best alternative with regard to their values and goals. However, research has continuously shown that people regularly reject optimal strategies in favour of ones that 'feel better'. In one study where participants were promised money if they succeeded in drawing a red sweet from a bowl of mostly white sweets, many chose to draw from a full bowl containing 7% red sweets rather than a half-empty bowl containing 10% of red sweets. When asked about the choice, many said that even though they were aware of the lower probability of success, drawing from the bowl with a larger overall number of red sweets felt right: the sight of several red sweets had overpowered statistical knowledge. (Denes-Raj & Epstein 1994.)

The omission bias – a tendency to do nothing rather than something – is a related phenomenon. We often avoid having to make decisions that could lead to harmful consequences, even if the likelihood of harmful consequences is larger when doing nothing. In some studies, a majority of people chose to refrain from taking a vaccine involving a 5% chance of death, even with the knowledge that the chance of death was twice as big (10%) for an unvaccinated person.(Zikmund-Fisher et al. 2006) Another illustrative example of the omission bias is the number of organ donors in different countries: in countries where you have to sign up to become a donor (an opt-in procedure) the proportion of donors is often less than 50%, but in countries where everyone is assumed to be a donor unless they specifically request not to be (an opt-out procedure), the number of donors in the population can be as high as 99%. The framing of alternatives, and the procedures required to make a particular decision, can thus have a massive impact on behaviour.

Emotions can influence our decision making in several ways. One way this can happen is through prediction of future emotion. Humans have a general tendency to overestimate the negative consequences associated with a potential loss, which is one explaining factor behind the human tendency to avoid risks. Also, the positive or negative framing of a problem can have an effect on our decisions: both cancer patients, students and physicians demonstrate more positive attitudes towards a suggested treatment if its predicted results are framed in terms of the probability to survive rather than probability to die (not survive).

Immediate emotions are emotions experienced in the moment a decision is being made. They can be either integrally associated with the act of deciding itself (such as swagger or anxiety about the decision) or incidental (such as emotions related to the environment, earlier events, or the decision maker's general disposition to feel certain emotions). An illustrating example comes from studies showing that people who have been predisposed to feel sad or disgusted are willing to sell items for less than others, and that sad people are on average willing to pay more for an item than non-sad people. It has been hypothesised that these effects could be due to disgust being associated with the need to expel things, and sadness being associated with a need for change (Lemer et al 2004). Similarly, even the weather has been shown to affect our decisions, from simple everyday choices to major life decisions.

Research also shows that social factors have a big effect on decision making. Research has shown for example, that we are more likely to agree to an unpleasant request if the person making the request has previously made another, even bigger request that we have turned down. Some possible explanations are that we feel pressured to reciprocate when the other person's 'compromise' of downgrading the request, or that the previous request creates a contrast that makes the latter feel smaller (Helkama et al. 2003).

Another noteworthy phenomenon of social cognition has to do with the human tendency to in-group favouritism and, correspondingly, out-group discrimination. The mere membership in a group, even an artificial one, evokes a tendency to perceive other groups as more negative and more homogenous than one's own group, clouding rational judgement. This inclination has been confirmed in numerous studies concerning multiple nationalities and age groups. However, status- and power difference between the groups can affect these perceptions. If an out-group is perceived as threatening the existence, status, well-being, lifestyle or values of the in-group, this can give raise to feelings of fear or anger. The majority may feel that their power or safety is in danger, while the minority fears for their existence (Helkama et al. 2003.) When these biases and risks in decision-making are not recognised, in-group favouritism/out-group discrimination can dead to unfounded decision making (Gilovich, Griffin & Kahneman 2002). In maritime surveillance and SAR contexts, increasing tensions between e.g. asylum seekers and European actions could lead to drastic consequences, such as the loss of lives.

Kahneman & Frederick (2002) have, based on their research, made a distinction between two systems for decision making: and intuitive one and an alternative, more controlled one. The intuitive system relies more on immediate, unconscious and uncontrollable reactions and is to a large extent subconscious. The alternative decision-making system is more controlled, deductive, serial and rule based. Reasoning and criteria for decision-making and their logical relationships are considered in a conscious process (self-awareness). (Kahneman & Frederick 2002, p. 51-59.) It must be underlined, however, that it is impossible to eliminate intuitive components from our decision-making processes (Edelman & Tononi 2001).

In addition to the cognitive-emotional mechanisms of bias described above, the work or business environment, pressure, stress, exhaustion, hurry and many other external or internal factors influence decision-making. Many of these are something that can be controlled. Organizations culture creates the setting for decision-making processes. When setting objectives and priorities, too much power on one instance can lead to problematic consequences from the perspective of the intended outcome, especially if agreements and decisions are made in closed circuits and concealed, breeding a culture of bias in support of the status quo (Matvejeff 2009.)

Ideally, we should be able to understand and accept that each and every human being is biased in his/her thinking and behaviour. If this can be achieved and openly discussed, adjusting culture, leadership and decision making to take bias-related factors into account will become easier, which is likely to result in better decisions as well as an improved ability to evaluate past decisions critically - to minimise the effects of cognitive bias (Matvejeff 2009.)

In the table below there are identified some biases which may be relevant in surveillance and SAR contexts.

Table 12: Examples of Cognitive Biases

Confirmation Bias	We favour information that confirms our existing beliefs and discount evidence that does not conform. Confirmation bias can also affect the way we view statistics.
Attentional Bias	This is the tendency to pay attention to some things while simultaneously ignoring others.
Anchoring Bias Overconfidence Bias	This is the tendency of being influenced by information that is already known or that is first shown, 'first impression'.
Framing bias	This happens when we place too much faith in your own knowledge and opinions. We may also believe that your contribution to a decision is more valuable than it actually is.
Omission bias	This happens when we are influenced by the way in which information is presented rather than the information itself.
	The tendency to do nothing rather than to do something, for example due to the tendency to judge harmful actions as worse than harmful omissions.

6.9 Confidentiality, Privacy and Trust

Authorities on the maritime domain are obliged to keep certain information they gather via different sources as confidential. The obligation is both legal and ethical. Confidentiality establishes a foundation for trust in authorities work among citizens. It is of utmost importance to define the information that can be exchanged, with which levels of confidentiality. For example, there are separate information flows for in different operations, e.g. SAR-operations vs. border controls. Also, the information must be prioritised. The information shared may serve as a basis for decision making directly affecting human lives (which is the case in many SAR-operations) and/or their physical and moral integrity. This also means that the information must be reliable and the sources traceable from the very beginning. When a large amount of information (e.g. surveillance data) is classified as confidential, this will raise on potentially ethical dilemma. How can we be sure that information gathering and other processes on the maritime domain are ethically sustainable, if we lack transparency? Can crucial, potentially life-saving data be hidden for different reasons, when labelled as confidential? These are examples of questions that are worth examining as a part of the societal impact assessment (SIA) during the ANDROMEDA project (see also separate chapter on SIA).

Levels of Trust

For fruitful interactions to be possible, it is vital to have some basic level of trust towards one and another; trust is a base that every joint- and co-operation action is built upon. Trust is pivotal for interaction, security and safety and the actualization and functioning of a common plan. There simply cannot be safety and security, if there is no trust towards the general public, the audience, the (paying) customer or toward the performers and other staff. A simple way to estimate trust is to use the black-or-white binary pairs: 'either/or' or 'trust/distrust'. The limitation of this strategy is that it does not allow further elaborations of the trust can be given.

In general, trust is much to do with social norms. Many of them are informal, but when widely shared and accepted they become formal through a social contract. This trust can be called formalised trust. Another way of building formalised trust is with written guidelines or laws, since their very essence is to define who to trust.

The guidelines, contracts between organisations and/or laws frame the trust: they are simultaneously the base but also the limits of interaction. In addition to this formal trust, individual's personal experience set the level of trust by increasing or diminishing it based on previous experiences with other organisations and/or individuals. This, very common informal form of trust is often gained by doing things together, creating an understanding of a common language (jargon) and working methods of all involved (Probst et al. 1999).

The main difference between formal and informal trust is that the former is often forced and rarely flexible. Trust between organisations is mostly formalised, and the formal level is easily seen as the maximum. An example of this is to limit the access and communication to formal channels and methods (although sometimes organizational and technical systems set similar requirements but that should not be mistaken here). Informal trust stems from actually knowing the other and is usually stronger but more prone to fluctuation. The gap between needed level of trust, for example for cooperative use of resources, can be overcome (at least locally) by personal informal trust. In many real-life situations, informal trust is accepted as sufficient level to form joint security management. This is the case especially in areas that are seemingly most efficiently and smoothly run (Järvenpää & Majchrazak 2008).

Privacy and Surveillance

New surveillance technologies became omnipresent in our everyday live. While early research was focused on functionality of these technologies, e.g., face recognition or violence detection, latterly also privacy and transparency related work is done. While this research helps us to design systems that combine functionality and privacy, only little understanding is present how the people under surveillance will react to the new systems; average citizens do not understand technological details and they are unable to distinguish between systems with varying privacy protection. Surveillance has a bad reputation in most countries. Many surveys for understanding the acceptance of surveillance were made in special places (airports, public transport and shopping malls), but their outcome depends on recently happened events, e.g., a terrorists attack or a reported misuse of a video sequence and the underlying factors are not considered and no generic model for the acceptance exists (Krempel & Beyerer 2014).

The PARIS (PrivAcy pReserving Infrastructure for Surveillance) project (2013-2015) defined and demonstrated a methodological approach for the development of a surveillance infrastructure which enforces the right of citizens for privacy, justice and freedom (PARIS 2015). The project took into account the evolving nature of such rights, since aspects that are acceptable today might not be acceptable in the future. It also included the social and ethical nature of such rights, since the perception of such rights varies over time and in different countries. Its methodological approach was based on two pillars: 1) a theoretical framework for balancing surveillance and privacy/data protection which fully integrates the concept of accountability; and 2) an associated process for the design of surveillance systems which takes from the start privacy (i.e. Privacy-by-Design) and accountability (i.e. Accountability-by-Design).

Multi-Use of Forensic Data

In the old days, the law enforcement authorities received a warrant and went to the government monopoly Postal Telephone and Telegraph (PTT) operator for phone tapping. In the modern Internet world, it is very hard to even name the operator. They may be abroad in a regulatory paradise, and their business idea may be to give a client de facto anonymity through technical features. Today's tech savvy criminal organisation use Thor-networks, multiple prepaid SIM-cards, even submarines or aerial unmanned vehicles to avoid detection when committing crimes such as drug trafficking. Although, the police have deployed new surveillance means, in many cases, one set of means is used to detect the crime and criminals, and another set of means is for

collecting and gathering the evidence for juridical process. These sets are becoming less and less overlapping due partly to the rapid technical development and partly to the slowness of legislative process to include novel technologies into their jurisdiction.

Law enforcement agencies (LEAs), too, seek constantly new technological recording, retrieving and monitoring solutions that would facilitate their combat against organised crime. For example, satellite-based sensors and systems benefit LEAs when tracking non-cooperative targets. However, management of numerous electronic tracking devices within many simultaneous crime investigations has proven to be a very demanding task, and complications have spawned many lawsuits and negative publicity. These cases have diminished citizens' trust in a constitutional state. Another questionably practice that has been verified in participative observations is that LEAs have a tendency to create two-level systems: some that work on the streets and others that are valid in the courts of justice. Some European countries are well on their way towards this phase of development. The importance of transparency is emphasised at all EU administrative levels. However, LEAs concentrate too often on data acquisition rather than on making their operations transparent throughout. Because of the privacy protection of suspects, the investigations and data acquisition cannot be made public. However, these operations could be transparent enough to meet the citizen's criticism. To improve LEAs processes, the three main functions (crime investigation, chain-of-custody and monitoring-of-legality) should be considered together. Combining their separate information systems will avoid tripling the workload.

Monitoring-of-legality can only happen if all the data that LEA is gathering is available also to legality control and all the parties in the court. Equality in the juridical system can be in danger if there is asymmetry in the information. For example, if only LEAs have the Big Data it can be debated that they can make any case just by choosing the facts that fit the story of prosecutors. A common claim is that they cannot proved them wrong, because nobody else has access to the Big Data. It will also lead to additional benefits, such as transparency of surveillance and a new tool for achieving a balance between surveillance and privacy.

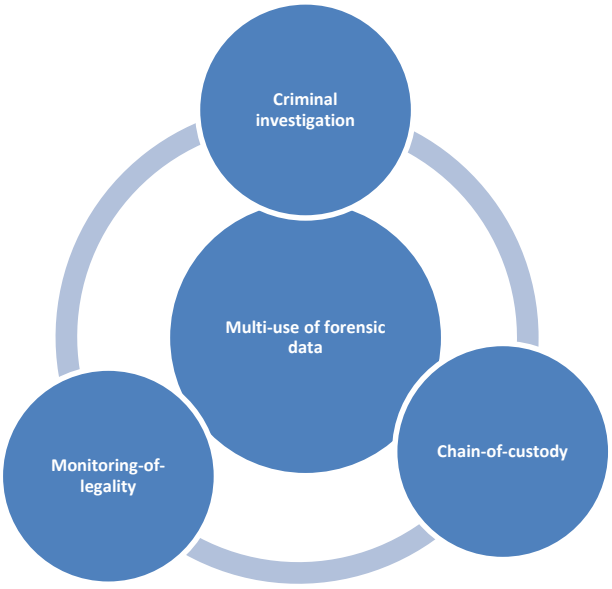

Figure 2: Multi-use of Law Enforcement Sensor Data

The figure above shows the principle of multi-use of law enforcement forensic sensor data that could be a part of the command, control and intelligence system of law enforcement. Integrating criminal investigations, chain-of-custody and monitoring-of-legality into the same system of software-intensive systems offers many advantages. One of the key strands of integrated criminal prevention policy starts with the multi-use of relevant information across sectors and borders, boosting the effectiveness and cost-efficiency of law enforcement

activity. Currently, however, the EU, national law enforcement and other public authorities are responsible for different functionalities of criminal preventions. A political, cultural, legal and technical environment should be created for enabling information sharing and multi-use between existing and future criminal investigations, chain-of-custody and monitoring-of-legality systems. The system should ensure data security, and especially information integrity and authenticity. It is also evident that the state authorities require some sort of institutionalised and standardised procedure in order to accept and trust the system. In addition, informal systems are needed to support the formal ones in order to survive the present social and political situation. According to conventional wisdom, trust is critical in such multi-use systems and procedures.

For improving law enforcement, different functions are needed, such as criminal investigation, chain-of-custody and monitoring-of-legality. All these systems and sub-systems have many stakeholders with different requirements. A modular approach (sensors, monitoring systems, and communications) means that new technologies are easy to apply, and new types of sensors can be easily included to the system. The integration of (1) investigation data, (2) digital evidence (=chain-of-custody requirements) and (3) monitoring-of-legality into the same system of systems will provides multiple applications and benefits for many stakeholders, and no triplicate work is needed. The table below summarises the main stakeholder needs, benefits, and applications of the new types of surveillance sensors, (mobile) monitoring stations and their associated communication channels for LEA operation in the field, taking into account the chain-of-custody requirements and the societal acceptance. (Rajamäki & al. 2012; Rajamäki & Knuuttila 2013).

Table 13: Stakeholders and their needs for LEA operations (by Rajamäki & al 2012)

Stakeholders and their needs/benefits/applications for LEA operations	
Stakeholder	Needs/benefits/applications
Citizens	Transparency of surveillance. Balance between surveillance and privacy. Efficient law enforcement; Value for money.
Targets	Fair, lawful, proportional and accountable surveillance.
LEAs	Better tools for the recording, retrieving and monitoring of criminal activities. Better tools and processes for cross-border operations and cooperation.
Prosecutors	Chain-of- evidence requirements.
Court of law	Chain-of-custody requirements.
Legal officers	Tools for legality control.
Legislators	Commonly agreed upon balance level between surveillance and privacy. Identification of the legal barriers to the EU-wide deployment of the system of interest.
Manufacturers and private service providers	More business opportunities by, for example, less fragmented markets and international standards.
Public service providers	More users of their services providing business continuity.
Funding agency	An efficient return on investment ratio of the solution

6.10 The Misuse of ANDROMEDA and Its Data

The term **'misuse'** refers to research involving or generating materials, methods, technologies or knowledge that could be misused for unethical purposes. Despite the fact that such research is usually carried out with

benign intentions, it has the potential to harm humans, animals or the environment. The main areas of concern regarding potential misuse could be:

1) Research providing knowledge, materials and technologies that could be adapted for criminal activities;
2) Research that could result in the development of chemical, biological, radiological or nuclear (CBRN) weapons and the means for their delivery;
3) Research involving the development of surveillance technologies that could result in negative impacts on human rights and civil liberties;
4) Research on minority or vulnerable groups and research involving the development of social, behavioural or genetic profiling technologies that could be misapplied for stigmatisation, discrimination, harassment or intimidation.

Of special concern to ANDROMEDA are the points three and four. If we move our focus from the ANDROMEDA project and its research to the proposed ANDROMEDA solution (either as part of the CISE environment or stand-alone) we can further separate the following risks to the misuse:

- The misuse of the data ANDROMEDA provides (including also military tracks)
- The use of the ANDROMEDA solution for purposes which are un-ethical and out of the scope of original purpose

The misuse of the **ANDROMEDA data** is possible if somebody who has misuse in mind will get access to the ANDROMEDA environment

- By capturing the ANDROMEDA data when it is transformed from its data sources to the ANDROMEDA platform
- By hacking the ANDROMEDA platform and its data bases
- Due to the human information leakage when somebody having access right to the ANDROMEDA data will intentionally or unintentionally deliver data to third parties.

To avoid this kind of data leakages strong focus should be set both on the design of the ANDROMEDA technology and data transfer, on user processes and access rights and finally on the governance model of the ANDROMEDA solution, including the processors and controllers of the ANDROMEDA data (see the EU Data Protection regulation discussed later).

The misuse of the whole **ANDROMEDA solution** is strongly linked to the business/adoption models of the **ANDROMEDA**, and especially as stand-alone solution. The key question is that how we can make it sure that the **ANDROMEDA** solution sold will be used only for the purposes it is mentioned. This has not so much to do with the technical features of the ANDROMEDA and their development during the ANDROMEDA project, but rather to the business and governance modelling to be applied after the project.

The term **dual-use** refers to products, services, applications, solutions etc. that can have both a military and civilian application, that is to say generally intended for civilian purposes, for example in industry, but also for developing weapons and military equipment. As such, their export is not prohibited in principle, but is subject to restrictive controls, generally in the form of a required licence. Certain dual-use goods and technologies may have a conventional military use, while others may serve to manufacture weapons of mass destruction, such as: chemical and biological nuclear weapons, as well as missiles capable of carrying such weapons.

Although ANDROMEDA has an exclusive focus on civil applications, the dual use issue will need to be addressed as a question concerning the publication of any outcome documents and envisaged exploitation of results from the project, including also future business model of ANDROMEDA.

7. Initial ANDROMEDA Societal Impact Assessment (SIA)

7.1 What is a Social Impact Assessment?

A Social Impact Assessment (SIA) is the processes of analysing, monitoring and managing the intended and unintended social consequences of planned interventions (policies, programs, plans, and projects) and social changes invoked by these interventions. SIA is, thus, more than just predicting impacts in a regulatory context; it is an active process of managing the social aspects of development. By identifying impacts in advance, better decisions can be made regarding which interventions should proceed and how they should proceed. Following this, mitigation measures can be implemented to minimise the harm and maximise the benefits from a specific planned intervention or related activity. Respect for human rights should underpin all actions. (Vancley & Esteves 2011.)

Societal Impact Assessment covers a wider perspective than traditional impact assessment focusing on economic, social and environmental impacts and impact assessment focusing on the measurement of the impacts afterwards. Further, when it comes to the risk management, SIA has a lot of common with it.

This SIA of ANDROMEDA is prepared by taking into consideration the guidelines provided by the ASSERT project. There is a minimum of 3 main impact assessment tasks during the actual project execution: 1) Initial Societal Impact review, typically during the first 6 months. This provides initial guidance and information for the developers. 2) Analysis of the requirements or scenarios defined by the project from the Societal Impact and acceptability perspective in order to provide guidance and recommendations for the developers. 3) Final Societal Impact Review. It summarises the SI issues that have been raised and how they have been handled by the project. It should also mention the potential Societal Impact issues facing the deployment of the solution. The contents of the social Impacts concern the following aspects in society (Vancley & Esteves 2011):

1) **Way of life, fears and aspirations** (how people live and interact with each other on a daily basis, their perceptions about their safety and that of their communities, and their aspirations for the future, including that of their children);
2) **Culture and community** (peoples' shared beliefs, customs, values and languages, as well as the cohesion, stability and character of their communities);
3) **Political systems** (participation in the decisions and processes that affect peoples' lives, the nature and functioning of democratic processes, and the resources available to support peoples' involvement in these);
4) **Environment** (access to clean air, water, and other natural resources, as well as the level of exposure to pollutants and harmful substances and the adequacy of sanitation);
5) **Health & well-being** (physical and mental well-being, not just an absence of infirmity);
6) **Personal and property rights** (economic effects, civil rights and liberties, personal disadvantages)

Contents are collected from the brainstorming sessions during the ANDROMEDA Kick-off Meeting in September 2019 and from Laurea networks and from Laurea Master level students of both Security, Social and Healthcare and Business.

7.2 The Barriers and Challenges Identified and the Activities Performed

In the table below, there are represented challenges identified and the corresponding activities needed to tackle the challenges. The challenges are organised from the viewpoint of ethics phenomena.

Table 14: Potential Negative Impacts and their mitigation¨

Challenge	Activities needed
(1) Justification of ANDROMEDA **>Way of life, fears and aspirations** **>Culture and community** **>Political system** **>Personal rights**	
Fear of Big Brother-type of society. People may feel suspicious and untrusting towards the ANDROMEDA technology and/or the authorities using it; concerns about ANDROMEDA representing orwellian developments that threaten the welfare of a free and open society.	We must be ambitious about data security and privacy issues – with regard to both development, technology, user processes, and business and adoption models. Transparency, accountability, and good communication are also key issues to be considered. ANDROMEDA must substantiate that it is necessary in democratic society, and its use must be proportional to the justified goals.
ANDROMEDA may have unintended negative impacts on society. Increased data fusion and awareness capability in a multi-national environment, for instance, has the potential to generate intelligence that conflicts interest between participating parties potential for increased difficulty in managing political agendas.	Ethics as a guide, continuous monitoring of the Societal impacts.
Crimes will be transferred elsewhere. Negative phenomenons might find new forms? The known and unknown evil. The use of ANDROMEDA in e.g. the Mediterranean will probably cause a displacement effect on irregular migration where people may choose even more dangerous routes to avoid being detected. Also human trafficking and smuggling of illegal goods can be affected in this way.	Getting prepared for the crimes and negative phenomenons finding new forms and places. SIA analysis is important in implementttion and as continuous process. The information sharing to border management authorities (Frontex) is also essential to develop and maintain an awareness of the big picture of the situation and to react appropriately.
ANDROMEDA toolkit not used by the stakeholders and /or it will have a bad reputation.	Conduct a good user need survey and repeat it after one year. Cultivate open communication and transparency, and collaboration with various stakeholders both during and after the project.
(2) Tension Between the Right to Security and Other Ethical / Legal Issues **>Way of Life, Fears, and Aspirations** **>Culture and Community** **>Political System** **>Health and Wellbeing** **>Personal Rights**	
The possibilities for the development of security tools (datasets, algorithms…) are balanced against other interests, such as data protection. The exploitation of ANDROMEDA's technical capacities is limited by laws and other	ANDROMEDA shall not be used identify individuals, but phenomena (e.g. terrorism) Privacy Enhancing Technologies (PET) and Privacy by Design/Default approaches shall be emohasized in the development and design of the technology and user processes.

Challenge	Activities needed
regulations – the dynamic nature of which makes it hard to predict how compliance can best be achieved and maintained also in the future. Law and ethics could 'punch holes in the ANDROMEDA tire', and even make it obsolete from the start.	Various layers of ethics shall be implemented for the different ANDROMEDA users/stakeholders, corresponding to their activities (terrorism detection and border control, fisheries control, oil spill etc.) User right limitations shall be dependant on the functional purposes of the end-user. During the pilots we can use fake data for demonstrations. So, these barriers are not barriers for the ANDROMEDA research and development, but for the future use of ANDROMEDA solution (unless the legislation will change, or the data fusion based on phenomena will be ready).
ANDROMEDA is used for border control activities in a way that is legally and/or ethically questionable, for example to deter or to block the entry of migrants or other people in distress at the sea.	The SAR communities are to be included in the user community. Their needs and requirements for the ANDROMEDA solution shall be heard and implemented appropriately.
The use or ANDROMEDA to enable border control at high seas may violate the principle of non-refoulement.	The non-refoulment issue must be discussed with CISE/EUROSUR: While there are no specific regulations on surveillance on the high seas, this should be carried out with respect for relevant international laws and especially the laws of the sea (UNCLOS; SOLAS and SAR).
Ethical issues in ANDROMEDA are linked to politics.	Lobbying/influencing political organizations.
People in distress outside a country's SAR responsibility areas (in the high seas, other countries' territorial waters) will be easier to detect, but the incentives and/or practical or legal recources to help them might be limited. Due to the information ANDROMEDA provides, 'Duty to render assistant' principle may bring more work the SAR organizations using ANDROMEDA.	When implementing ANDROMEDA, points of contact/national coordination centrals in the area ANDROMEDA covers are to be defined. In addition, a joint operation plan with all the third countries in the area is to be done before starting to use ANDROMEDA. Third countries in the sea in case should be seen as end-users of the ANDROMEDA information, as well as real partners solving the joint problem with new technology. The extension of cooperation towards third countries must be respectful of these countries' sovereignty and right to decide over their own territory.
Detection of immigrants crossing borders and detection of boats with mixed payload of humans escaping + illicit traffic of goods) > insecure situation threats from them if captured	Proper user training for end-users must be conducted concerning the decision making and when implementing the corresponding activities in practice.
Effects to the life of people living at the boarders?	Map the local regulation + code of conduct: areas where drones may fly.
Distribution rules of partner organizations may hinder the communication on ANDROMEDA business models.	Harmonization of the legislation.

Challenge	Activities needed
	How to get people to co-operate if they are not motivated for that (jealousness over the information or fear of their rights to share the information)
Sensors exeeding their limits/range?	Technical solution, e.g. limiter. Is it threthening sovereignty of a state?
(3) Differencies in ANDROMEDA usercountries in Maritime Surveillance and Land Boarders **>Culture and Community** **>Political Systems** **> Legislation**	
Ethics is case-dependent. The ethical sensitivity of the decisions made with the help of ANDROMEDA varies from case to case and context to context. For example, data protection regulation is different for crime prevention activities compared to other domains.	Ethics management and training concerning the use of ANDROMEDA in decision making. We may need various layers of ethics with ranking depending on the activities taken (terrorism detection and border control, fisheries control, oil spill etc.) Limitations depends on the functional purposes of the end-user.
Different countries have different legislations, operational needs (South vs. North Europe), and cultural environments and traditions. This may have impact both on the configuration and on user processes and training, and finally to the business models. Legal rules are not compliance in countries using ANDROMEDA. Government regulation on the activities in which ANDROMEDA will be used may hinder the use of it.	Market research early enough (as part of the business model) to be able to adapt the features of ANDROMEDA in various markets in the future/after the project. Modularity and possibility to customization and parallelization. Make a deep analysis before we begin with the demonstrations and trials. Lobbying and political influencing for synchronizing the legislation. Properly managed PR and communication and dissemination. Mapping the different practices in all the countries. Should a policy brief be done?
Failure to share information due to the conflicting priorities in maritime surveillance.	Discussion and distribution of information.
Difficulties in the sharing of classified information due to the fact that confidentiality and integrity law are not developed at a central level.	Lobbying.
End-users are not forced to share information for internal policies Will every subscribing user of ANDROMEDA equally or correctly share information? Lack of collaboration between countries> exchange of information is limited or partial.	Common rules for the collaboration as part of the ANDROMEDA governance model.

Challenge	Activities needed
An inability to share information for fear of undermining operational security/source privacy. Failure to share information due to the lack of trust.	Where ever possible, encourage or mandate the sharing of open source of information in lieu of finished intelligence products. Establish trust-building initiatives. limited exchange and storage and only with trust parties.
End-users' legacy systems are often proprietary, meaning that some of the them might not be "open" to be integrated in ANDROMEDA solution. This may induce a barrier as certain actions should be taken in order to integrate newly developed systems with the legacy ones. Different agents may have different operating models and operational cultures. How to reconcile those?	Define such barrier as early as possible in the project and collaborate with the end-users for providing the necessary interfaces. A subcontracting to the involved vendors who have developed the legacy systems might be needed.
A potential barrier is that Service Level Agreements (SLAs) might be needed to be in place in order to officially enable the cooperation and information exchange between competent maritime & land border authorities at cross-border and cross-sectorial level.	Take advantage of EMSA's role on CISE and through the transition phase and the activities undertaken by the CISE Stakeholders Group to potentially overcome such legal constraints.
(4) ANDROMEDA & Liability Issues **>Culture and Community** **>Political Systems** **>Personal Rights**	
Confidence of ANDROMEDA data>can the end-user rely on it? The fear for false positive and false negative decisions. Implementing decision support functions (behavioural analysis models) that could lead to wrong action.	Transparency of the data fusion and of the data used in it. Triangulation of the data sources. The user of DARK internet. (Machine learning in the next version).
Incomplete set of data due to ethics limitation >biased/incomplete/false analysis is risky.	Transparency of the data fusion and of the data used in it. Tackling the ethical challenges rigorously during the project. (technical solutions & lobbying)
Liability: System might not provide correct information. What happens if operation fails due to mis-information? E.g. national suspect identity data exchanged with other nations>person jailed without real reason when person entered the nation.	Operational decisions will never be made by a computer, even the most efficient one: it will always be a human who makes the final decisions. ANDROMEDA is meant to assist decision making. This is a matter to be considered by the end-users. They have to be informed regarding these liability issues in the training material.
(5) Privacy and Data Protection **>Political Systems** **>Personal Rights**	

Challenge	Activities needed
MMSI (maritime mobile service identity) > Ship > crew > person AIS-data –services may lead to storing of signal of private user Correlation of personal data with location information	ANDROMEDA architecture & technology, user processes and the governance are to be designed from the early start by applying the GDPR coming into effect 5/2017. >privacy by design and other data protection regulation to be included in the ethical requirements e.g. Replace MMSI/AIS with track number table. Anonymization, correlation only on request, delete location after a defined time. And during the trials we can operate as follows: -evaluate trials at open sea -do not store any data -use simulated data for evaluation
Identifyable persons. Algorithms to identify and track suspect targets are more efficient if they use a lot of personal data. OSINT data sources can contain several data privacy aspect. Collection and storage of personal data from social media.	Take into consideration privacy by design approach. Features cannot identify a specific person. ANDROMEDA will not be used for identification of individuals, but to the identification of phenomenon (e.g. terrorism). In general ANDROMEDA is not interested in persons (in land boarders there might be interest for persons as well?). The data fusion technology concerning the above issue is to be investigated as part of the ANDROMEDA research. And during the trials we can operate as follows: -evaluate trials at open sea -do not store any data -use simulated data for evaluation
Each country has organizations to handle data protection and ethics. How are they capacitated to understand the maritime domain?	Reinforce community this topic with relation to the maritime information. New data protection regulation comes into effect 5/2018, harmonizing a lot of the legislation.
The ethical constraints on length of personal data storage for such ANDROMEDA application may hinder the requested ANDROMEDA performance objectives.	During the trials adapt ethical constrains to end-user ethical frame where data can be collected and maintained much longer that for general application development applicable to any industry within European union.
Privacy and data protection of ANDROMEDA service/product concern both technical and organizational solutions (user processes, training, governance model and business model.) The latter may be in the real-life context after ANDROMEDA project much more complicated than during the pilots.	
Potential dangers arising from the transfer of data through CISE between countries which may also include personal data - especially to countries outside EU.	Non-classified data and filtered data exchange will be demonstrated over CISE. The personal data handled by ANDROMEDA will be described in separate PIA (privacy impact assessment).
Will the control of smuggling effect to recreational fishing?	Informing people at general level. ANDROMEDA is not interested in persons.

Challenge	Activities needed
Privacy policy, data protection (e.g. drones, video surveillance), how is the data used – can it be misused? Is the information/data collected coherent? Ethical problems could arise from an unappropriate usage of the ANDROMEDA systems if sensitive data on people on vessels or along the land border, personal images due to video streaming systems acquisition could be detected or sniffed by external systems.	Privacy by Design, Privacy Enhancing Technologies, GDPR ja LED compliance. To anonymize sensitive and visual information, to protect the exchange of information among the different situation awareness.
Person's right to check the data about oneself. The understanding of one's rights - or even the understanding of all kind of data that is collected is not clear for all the people. People are not on equal position based on their knowlede about the data collected.	Data subject rights are not relevant because ANDROMEDA will not restore/save the information (accoring to GDPR article 6 + LED).
(6) Challenges with OSINT, Big Data and AI **>Way of Life, Fears, and Aspirations** **>Culture and Community** **>Personal Rights**	
The social network contents could be complicated to manage from ethical and legal viewpoint. To which extend are we allowed to use open-source data from social media?	Data management (including the restricted time for storing). Transparency of data. Coding on the reliability based on the source?
How do we know that the data is reliable and relevant? Data is not always reliable and/or valid. > false positive, false negative situations.	Each informant needs to be evaluated for reliability. Need for having meter for that (for the adaptation of the business model).
Knowledge & informa-tion management risks. One very important issue is who watches the watchers (political issue) and how this can be carried out. Utilizing Big Data Analysis in the security domain requires intensive oversight (Broeders, et al., 2017). However, Big Data Analysis is often a 'black box', and more research is needed, especially in the phase of the analysis: selecting the algorithms,data sources and categorization, assigning weight to various data.	Adequate training for ANDROMEDA OSINT professionals in the proper management of ope3n source information in ANDROMEDA Development and implementation of European best practices for data management across all law enforcement and security services. Ensure the adoption of common data management processes, taxonomies, ontologies to enable the sharing of knowledge.
How to ensure the ethics of AI?	AI Ethical Quidelines –document as a tool.
Do authorities have adequate skills to use the system?	Proper training and feedback during pilots?
Data analysis: is all the data used, or only partly? Who will interpret the data and on what grounds? Is the data being sold (outside of EU?)	Data management plan / technical documentation + pricacy impact assessment, code of conduct, regulations. Understanding that neutral data does not exist.

Challenge	Activities needed
How is the data stored, for how long and where? Who owns the data? The data is not neutral, free of values. Ethinic profiling? Restircting the access to/right to use the data. What is the hierachy about handling the data? Who defines the parametres? How to prioritize?	
(7) Challenges with Human Decision Making **>Way of Life, Fears, and Aspirations** **>Culture and Community** **>Personal Rights**	
Information overload.	Development and application of effective needs identification and collection planning processes. Development of smarter collection systems to ensure adequate data are collected in the right time, in the right format, and for the right circumstances.
Cognitive biases: human decision making is inherently biased: various internal and external factors affect our attention and thinking, often unconsciously.	Adequate training in understanding and mitigating cognitive biases and other analytic spots. The use of a broad range of analytic techniques to identify and resolve biases, e.g. assumption surfacing, red teaming, post mortem analysis.
Difficulties to share between civilian and military services (>different regulation) in case the user serves both.	Rules & regulation on the use of data must be defined. Training as part of the ANDROMEDA implementation on necessary also from this point of view.
(8) Data Leakages and the Misuse of ANDROMEDA **>Way of Life, Fears, and Aspirations** **>Political Systems** **>Personal Rights**	
Wrong usage of data provided by other stakeholders, that might imply disadvantages of damages for someone from the strategical/economical/political perspective.	
Diplomacy issue: how to use the data that inevitably include also military tracks?	Rules & regulation on the use of data.
Lack of security> illegal usage of the system, abuse of the system, using ANDROMEDA data in DARK web Technical Information leakage: The data ANDROMEDA collects will be captured and misused e.g. for spying, military or terrorist purposes. Leak of classified information regarding criminal actions. Private or sensitive info leaking out.	Connect with EUCISE2020 network do not use the data sharing infrastructure. Specific security standards are to be followed.

Challenge	Activities needed
Human information leakage: ANDROMEDA data will be delivered to someone who should not have it	User logs as part of the system. Check and balance approach. Any information put into the system and shared through it should be traceable, in order to verify sources and their reliability when necessary.
The ANDROMEDA system or certain components of it will be sold to customers who could use it for other purposes than MS (e.g. military purposes or terrorism).	*Consortium partners and the EC together should make sure that adequate regulation, control and licensing are available for the developed system, technology or technique before it is finished and can be sold or exported.'* [40] This means that when designing the ANDROMEDA business models, proper regulation, control and licensing measures have to be taken into consideration. If ANDROMEDA technologies are used for any other operation than MS, then a special guidelines book including ethical restrictions of use should be created.
How to control the people doing the surveillance (e.g. prevent voyeurism).	ANDROMEDA code of conduct, what else? Ethical awareness of the people working among surveillance, e.g. at municipalities.
(9) The Value of ANDROMEDA for the End-users in the Long Run	
How can we make it sure that ANDROMEDA will be developed continuously based on end-user requirements and ethical/legal requirements after the project ends? By whom and how is the solution and further developing funded? Are all ANDROMEDA-services needed and relevant in the future (e.g. drones)?	Continuous development of the ANDROMEDA should be embedded in the business model from the early beginning. Being aware of the real interest of the funding agency (see below). How to ensure that the developing work will continue after the project? In the future business model there should be part where co-creation is essential part. To develop the legislation.
Due to the capacity of ANDROMEDA there is a risk that some countries choose to be free riders. They might leave the costly surveillance work and investments for other countries. This may be the case both in Europe and outside in the third countries.	Responsibilities and the moral division of labour in maritime and land boarder surveillance is to be discussed. This can include e.g. the bigger role of Frontex in some situations where the responsibilities and the amount of inputs are not in balance?
Need to change actual operating systems already in use (MS need to make investments and to buy new systems) Need to change operative subjects for adequate to all interoperability.	
Fear of decrease of jobs, e.g. people working on patrol boats.	Analyzing the real situation and it's effects? Offering adequate information to tackle the fears.
(10) The Value of ANDROMEDA for the Business Model	

Challenge	Activities needed
Is there a risk that we are developing a system, which is too expensive to use in less affluent societies?	A proper business modelling by taking into consideration various markets and their limitations and needs for various ANDROMEDA components. ANDROMEDA should be a flexible system with a scalable deployment.
ANDROMEDA solution financed by EU money prevents competition.	Good communication. ANDROMEDA is based on free competition of the research and developing funds.
IPR interests of technology partners from the viewpoint of real collaboration also after the project.	Future business model should be commented enough during the project (e.g. IPR).
Scare availability of fundamental data to developers.	Use only open data. Start a political process.
How commerzialisation will take place? The risk for being sold for unethical purposes.	Regulation, code of conduct.
Software licenses might hinder efficient development. Same is with patents. Is this a problem in ANDROMEDA?	The use of open standards and source. No patents should be held by partners. National ANDROMEDA license that can be deployed locally by the national authorities. Use of permissive SW license.
(11) Other Issues	
People say they do not care about ethics. People don't know they have ethics dots, and some are blurred?	Mandatory written ethics, practical, principles in all projects and WP's. Practical use-cases that stress the ethical issues and small brainstorming on it. Write and publish results.
Low communication between the end-users and/or developers	
Do not confuse software development with data storage.	Need to know CISE legal agreements Maximise the development of software. Manage data according to national regulations. Understand that the ethics of data before and after analysis is different.
Understanding that ethics is not only a challenge, but also a possibility.	Understanding ethics as a driver for development and value creation.
Rights of the people, refugees: are people aware of their rights? Or the data being collected?	Increase awarenes of ordinary citizens? There will be an analysisis in D2.4 of the fundamental rights in relation to ANDROMEDA.
From humanitarian point of view, border surveillance systems act more like taking care of the symptoms than preventing the origine of the migration flows.	

Challenge	Activities needed
The randomness of a human being to be born in different country/nation raise an "unfair" barrier in terms of unconditional freedom.	
Conflicts with the participants?	

In the table below are presented some positive impacts of ANDROMEDA identified during the SIA, however it must be noted that the stress and emphasis was not in these when the SIA was carried out, since the positive impacts were very well and clearly stated in the ANDROMEDA proposal.

Table 15: Positive societal impacts of ANDROMEDA

POSITIVE IMPACTS IDENTIFIED	HOW TO PROMOTE
CITIZENS	
Enhancement of security for EU citizens.	By better handling of irregular migration and human trafficking enhancing coordination and sharing of information among maritime surveillance and land border authorities and border control Agencies including cooperation as coordinated by Frontex.
SOCIETY IN GENERAL	
Positive impact on academia, industry and technology providers and companies.	Through matching requirements and capability gaps of users and promoting exploitation and collaboration.
Diminishing corruption?	
Preventing crimes	
Better structure within a country?	Possibility to use the data for "right/good" purposes.
Being better prepared for alerts during crises	
Business opportunities might increase (wider market)	Through the exploitation and standardization activities within ANDROMEDA.
NATURE	
Preventing overfishing, better environmental protection, sustaining the diversity of the nature, e.g. forest fires. Better maintenance and surveillance of the operational environment: e.g. oil catastrophes. Intensifying anticipation: e.g. nature catastrophes, accidents, protecting endangered species.	Encouraging authorities to use ANDROMEDA also for these purposes.
END-USERS OF ANDROMEDA	
Technology enables eliminating human beings from dangerous tasks.	

POSITIVE IMPACTS IDENTIFIED	HOW TO PROMOTE
Common shared system eliminates the need for several different solutions –> saves money. Data available for all.	
Better performance, better snapshot and improved resource management: control of smuggling, illegal immigration, rescue operations, customs.	
Sharing the resources: more effective use and allocation of the resources. Better use of devices.	
IMMIGRANTS	
More effective rescue operations	

8. Initial ANDROMEDA Ethical Requirements

The initial ethical requirements for ANDROMEDA solution and its development are presented below in the form of a table. They are defined by taking in to account corresponding requirements defined in the MARISA project and complementing these requirements with the ethical requirements emerging from the Land Border domain.

These requirements are aiming to create a solution which is sustainable from ethical, legal and societal points of view. The list will be a living document until the end of the ANDROMEDA project. The categories and classifications used in the table are explained below.

Table 16: Categories used in the Ethical Requirments

Importance of the requirement:	**Type of requirement**
Essential	(ethical) Awareness during ANDROMEDA project
Important	(ethical) Activity -"-
Desirable	
	(ethical) technical feature of ANDROMEDA solution
	(ethical) user process feature -"-
	(ethical) business model feature -"-

GENERAL REQUIREMENTS FOR ANDROMEDA DEVELOPMENT AND ETHICAL AWARENESS[18]	**TYPE**
EG1: Take ethics and societal challenges seriously; concerning both technology, user processes, and business/governance model, including information management.	***Essential*** *Awareness*
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.	***Essential*** *Awareness*
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.	***Essential*** *Activity and Governance/Business Model Feature*
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)	***Essential*** *Activity and Adoption/governance Business Model Feature*
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	***Essential*** *Awareness and Activity*

[18] 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.

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.	
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	***Essentia**l Activity and Essential Adoption / Governance Model Feature*
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.	***Essential** Activity and Governance Model Feature*
EG8: Adopt common data management processes, taxonomies, and ontologies to enable efficient sharing of knowledge. This includes the implementation of European best practices for data management across all law enforcement and security services. >(availability, confidentiality and integrity)	***Essentia**l Activity*
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)	*Important Activity and **Essential** in Exploitation.*
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.)	*Important Activity*
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)	*Desirable Activity*
EG12: Include SAR people in the user community: their needs are as important for ANDROMEDA as everyone else's.	***Essential** Activity*
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.	*Important Activity and **Essentia**l Exploitation*
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)	*Important Activity and essential Business Model Feature*
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.	*Important Activity*

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.	*Essential Activity*
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?)	*Important Feature*
EG18: Update current societal/surveillance impact assessment (SIA) to secure that ANDROMEDA is compliant with ethics and legislation.	***Essential** Activity and Governance/Business model Feature*
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/ pseudo-nymisation, 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.	***Essential*** *Technical Feature*
ET9: Specific security standards are to be followed up to the EU restricted level.	***Essential*** *Technical Feature*
ET10: A vast array of analytic techniques to identify and resolve biases, (e.g. assumption surfacing, red teaming, post-mortem analysis, etc) is encouraged.	*Interesting Technical Feature*
ET11: The quality of data is to be investigated both automatically and manually when first transferring it as well as in each use case.	***Essential*** *Technical and User Processs Feature*
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: • 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.	***Essential*** *Technical Feature*
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	*Interesting Technical Feature*
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.	***Essential*** *User Process and Technical Feature*
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.	***Essential*** *User Process Feature*
EP3: Adopt the check and balance approach to avoid data leakages and mis-use of it.	***Essential*** *User Process Feature*
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	***Essential*** *User Process Feature*

& privacy) 2) OSINT and the dual roles of the users are ethically challenging. 3) the inherent biases in cognitive processing are relevant to recognize	
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.	***Essential** User Process Feature*
ADOPTION/GOVERNANCE/BUSINESS MODELS (in the future)	
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.	***Essential** Governance/Business Model Feature*
EB2: Ethical (economic, social, environmental) sustainability is a part of the MARISA 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.	***Essential** Governance/Business Model Feature*
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.	*Important Business Model Feature*
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.'	***Essentia**l Business Model Feature*
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.	***Essential** Business Model Feature*
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.	***Essential** Adoption Model Activity*
EB7: It is essential for ethical compliance that the following activities are performed in each ANDROMEDA environment: - Defining a Social Media Strategy - Defining an explicit legal Duty of Care, including external reviews - Audits of Big Data and AI components	***Essential** Adoption/Busines Model Feature*
EB8: Ethics management and training concerning the use of MARISA in decision making must always be included in the business model. (training during each new implementation)	***Essential** Business Model Feature*

9. Initial ANDROMEDA Code of Conduct

The values and principles discussed in the previous sub-section form the fundamental ethical framework for ANDROMEDA as well as its user guidelines and business and adoption models. These principles are summarised in the ANDROMEDA code of conduct', which can be found below. This Code of Conduct is designed for end-users, decision makers and developers of ANDROMEDA. It establishes 9 points of principles which should be taken into consideration when deploying, using and developing ANDROMEDA solution.

When applying these principles in specific user community contexts, they are to be further specified and integrated into other existing codes of conduct.

9.1 The Justification of ANDROMEDA is Based on Ethical Grounds

The adoption of new Maritime and Land Boarder Security Surveillance technologies in border control and other such activities easily gives rise to tension concerning fundamental and human rights such as the rights to freedom, security and justice. ANDROMEDA is no exception to this. It is therefore vital that its use can be justified on ethical grounds: ANDROMEDA must respect fundamental rights and other applicable legislations, regulations and values. An ethically conscious approach is important also to enable the sustainable competitiveness of ANDROMEDA and its various components.

The challenges – but also opportunities - stemming from numerous ethical, societal and legal viewpoints have implications on both the technology and user processes of ANDROMEDA, as well as on decision making and the future governance and business models of ANDROMEDA. Establishment of a dynamic review process of the system in order to take into account the evolving technologies in this area as well as future changes in the legal and ethical framework is essential.

ANDROMEDA does not endorse any operations not strictly adhering to regulations. It is also required that a context-specific Societal Impact Assessment (SIA) is conducted as part of each implementation of the solution, and the use of sunset provisions (3-5 years) is recommended.

9.2 The Humanitarian Imperative and the Rights of the People at Land Boarders and Sea

Duty to Render Assistance is the hallmark of SAR regulation. ANDROMEDA will drastically improve the response and intervention capacities of European SaR services and personnel, severely reducing the expected number of casualties in the Mediterranean. Furthermore, early detection of anomalies allows interventions to occur before an incident that would require a SAR operation does. This will save lives at sea.

The human rights and dignity of the people at sea and at boarders need to be respected, regardless of their origin or nationality. The information ANDROMEDA collects should not be used for discrimination or other such unethical purposes.

Non-refoulement is a core principle of international refugee law which means that a refugee should never be returned to a country where they face threats to their life or freedom. ANDROMEDA enables an effective identification vessel on high seas and even on the territorial waters of third countries. It is therefore technically possible that ANDROMEDA will be used to enable to organise border control outside countries' own borders and to redirect intercepted migrants to the coasts of third states. One key challenge for ANDROMEDA is to prevent the creation of such processes.

9.3 Moral Division of Labour in Maritime Surveillance and SAR

ANDROMEDA provides improved Marine and Land Border Surveillance awareness and capabilities for more effective and efficient decision making. It is possible that this new technology will affect the division of labour between EU member states; some states might become free riders regarding with surveillance activities. Responsibilities between member states and the moral division of labour in surveillance should be discussed.

States enjoy sovereignty in their coastal waters. 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.

9.4 Value for End-users Involvement

Providing improvements in situational awareness, ANDROMEDA is likely to result in changes in the daily work routines of different end-user groups (e.g. coast guards and SAR teams), as they will have more time to plan and to act proactively. Thus, it is important that end user communities are involved in the ANDROMEDA development also after the ANDROMEDA project. Different actors (SAR, border control, fisheries control, customs, environment, general law enforcement) should be involved in active collaboration from top management to operative actors.

The ethics training of operational personnel is a necessary part of the implementation ANDROMEDA technology.

9.5 Transparency, Liability and Human Decision Making

AI systems can be used to empower human beings, allowing them to make informed decisions. At the same time, mindfulness of the associated risks is to be emphasised and proper oversight mechanisms must be established. This can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches.

Both the data and the system shall be transparent. This can be achieved with the help of traceability mechanisms. 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.

Any decisions on Maritime and Land Border Surveillance and SAR must always be made by the competent human decision makers - computer systems such as ANDROMEDA can only have an assisting role in operational decision making.

A relevant question is also that what is the general awareness of different information collecting systems that citizens are aware or can be expected to be aware.

9.6 Privacy and Data Protection

Privacy and data protection measures must be embedded in the ANDROMEDA technology so that compliance is achieved with both the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). ANDROMEDA Procurement Strategies/Adoption Models and Training material in turn provide guidelines for organizational arrangements to ensure data protection. ANDROMEDA technology, shall

respect, throughout its life cycle, 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. Furthermore, a Data Protection Impact Assessment (PIA) is a compulsory part of each ANDROMEDA configuration and business model, including establishment of clear lines of responsibility, where each agent dealing with data is responsible for ensuring appropriate levels of protection.

Privacy of people at the sea or at the boarders, especially of those in a vulnerable position (e.g. refugees, victims of human trafficking), must always be protected when ANDROMEDA technology and information is used and available. Sensitive ANDROMEDA data should never be used for media purposes. It is also important to keep in mind that non-sensitive data may become sensitive following their transmission to another user, if this user holds other relevant information that can be combined with the data exchanged.

9.7 Data management and organizational arrangements and part of ANDROMEDA solution

Data management and organizational arrangement are essential related to the privacy and data protection but also to other legal and ethical aspects, such as IPR's.

Create as part of each ANDROMEDA implementation a data 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.

Perform an explicit legal Duty of Care before utilizing any Big Data or Artificial Intelligence (AI).

9.8 Robustness, Accountability and Learning

AI systems must be resilient, secure accurate, reliable and reproducible. A fall-back plan must be in place to ensure safety in case something goes wrong.

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. (Moreover, adequate an accessible redress should be ensured.) Conducting external reviews and audits concerning the analysis of Big Data and the use of Artificial Intelligence (AI) is essential.

Accountability and learning must be embedded in the functionalities, and proper user guidelines of ANDROMEDA shall be provided. Transparency and on the accountability of ANDROMEDA and its information management and use must be prioritised.

9.9 Respect the privacy and rights of the people living near land boarders

This means mapping the local regulation, e.g. concerning the areas where drones may fly.

ANDROMEDA is not used to identify individuals but phenomenons. Respect requires increasing the awareness of practices, regulations and rights of the people among ordinary citizens so that they have a chance to know what might be done around their neighborhood and what all is allowed.

Respect for privacy and rights requires people working among surveillance to have ethical awareness.

Feedback is welcome and addressed.

10. Summary and Conclusions

In ethics, question is often more important than the answer. This is because for someone to raise a question, he or she had to ponder it first in his or her mind, thus ethical thinking had to happen. And only when thinking first, ethics can materialise into action.

Therefore, on one hand, this deliverable aims to help ask questions. All in ANDROMEDA, and others interested in maritime and land border security, should be interested in the ethical and legal dimensions. This is due to the fact that only legal but also ethically sustainable and societally acceptable solutions and practices can survive in the long run. Thus, if someone aims to deliver anything long lasting and remarkable ethics must be taken seriously and put into action.

One the other hand, it is not realistic or even meaningful that everyone is equally interested in legal and ethical questions. Understanding of the necessity is often enough. For that reason, this deliverable gives tangible instructions on how ethics and legalities are taken into account in ANDROMEDA. These are the ethical requirements: 21 general ethical requirements, 13 requirements specifically for the technology, five for user processes and training material, and eight requirements for adaptation and business/governance models. It must be taken into account that this list lives during the project as more detailed information, for example, on the data sources, sensors and legacy systems is collected and analysed. Further, ethics never ends, nor does technical advancement, so there might be changes or adjusts in the existing requirements, too.

Perhaps, above is also the justification for the initial Code of Conduct of ANDROMEDA that is described in this deliverable. This code contains of nine ethical and moral principles according which ANDROMEDA, both the project and the results, is done. In short this deliverable ensures that ANDROMEDA' justification is based on ethical grounds, the project follows humanitarian imperative, takes into account the moral division of labour, stress the importance of value creation, aims to ensure transparency, liability, and human decision making, protects privacy, emphasises data management and quality, and last but not least respects the rights of people.

11. Annex B: 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.

11.1 Reviewers

Project Coordinator	Mrs. Athena Foka
Management Support Team Member	Mr. Alkis Astyakopoulos
Internal Peer Reviewer	Mr. Giovanni Barrone, Ms. Georgia Melenikou

11.2 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

11.3 Consolidated Comments of Quality Reviewers

General Comments	
Deliverable contents thoroughness	Reviewers comment: Yes, even the structure of the deliverable can reveal the thoroughness of the deliverable's content. Author's reply:
Innovation level	Reviewers comment: Yes, high innovation level in full correspondence to the innovative character of the entire ANDROMEDA project. Author's reply:
Correspondence to project and programme objectives	Reviewers comment: Yes, there is correspondence to the entire project's and programme's objectives. Author's reply:
Specific Comments	
Relevance with the objectives of the deliverable	☒ Yes ☐ No ☐ Partially ☐ Not applicable Reviewers comment: Author's reply:
Completeness of the document according to the its objectives	☒ Yes ☐ No

	☐ Partially ☐ Not applicable Reviewers comment: Author's reply:
Methodological framework soundness	☒ Yes ☐ No ☐ Partially ☐ Not applicable Reviewers comment: Author's reply:
Quality of the results achieved	☒ Yes ☐ No ☐ Partially ☐ Not applicable Reviewers comment: Author's reply:
Structure of the deliverable with clear objectives, methodology, implementation, results and conclusions	☒ Yes ☐ No ☐ Partially ☐ Not applicable Reviewers comment: Author's reply:
Clarity and quality of presentation, language and format	☒ Yes ☐ No ☐ Partially ☐ Not applicable Reviewers comment: Few formatting issues to be checked before the submission like the logo or the contrast of some text in some tables. Author's reply:

Detailed Comments (please add rows as appropriate)		
No.	**Reference**	**Remark**
1	Page 16	The image at page 16 has to be updated
2	Page 4	Any reference to OSINT should be removed, as far as we know, no partner manages OSINT data
3	Page 55	Should a section named like 6.3 Illegal Smuggling activities (including goods and people?) be added before the section 6.4 Irregular Immigration and the Surveillance of National Borders?
4	Page 62	Document management system such as Alfresco and MARISA website. This should be changed to Sharepoint and ANDROMEDA Website.
5	Page 83	The requirements inherited from MARISA are, in this context and to all effects, the requirements of

		ANDROMEDA. To remember that these are requirements imported from another project, would it be better to add a column? "Imported Req. From MARISA" (Yes / NO)
6	Page 84	Is there any ANDROMEDA Adoption Model?

