Maritime Integrated Surveillance Awareness (MARISA)

Grant Agreement No.740698

MARISA LEGAL, ETHICAL AND SOCIETAL ASPECTS (FINAL VERSION)

Deliverable Identifier:	D2.13
Deliverable Date:	25/06/2019
Deliverable Version:	1.3
Author:	Sari Sarlio-Siintola (LAUREA)
Dissemination Level:	Public

This work was performed within the MARISA Project, with the support of the European Commission and the H2020 Program, under Grant Agreement No.740698

Document Control Page

Title	MARISA legal, ethical and societal aspects (Final version)	
Version	1.3	
Deliverable Number	D2.13	
Work-Package	WP2	
Status	□ Draft ☒ Consortium reviewed ☒ Peer reviewed ☒ Quality Assurance Team reviewed ☒ Project coordinator accepted	
Author(s)	Sari Sarlio-Siintola	LAU
Contributors	Pekka Matvejeff	LAU
	Jyri Rajamäki	LAU
	Saara Siintola	LAU
	Laura Tarkkanen	LAU
	Ilkka Tikanmäki	LAU
Peer Reviewers	Paolo Salomone	LDO
	Tilman Selig	PLATH
	João Pastor	INOVAWORKS
Date of delivery	25/06/2019	
Dissemination level	☒ Public □ Confidential, only for MARISA Consortium (including EC) □ EU-Restricted	
Security Assessment	□ Passed □ Rejected Comments:	

Version History

Version	Date	Description	Edited by
0.1	20.6.2018	Table of content and contents from D2.6	Sari Sarlio-Siintola
0.2	31.12.2018	First contributions from partners to SIA and ethical requirements	Sari Sarlio-Siintola
0.3	28.02.2019	Version for MS5 meeting including feedback from coordinator and partners to ethical requirements and to SIA, as well as new chapter on values, principles and norms and a subsection on MARISA code of conduct	Sari Sarlio-Siintola
0.4	05.05.2019	Full version including updated legal framework, CISE framework, as well as contents from EU AI guidelines and on biased decision making	Sari Sarlio-Siintola
1.0	21.05.2019	Full version for peer-review, including comments from partners	Sari Sarlio-Siintola Saara Siintola
1.1	10.06.2019	Peer-reviewed version	Sari Sarlio-Siintola Saara Siintola
1.2	19.06.2019	Partners' final comments to Code of Conduct and to Ethical Requirements	Sari Sarlio-Siintola
1.3	25.06.2019	Updated status of ethical requirement MARISA-T13/U1. Editorial changes	Sari Sarlio-Siintola

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1. Purpose of the Document

The purpose of this deliverable is to help MARISA developers, end users, and business/adoption modellers take into consideration legal, ethical and societal dimensions of the proposed MARISA solution (MARISA GA 2017).

The sea is an important source of both pleasure and prosperity that touches each of us in various ways. It plays a substantial part in climate regulation, oxygen production and is hugely important for the well-being of the planet’s ecosystem. From a societal perspective, its role expands from recreational activities such as swimming, sailing and relaxation to economical ones such as energy production, aquaculture, fisheries, sea-related tourism and shipping. In order to maintain a thriving society, it is thus of utmost importance that the seas are protected from illicit and destructive activities, be it ecosystem destruction or safety-related concerns such as the transport of illegal goods, other black-market activities, human trafficking, irregular migration, or emergencies taking place at sea.

In order to combat security threats and other challenges at sea, it is essential to maintain a comprehensive understanding of activities associated with the marine environment that could impact upon security, safety, economy or environment. This maritime awareness enables the relevant authorities to monitor and manage situations, events and actions related to the maritime domain in a comprehensive way (COM 2009). The aim of MARISA is to improve information exchange, situational awareness, decision making and reaction capabilities of maritime security communities by providing a data fusion toolkit that utilises various heterogeneous and homogeneous data.

However, not anything goes when it comes to security research and technologies. A thorough ethics appraisal procedure is an integral part of all activities funded by the EU from beginning to end, and ethical compliance is seen as pivotal to achieve real research excellence. The mandatory ethical assessments shall not be viewed merely as legitimizing tools of ‘ethics approval’, but as critical correctives to be put into action (Leese et. al. 2019). In the context of MARISA, an ethically informed approach is needed to enable the societal, economical and legal sustainability of the solution, its governance and business models, user processes and decision making. MARISA has implications for not only safety and security related activities, but also for the fulfilment of e.g. various other fundamental and human right and can and should be used to promote them. By integrating ethics into MARISA from the beginning we are seeking not only to prevent and minimise any ethical risks, but also to maximise the benefits of the solution to society as a whole.

The structure of this deliverable is as follows: in chapters two through four, an overview of the legal framework of MARISA is provided, beginning with a big picture description of the relevant principles and norms, and ending with more detailed descriptions of the legislation concerning border control, information sharing, privacy and data protection. In chapters five, we dive deeper into the practical approaches for implementing requirements set in the data protection legislation. In chapters six and seven, the central challenges of MARISA in light of the legal framework, including challenges related to OSINT, Big Data and Artificial Intelligence, are discussed.

Chapter eight contains a Societal Impact Assessment (SIA) for MARISA: the focus is on identifying, analysing, monitoring and managing the intended and unintended social consequences, risks and change processes brought about by MARISA. The main emphasis is put on the maritime surveillance operations which are currently most ethically laden, namely border control, search and rescue and the operations around irregular immigration.

Finally, in the ninth chapter, we present a checklist of ethical requirements and a MARISA Code of Conduct. The chapter essentially summarises the ethical framework for MARISA, including its development, deployment and use.

The MARISA Social Impact Assessment, MARISA ethical requirements, and the MARISA Code of Conduct have their basis in both desktop studies on ethical and legal frameworks, and in collaborative workshops on societal challenges.

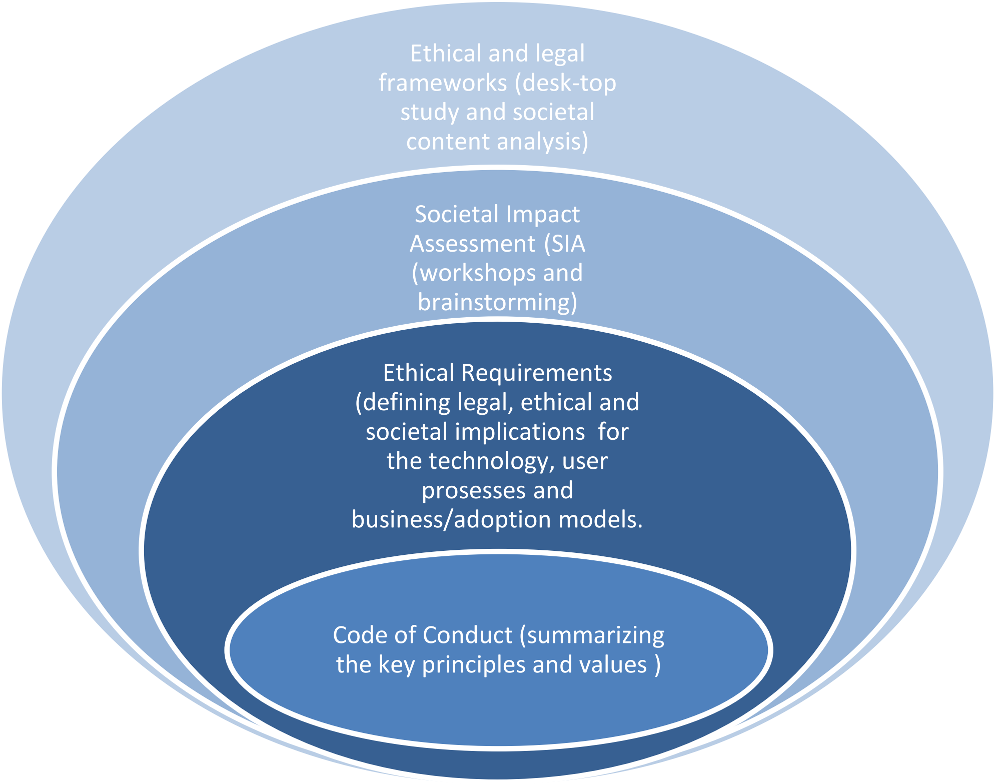

Ethical and legal frameworks (desk-top study and societal content analysis)
Societal Impact Assessment (SIA (workshops and brainstorming)
Ethical Requirements (defining legal, ethical and societal implications for the technology, user prosesses and business/adoption models.
Code of Conduct (summarizing the key principles and values)

Figure 1: The approach to MARISA ethics analysis

1.2. References

Project Reports

ASSERT (2014). ASSSERT Toolkit for Societal Impact Assessment in Security Research. Retrieved from: http://assert.maisondx.com/. (Accessed 15. May 2019).

EUCISE (2015). The Development of CISE of the Surveillance of the EU Maritime Domain and their related impact assessment.

MARISA GA (2017). MARISA Grant Agreement.

MARISA (2017b). Legal, Ethical and Societal Aspects D2.6. (An internal document).

MARISA (2018a). MARISA Adoption Models D2.3.

MARISA (2018b). User Community Report D2.1.

MARISA (2019a). Overall Architecture D3.6.

MARISA (2019b). Service Description D3.7.

MEDI@4SEC (2016a). Ethics and Legal Issues Inventory.

MEDI@4SEC (2016b). Descriptive Framework for Analysis of Social Media Use.

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

PERSEUS. Overview report on trans-national and European law and regulation relative to maritime border control. D13.2.

PERSEUS. Report on national and international political dimensions of developing, financing and implementing maritime border security. D13.4.

PERSEUS. Report on relevant legal, ethical and rights issues on data collection, retention and transmission. D13.5.

RANGER (2016). Societally acceptable and ethically sustainable way of performing MS. D5.3.

SAPIENT (2012). Supporting fundamental rights, privacy and ethics in surveillance technologies (SAPIENT). Deliverable 1.1. Smart surveillance – Stated of the Art, 23 January 2011.

SUNNY (2014). Deliverable 1.4: Surveillance societal and Ethical Aspects. Project co-funded by the European Commission within the Seventh Framework Program.

SURVEILLE (2015). Deliverable D4.10 Synthesis report fromWP4, merging the ethics and law analysis and discussing their outcomes.

VIRTUOSO (2011). Privacy Impact Assessment PIA 3.1.1.

VIRTUOSO (2012a). Analysis of the legal and ethical framework for open source intelligence.

VIRTUOSO (2012b). Code as Code assessment v1.0.

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.

COM (2010). European Commission: Overview of Information Management in the area of freedom, justice and security. 385 final.

CVRIA (2008). Case c-91/05 Commission v Council. Judgement of 20 May 2008.

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 (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.

EU (1725/2018). Regulation of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

EU (458/2017). Regulation No 2017/458 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at the external borders.

EU/PROPOSAL (2018). Proposal for a Regulation of the European Parliament and of the Council on the European Border and Coast Guard and repealing Council Joint Action n°98/700/JHA, Regulation (EU) n° 1052/2013 of the European Parliament and of the Council and Regulation (EU) n° 2016/1624 of the European Parliament and of the Council - Mandate for negotiations with the European Parliament.

EU-LEX. Glossary https://eur-lex.europa.eu/summary/glossary.html.

European Council (2014). Strategic Agenda for the Union in times of change 26/27 June 2014.

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

[29] EUROSUR (2013). Regulation No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (EuroSur).

EUROSUR HB (2015). Annex 1 to European Commission Recommendation adopting the Practical Handbook for implementing and managing the European Border Surveillance System C (2015) 9206 final, 15.12.2015.

FRONTEX (2015). Frontex Report to the European Parliament and the Council on Art 22(2) of Regulation (EU) No 1052/2013 – The functioning of EuroSur. Warsaw 1 December 2015.

FRONTEX (2016). Regulation 2016/1624 of the European Parliament and of the Council of 14 September 2014 on the European Border and Coast Guard and amending regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC.

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).

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).

SBC (2016). Regulation No 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code).

CIES (2012). Societal Impact Expert Working Group EC DG ENTR Report. CIES. Available from: http://cies.ie/wp-content/uploads/2014/05/Report-of-the-Societal-Impact-Expert-Working-Group.pdf. (Accessed 15. September 2017).

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).

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

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

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 17th of November 2016).

Antignac, T. & Le Métayer, D. (2014). Privacy by Design: From Technologies to Architectures. In: *Privacy Technologies and Policy*. Cham: Springer, pp. 1-17.

Broeders, D., Schrijvers, E., van der Sloot, B. & van Brakel, R. (2017). Big data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data. *Computer Law & Security Review* (33) 309-323.

Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*, Ontario: Information and Privacy Commissioner of Ontario.

Chen, K., Qiao, F. & Wang, H. (2016). Correlation Analysis Using Global Dataset of Events, Location and Tone. *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*, pp. 648-652.

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.

Colesky, M., Hoepman, J.-H. & Hillen, C. (2016). *A critical analysis of privacy design strategies*', Procs. IWPE'16, IEEE, 33–40.. 2016 IEEE Security and Privacy Workshops (SPW), pp. 33-40.

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.*

Fiott D & Linström G (2018). Artificial Intelligence. What Implications for EU security and defence? European Institute for Security Studies (EUISS).

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.

Glasgow, K. (2015). Big data and law enforcement: Advances, implications, and lessons from an active shooter case study. In: *Application of Big Data for National Security*. Waltham: Butterworth-Heinemann, pp. 39-54.

Glassman & Kang (2012). Intelligence in the internet age: The emergence and evolution of OSINT. *Computers in Human Behavior* (28) 673-82.

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

Guo, L. & Vargo, C. (2017). Global Intermedia Agenda Setting: A Big Data Analysis of International News Flow. *Journal of Communication*, pp. 499-520.

Hayes, B. & Vermeulen, M. (2012). *Borderline - The EUs new Border Surveillance Initiatives: Assessing the costs and fundamental rights implications of EUROSUR and the smart borders proposals.* Heinrich Böll Foundation.

Hoijtink, M. (2014). Capitalizing on emergence: The ‘new’ civil security market in Europe. *Security Dialogue*. Vol 45(5), p. 458-475.

Hu, E. (2016). Responsible Data Concerns with Open Source Intelligence. Available from: https://responsibledata.io/2016/11/14/responsible-data-open-source-intelligence/. (Accessed 19. April 2019).

ICO (2014). *Conducting privacy impact assessments code of practice*. The UK Information Commissioner’s Office. Available from: https://iapp.org/resources/article/conducting-privacy-impact-assessments-code-of-practice/. (Accessed 19. April 2019).

Jain, P., Gyanchandani, M. & Khare, N. (2016). Big data privacy: a technological perspective and review. *Journal of Big Data.*

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.

Koops, B-J., Hoepman, J-E. & Leenes, R. (2013). Open-source Intelligence and privacy by design. *Computer Law & Security Review* (29) 676-688.

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

Kung, A. (2014). PEARs: Privacy Enhancing Architectures. In: *Privacy Technologies and Policy*. Springer, pp. 18-29.

Leese, Liden & Nikolova (2019). *Putting critique to work: Ethics in EU security research. Security dialogues* Vol. 50(1) 59-76.

Lerner J. S. & Small D. A. (2004). Lowenstein G: Heart strings and pulse strings: Effects of emotion on economic transactions. *Psychological Science.*

Lichenstein S., Slovic P., Fischoff B., Layman M. & Combs B. (1978). Judged frequency of lethal events. *Journal of Experimental Psychology*.

Mannermaa M. (2007). Living in the European Ubiquitous society. *Journal of Future Studies*. Report 105.

Marin, L. (2013). Protecting the EU's borders from …fundamental rights? In R Holzhacker & P Luif (eds.): *Freedom, Security and justice after Lisbon*. New York: Springer.

Martín, Y. S. & Kung, A. (2018). *Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering*. 2018 IEEE European Symposium on Security and Privacy Workshops, pp. 108-111.

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.

Matturdi, B., Zhou, X., Li, S. & Lin, F., (2014). Big Data security and privacy: A review. *China Communications*, pp. 135-145.

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

Moallem, A. (2019). Perspectives on the future of human factors in cybersecurity. In: *Human-computer interaction and cybersecurity handbook*. Boca Ratom: CRC Press, pp. 353-366.

Nelson, B. & Olovsson, T. (2016). *Security and privacy for big data: A systematic literature review*. 2016 IEEE International Conference on Big Data (Big Data), pp. 3693-3702.

Panizza, R. (2018). *European Parliament Fact Sheets on the European Union*. The principle of subsidiarity. Available from: http://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.2.pdf.

Passos dos (2016). Big Data, Data Science and their contributions to the developnment of the use of open source intelligence. *Systems & Management* (11), 3392-396.

Probst, G., Raub, S., Romhardt, K. & Doughty, H. (1999). '*Managing knowledge: Building blocks for success'.*

Podbregar, I. (2016). 'Some Counterintelligence Dilemmas', in I. Podbregar, & T. Ivanuša, *The Anatomy of Counterintelligence: European Perspective*, Sharjah: Bentham Science Publishers, pp 133-141.

Quilici-Gonzalez, J., Broens, M., Quilici-Gonzalez, M. & Kobayashi, G. (2014). Complexity and information technologies: an ethical inquiry into human autonomous action. *Scientiae Studia*, vol.12 no.spe São Paulo.

Rahman, F. (2017). Smart Security: Balancing Effectiveness and Ethics. *RSIS Commentary*, 14 Dec.Volume 235.

Rumbold, B. & Wilson, J. (2018). Privacy Rights and Public Information. *The Journal of Political Philosophy*.

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.

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.

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

Shorrock, S. & Williams, C. (Eds.) (2016). *Human Factors and Ergonomics in Practice. Improving System Performance and Human Well-Being in the Real World*. CRS Press.

Surveillance Studies Network (2006). *Report on the Surveillance Society*. Report to the Information Commission Office (UK).

Trottier (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critics. *European Journal of Cultural Studies* (18), 530-547.

Tversky, A. & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability (1973) *Cognitive Psychology.*

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

US Executive Office of the President (2014a). *Big data and privacy: a technological perspective*. President's Council of Advisors on Science and Technology.

US Executive Office of the President (2014b). *Big data: seizing opportunities, preserving values*.

Van Aubel, P., Colesky, M., Hoepman, J-H., Poll, E. & Montes Portela, C. (2018). *Privacy by design for local energy communities*. Ljubljana, 7-8.6-2018.

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.

Wood, M. G. (2016). *Social media intelligence, the wayward child of open source intelligence*. Available from: https://responsibledata.io/2016/12/12/social-media-intelligence-the-wayward-child-of-open-source-intelligence/. (Accessed 20. September 2017).

Wójtowicz, A. & Cellary, W. (2019). New challenges for user privacy in cyberspace. In: *Human-computer interaction and cybersecurity handbook*. Boca Raton: Taylor & Francis Group, pp. 77-96.

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. Definitions

ELSI is an approach where one anticipates and addresses the **ethical, legal and societal implications** of an activity or a project. In the context of MARISA, the ELSI are seen as both challenges and as opportunities. They are to be specified and converted into concrete requirements for the MARISA technology, user processes and governance/business/adoption models. It must be emphasised that each of the aspects – ethical, legal and societal – is important. Though legislation sets concrete minimum requirements, the investigation of legal aspects alone is insufficient, as legislation is always time-bound and obsolete in the sense that it takes time for it to adapt to e.g. technological developments. Ethics offers a perspective independent from legislation to evaluate the sustainability of MARISA and its use and is vital to ensure the political acceptability and public trust in the solution. The societal aspect finally complements these two viewpoints, putting focus on the various intended and unintended consequences of MARISA for society in the long run.

Maritime Surveillance is the set of activities aimed to understand, prevent and/or manage events and actions related to the maritime domain that could impact the areas of maritime safety and security, law enforcement, defence, border control, protection of the maritime environment, fisheries control, trade and economic interest of the EU. The aim of MARISA is to provide the security communities operating at sea with a data fusion toolkit that makes available a suite of methods, techniques and modules to correlate and fuse various heterogeneous and homogeneous data from different sources.

Personal data is any information relating to an **identified or identifiable** natural person (‘data subject’). 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. Information can fall under the category of personal data for example if it can be linked to an identifiable person through accessing a register.

Privacy by Design (PbD) is the principle that privacy should be promoted as a default setting of every new ICT system and be built into systems from the design stage. Although often used synonymously with Privacy Enhancing Technologies (PET), ‘Privacy by Design’ can better be regarded as the *philosophy behind* PETs.

Data Fusion is the process of integrating multiple data sources to produce information that is more consistent, accurate, and useful than that provided by the individual data sources alone. Data fusion is analogous to the process in the human brain where information from the different sensory modalities (sound, temperature, taste, etc) is integrated to enable the perception of a world consisting of coherent perceptual entities.

Privacy-Enhancing Technology (PET) is a system of ICT measures that protects privacy either by eliminating or reducing personal data, or by preventing unnecessary or otherwise undesired processing of personal data.

OSINT; Open Source Intelligence involves the collection, analysis, and use of data from publicly available sources. OSINT deals with any unclassified information that is generally available to the public, even if its distribution is limited or only available upon payment.

SOCMINT; Social Media Intelligence is an intelligence discipline built upon tools and solutions for monitoring and analysing information available on social media. The concept highlights social media content in particular as a challenge and opportunity for open source investigations; some scholars argue that the SOCMINT should be separated from the concept of OSINT and treated as an issue of its own.

Big Data describes exceedingly large or complex data sets with the potential to be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour analysis and prediction. Changes the way data analysis is traditionally performed and seen. It includes processes of analysis, capture, research, sharing, storage, visualization, and safety of information.

Data Science is the science of extracting knowledge from structured or unstructured data, incorporating techniques and theories from fields such as logic, mathematics, statistics, computing, engineering, and economics. It is utilised in OSINT to make up for the lack/low quality of BIG DATA, to draw the correct conclusions, capture the correct data and to have the correct perception in how to proceed throughout the process.

Artificial Intelligence (AI) refers to systems designed by humans that act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve a specific (complex) goal. AI systems can be designed to learn to adapt their behaviour through analysing how the environment is affected by their previous actions. AI incorporates several approaches and techniques, such as machine learning, machine reasoning and robotics.

Bias is an inclination or prejudice for or against something or somebody that may result in unfair or inaccurate evaluations and decisions. It is known that human cognitive processes such as perception and decision making are inherently biased. Since AI systems are designed by humans, it is possible that humans inject their biases into them, even unintendedly. Many current AI systems are based on machine learning data-driven techniques. Therefore, a predominant way of injecting bias into them is related to biases in the collection and selection of the training data. If the training data is not sufficiently inclusive and balanced, the system could learn to make inaccurate estimations and unfair decisions. On the other hand, AI has potential to help humans to identify their biases and assist them in making less biased decisions.

1.4. List of Acronyms

List of acronyms	
AI	Artificial Intelligence
AIS	Automatic Identification System
CISE	Common Information Sharing Environment
ELSI	Ethical, Legal and Societal Implications
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EUROSUR	European Border Surveillance System
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
GDPR	General Data Protection Regulation
HCI	Human Computer Interaction

IBM	Integrated Border Management
LED	Law Enforcement Directive
MS	Maritime Surveillance
OSINT	Open Source Intelligence
PbD	Privacy by Design/Privacy by Default
PET	Privacy Enhancing Technologies
SAR	Search and Rescue
SD/SDL	Service Logic/Service Dominant Logic
SBC	Schengen Border Control
SIA	Social Impact Assessment
SOCMINT	Social Media Intelligence
SOLAS	The 1974 International Convention for the Safety of the Life at Sea
UNCLOS	United Nations (UN) Convention on the law of the Sea

Table 1: List of Acronyms

1.5. MARISA in a Nutshell

The aim of MARISA is to aid the security communities operating at sea in their activities by providing them with a data fusion toolkit that correlates and fuses various heterogeneous and homogeneous data from different sources, including the Internet and Social Media. The toolkit makes available a suite of modules, methods, and techniques to get insights from any big data source. These include data analyses based on geographical and spatial presentation, analyses to identify patterns that reveal connections between events, and predictive analysis with models to represent the effect of the relationships of objects observed at sea, as well as presentation tools for navigating and visualizing results of data fusion processing. (MARISA GA 2017.)

1.5.1. The MARISA Architecture and Services

The aim of MARISA is to improve the situational awareness, information exchange, decision making, and reaction capabilities of the maritime security communities. The starting point for the design of the MARISA solution is that of an eco-system of innovation. This the integration of new actors and information providers beyond the original MARISA consortium to the MARISA solution, also at later stages, shall be easy and flexible. The MARISA Toolkit can be operated both directly, with a legacy system via an adaptor, or via an EUCISE node that wraps the legacy systems. (MARISA GA 2017.)

The architecture, services and components of MARISA are described in the figure below (MARISA 2019a; MARISA 2019b):

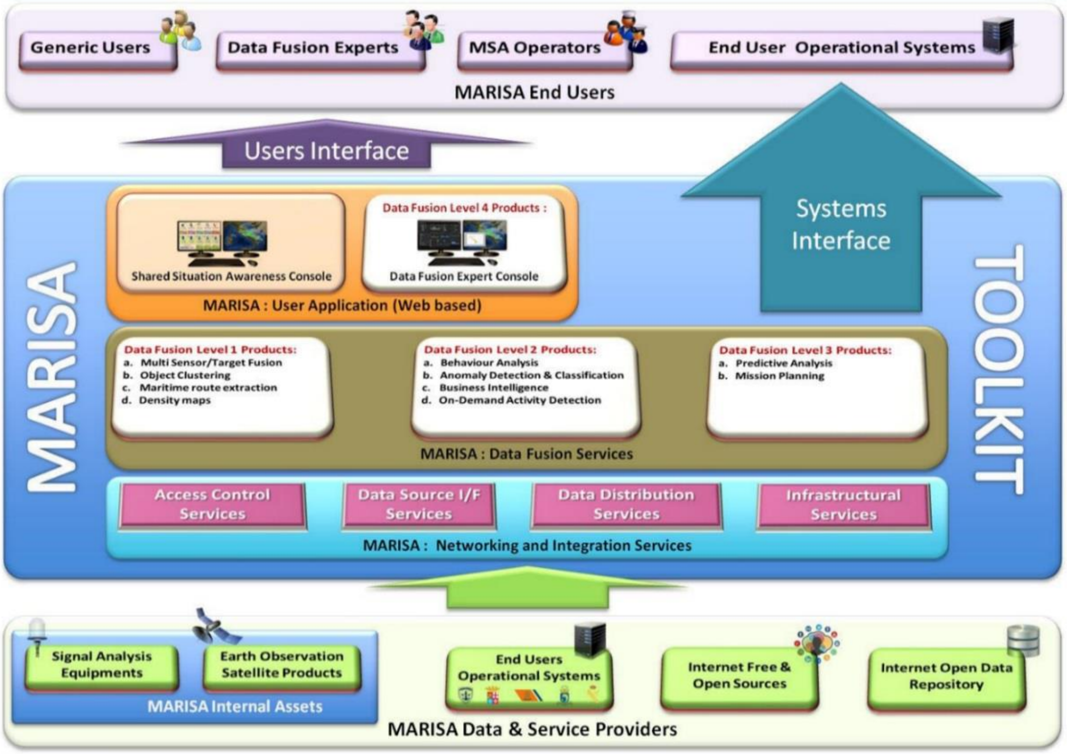

Generic Users
Data Fusion Experts
MSA Operators
End User Operational Systems
MARISA End Users
Users Interface
Systems Interface
MARISA
TOOLKIT
Data Fusion Level 4 Products :
Shared Situation Awareness Console
Data Fusion Expert Console
MARISA : User Application (Web based)
Data Fusion Level 1 Products:
a. Multi Sensor/Target Fusion
b. Object Clustering
c. Maritime route extraction
d. Density maps
Data Fusion Level 2 Products:
a. Behaviour Analysis
b. Anomaly Detection & Classification
c. Business Intelligence
d. On-Demand Activity Detection
Data Fusion Level 3 Products:
a. Predictive Analysis
b. Mission Planning
MARISA : Data Fusion Services
Access Control Services
Data Source I/F Services
Data Distribution Services
Infrastructural Services
MARISA : Networking and Integration Services
Signal Analysis Equipments
Earth Observation Satellite Products
MARISA Internal Assets
End Users Operational Systems
Internet Free & Open Sources
Internet Open Data Repository
MARISA Data & Service Providers

Figure 2: MARISA Architecture (from MARISA D3.6)

MARISA Networking and Integration Services includes the following components:

Access Control Services: services for managing access to the MARISA Data Fusion products. They concern the ability of MARISA to identify, record and manage users' identities and their related access to all the services made available by the toolkit. The services include

a) *Identity and Access Management Services* to identify all users connecting to the toolkit's services, to ensure that access privileges are granted according to defined security policies, and to make sure that all individuals and systems are properly authenticated, authorised and audited, and
b) *A User Profiling Service* to record and assign privileges to all users (human/device/process) connecting to MARISA.

*Data Source Interfaces (I/F) Services***:** for gathering data, information, and services. These could include e.g. end user legacy systems & assets, free & open internet sources, simulation sources, and assets directly provided by MARISA from external sources (i.e. Satellite Data, Signal Analysis Devices, AIS Sources). The sources feeding the MARISA toolkit are expected to be maritime data (e.g.: AIS Network, System Tracks, Mission Plans, etc.); Satellite data (e.g.: COSMO-SkyMed SAR data, Sentinel-1, Sentinel-2, commercial optical missions, etc.); Intelligence data (e.g.: OSINT, Signal Analysis).

MARISA Data Fusion Services level includes the analytics techniques and algorithms for data fusion. This level is capable of handling both structured and unstructured data, and of linking data representing different typologies and/or originating from disparate sources, to enable the different data fusion processing levels:

MSA Level 1 Processing: addresses the ’Observation of elements in the environment’ to create Maritime Situational Awareness. The main focus is on obtaining information about the geographical position of observed objects. This is achieved with the help of Data Fusion services, such as ‘Multi Sensor/Target/Common Operating Picture (COP) Fusion’, ‘Object Clustering’, ‘Maritime route extraction’, ‘Density maps’ and ‘Multilingual Information Extraction and Fusion from Social Media’.

MSA Level 2 Processing: addresses the ‘Comprehension of the current situation’ to provide useful information about the relationships between different objects in the maritime environment. The goal is to detect suspicious behaviours (particular or irregular patterns) and infer the real identity of a vessel (fishing, polluting, smuggling). This is achieved through providing Data Fusion services, such as Business Intelligence, On-Demand Activity Detection, Behaviour Analysis, Anomaly Detection & Classification, and Alarm Generation.

MSA Level 3 Processing: addresses the ‘Projection of Future States’ to predict the development of a maritime situation, thus supporting rapid decision-making and action. The goal is to predict vessels’ behaviour at sea and to support the planning of missions based on these predictions. The Data Fusion services provided on this level include e.g. Predictive Analysis and Mission Planning.

MARISA User Application level includes the computing services that allow the users to visualise the results of MARISA using of graphic and statistical presentations, based on the web-based approach. A different version of MARISA Data Fusion Products is made available for each user community of interest (e.g. generic users, data fusion experts, and MSA operators) based on the access privileges assigned to them:

The MSA Presentation Web Console enables generic users to access, analyse and visualise maritime entities in textual (dashboard) or graphical views, using a web browser as a client. Both a fused maritime picture based on a WebGIS and reference detailed cartographic map of a selected Area of Interest (AoI) are provided to increase situational awareness. The service makes it easier to detect abnormal behaviour and highlight alarms.

The System Administration Console is primary devoted to address the general management activities of the MARISA system. The console will also be used to profile and assign privileges to generic users and operational systems when accessing data fusion and HCI services.

The Service Administration console provides the interface to manage the various data fusion services included in the toolkit.

1.5.2. MARISA End Users

The end users of MARISA can be divided into four groups: Generic users, Data fusion experts, MSA Operators and End-User Operational systems. Together with other stakeholders, they represent various actors in maritime surveillance: border control, customs, defence, general law enforcement, fisheries control, and actors within maritime environment and maritime safety. (MARISA 2018.)

MARISA END-USERS AND ACTIVITIES		
End users	**Maritime aspects and**	**User benefits**

	user communities	
Generic Users Data Fusion Experts MS operators End-user Operational Systems	Border control Customs Defence General Law Enforcement Maritime Environment Fisheries Control Maritime Safety	Obtaining a multinational maritime picture to be routinely used during illegal crossings from third countries to Europe. Both national and cross-national anti-drug operations. Early warnings of smuggling, illegal immigration, terrorism, etc. before they reach a nation's coastline. Support to anti-piracy operations by improving the maritime picture in remote areas. Fisheries control & tracking malevolent operators that spoof their AIS declarations in order to enter closed areas or valuable fish stocks. Early warnings about environmental disasters.

Table 2: MARISA End-users

The process of decision making in Maritime Surveillance can be described as MARISA Pyramid Model presented in the MARISA User Community Report (MARISA 2018).

MARISA PYRAMID AS DIMENSIONAL LEVELS		
1	**Collect**	Sensor data | Multisensor data | Extended Data Sources | Social Media
2	**Process**	Detection | Radar Clutter Reduction | Data Refining and Correlation | Object Detection | Target Identification | Classification | Tracking | Target Data Integration and Fusion
3	**Fuse**	Sensor-fusion | Tracking | Data Fusion | Persistent-Tracking | Ontology Alignment | Terminology and Common Definitions | Data Models | Information Fusion
4	**Analyse**	Context | Spatial | Temporal | Interactions | Reasoning | Patterns Recognition | Anomaly Detection | Business Intelligence | Fusion of Data from Heterogeneous Co-operations | Alarm generation | Threats Analysis | Density and Risk Maps
5	**Decide Decision-making**	Expert Knowledge | Local Situational Picture | Recognised Maritime Picture | Decision Support System for Action and Domain | Human in the Loop | Action Competence
6	**Disseminate Sharing**	Authorities Co-operating | Cross-border Co-operations | CISE Services | National Service Bus | International Services | Harmonisation | Continuum of Research
7	**Act**	Inclusion of Implications and Findings into the Furthered Body of Knowledge

Table 3: MARISA Pyramid Model (from MARISA D2.1)

1.5.3. MARISA Business and Adoption Models

The MARISA solution, including all of its components, is very close to application. The components will reach the target TRL as deliverables WP4 and WP5 as follows: Networking and Integration Services TRL8, Data fusion level 1/observation and 2/comprehension TRL8, Data fusion level 3/projection of future states TRL6/7, User Application TRL7/8). The integrated MARISA toolkit will be composed iteratively in two phases and validated during the pilots.

The definition of the business model takes into account Business to Government (B2G). In addition, a broad diffusion of the service (number of possible adoptions) and the consideration of future developments and needs are necessary for a sustainable business model.

Maritime security organizations and authorities represent the primary target sector of the MARISA toolkit. The growing demand for situational awareness in security and surveillance applications worldwide is one of the key drivers for the sector. Our estimation is that there are over 400 relevant actors in this field in the EU alone. Several potential customers have already been identified: the full partners of MARISA, the EUCISE partners and some institutions members of the MARISA advisory board.

MARISA services are developed in full compliance with the CISE data model. They will be available as both, a stand-alone, configurable version to be embedded within an end user operational domain, and a version made accessible through the MARISA user interfaces. Furthermore, MARISA is available as both the full set of technologies, and as individual configurations constructed component-by-component according to needs of the different actors (security, environment, transport, shipping etc.).

The term ‘MARISA Adoption Model’ addresses the progress that is applied to drive an alignment paths of the innovative services based on the user needs and evaluate the implementations with respect to the needs. It provides an end user-centred involvement for the design, development, improvement, integration and validation responsibilities; serving as a structured path on which the harmonisation and standardisation proposals stemming from this project can be build and promotes a use of stakeholders’ action competence and knowledge in progress. (MARISA Ethics 2017) The ethical, legal and social issues described in this deliverable have a strong impact not only on the level of technical requirements, but also on the levels of adoption models as such issues are strongly connected to users and more specifically to their behaviour in decision-making contexts. One issue to be considered in particular is that the information that is exchanged in MARISA, in the context of each of the specific adoption models, meets the requirements of *availability*, *confidentiality* and *integrity*.

Another relevant factor with regard to adoption models is the existing codes of conduct for the different actors in maritime security, which sometimes differ from one jurisdiction to another and may be in conflict and therefore, if possible, need to be harmonised. The most ethically challenging context for MARISA is the border control, where ethical, political and legal tensions exist between humanitarian interest, security, and the rights of both EU citizens and migrants. In defining the various adoption models, it is therefore necessary to promote a strong user-community involvement and also to consider the social aspects of collaborative practices between users and other stakeholders.

1.6. Lessons Learnt from Other Projects

Some general insights and viewpoints to the ethics and legislation in maritime surveillance and information sharing have been provided in the context of the PERSEUS and BLUEMASSMED projects. These include:

1) The importance of clear lines of responsibility, where each agent is responsible for ensuring an appropriate level of protection for the data they handle.
2) The importance of a proper supervision mechanism over agents processing personal and/or otherwise sensitive data.
3) The need to respect fundamental and human rights in the possible exchange of information with third countries.
4) Right to the privacy and freedom of navigation
5) The importance of a dynamic review process for the system in order to take into account technological developments and future changes in the legal framework.
   (For a more detailed explanation, see MARISA Ethics 2017).

Practical tools and frameworks that can be adapted in MARISA with minor updates are provided by the VIRTUOSO and MEDI@4SEC projects. These include the privacy enhancing technologies, a legal and ethical framework for OSINT, as well as Ethical and legal challenges SOCMINT. These will be further discussed in chapter seven.

2. 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. Both international law and a broad overall view of EU law will be discussed. More specific and detailed legislation will be discussed in chapters 3 and 4.

2.1. International Law

2.1.1. 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.

The scope of subjects addressed by international law ranges from traditional topics such as war and peace and diplomacy to human rights, rules on trade, protection of the environment, maritime law, international criminal law and the protection of refugees. International agreements are often developed and negotiated within the framework of international organizations such as the United Nations (UN) or the Council of Europe. Also disputes relating to international law are typically solved with the help of such organizations. The International Court of Justice is the principal judicial organ of the UN that settles, in accordance with international law, legal disputes submitted to it by states.

2.1.2. The European Convention on Human Rights

Human rights and the idea of individuals as subjects of international law is new. For centuries, states were seen as eligible to treat their citizens as they pleased. Some of the earliest developments in human rights were the abolishment of slavery in the 19th century and the requirement of minority protection by the League of Nations after WW1, but in both cases people were treated as groups rather than individuals, and the motives were perhaps economical and practical as much as humanitarian. 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 (http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm).

2.1.3. United Nations Convention on the Law of the Sea

The general international law of the sea was long heavily dependent on customary international law. Nowadays a great deal of it is found in the United Nations Convention on the Law of the SEA (UNCLOS) - a treaty that was concluded in 1982 but entered into force as late as 1994, replacing several smaller but relatively outdated treaties. The UNCLOS 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

In addition to this, 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.)

2.1.4. International Convention for the Safety of Life at Sea

The 1974 International Convention for the Safety of Life at Sea (SOLAS Convention) in its successive forms is perhaps the most important treaty concerning the safety of merchant ships. Its fifth chapter, Safety of Navigation, however, generally applies to all ships, including yachts and other private ships, on all voyages, including local ones.

From the perspective of maritime surveillance and security, two provisions stand out. The first one is a general obligation for ship masters to render assistance, similar to the provision found in UNCLOS: '*The master of a ship at sea which is in a position to be able to provide assistance, on receiving information* ***from any source*** *that persons are in distress at sea, is bound to proceed with all speed to their assistance, if possible, informing them or the search and rescue service that the ship is doing so*.' Should the ship be unable to provide help or consider it unnecessary (e.g. if they are aware that help is already being provided), they are required to enter in the log-book the reason for failing to proceed to the assistance, taking into account the said recommendation to inform the appropriate SAR service. In addition to this, ships can be requisitioned by the master of a ship in distress or the SAR authorities to render assistance. (SOLAS 1974.)

The provision has later been amended with a few clarifications: 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.)

SOLAS also contains a provision on search and rescue services: each government undertakes to ensure that necessary arrangements are made 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.)

2.1.5. The International Convention on Maritime Search and Rescue

Even though both custom and treaties such as SOLAS oblige ships to provide help for those in distress, it was only after the 1979 International Convention on Maritime Search and Rescue (SAR Convention) that an international system for SAR operations was established. The SAR Convention is aimed at developing an international SAR plan so that no matter where an accident occurs, their rescue would be coordinated by a SAR organization or, when applicable, several SAR organizations in cooperation. The SAR convention obliges the contracting states to, individually or in cooperation with other states, develop SAR services to ensure that assistance is rendered to anyone in distress at sea. On receiving information about such a situation, urgent steps to endorse the necessary assistance shall be taken. The treaty has been ratified by 113 countries. (SAR Convention 1979.)

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 followed in MARISA toolkit services, so that they are well suited for rescue purposes, too:

- 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.).

2.1.6. The Convention Relating to the Status of Refugees

The **Convention Relating to the Status of Refugees**, also known as the **1951 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.)

2.2. European Union Law

2.2.1. Overview

The European Union (EU) is a political and economic union with 28 member states who have decided to act as one to achieve mutual peace and prosperity. The driving forces behind its development were originally related to the perseverance of peace and liberty as well as mutually beneficial economic integration, but in the recent decades the range of goals has expanded also to areas such as social progress and environmental protection.

The EU is based on the rule of law: each action taken by the EU is founded on treaties voluntarily and democratically approved by all member states. The EU is not a typical international organization, however. First of all, most of its acts are based on majority opinion (not consensus), and are adopted by EU: s own institutions, not the member states themselves (even if both member states and individual citizens have good representation in different EU organs). Secondly, as the member states have conferred to the EU competences to legislate and adopt legally binding acts – regulations, directives and decisions – in certain areas, no national ratification processes are needed for such acts to become binding for them.

In addition to this – and in order to ensure that the system can function in practice - EU law takes precedence over national law: the member states cannot adopt legislation that conflicts with EU law. Should such legislation nevertheless exist, it must be either given an interpretation that removes the conflict or be outright ignored. This is a fundamental principle in the EU law, as it is necessary for uniform and consistent application of the EU law.

2.2.2. The role of 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. The European Council meets twice every half year, and its task is to **define the overall political directions and priorities of the Union**. It is not one of the EU's legislating institutions, however, so it does not exercise legislative functions. Specific EU legislation with relevance to maritime surveillance will be discussed in the next chapters. (TEU 2007, article 15.)

The European Council traditionally works by adopting 'conclusions' that identify issues of concern and actions to take. In June 2014, the European Council agreed on **five priority areas** to guide the EU's work over the **next five years**. This strategic agenda will be used to plan the work of the European Council and also acts as a basis for the work programs of other EU institutions. From the viewpoint of MARISA and maritime surveillance, two priority areas a very relevant, namely ‘Freedom, Security and Justice’ and ‘EU as a strong global actor’ (see the table below). ‘Freedom, security and Justice’ is relevant if we are talking about the ethics and societal sustainability of MARISA in European context (e.g. border control and migration). Nevertheless, since MARISA also aims for businesses outside EU, ‘EU as strong global actor’ asks for solid societal consideration of MARISA and its impacts on societies. (European Council 2014.)

Priority area	Contents	Maritime Surveillance Aspects
Freedom, security and justice *‘The European Council emphasises the **importance of good EU cooperation** on security issues like terrorism and managing migration flows.’*	*better management of all aspects of migration, including irregular migration, asylum and border management* *preventing and combating organised crime, corruption and terrorism* *improving judicial cooperation between EU countries*	Privacy is strongly associated with freedom, and a society where every movement and action is recorded is considered as contrary to this idea of freedom. In the context of maritime surveillance, the principle of ‘freedom of navigation’ is important to protect. Increased control and security measures are justified with the need to protect Europe against cross- border crime, such as illegal trafficking and smuggling. The European maritime border is however not only a security issue for the EU, but also for those seeking to enter Europe by sea. Protecting the European seas and borders should be aimed at both creating a secure maritime environment, but also protecting the lives and physical and moral integrity of those who circulate at sea.

EU as a strong global actor *'The European Council calls on the EU to ensure its* ***strong engagement in world affairs****.'*	*ensuring consistency between member states' and EU foreign policy goals* *promoting stability, prosperity and democracy in the countries closest to the EU* *engaging global partners on a wide range of issues such as trade, cyber security, human rights and crisis management*	In the context of maritime surveillance, the lack of accountability and clear lines of responsibility between EU member states and their different actors is a persistent problem. Furthermore, the diverging interpretations of rules of international law hinder the cooperation between Member States in maritime surveillance. Maritime surveillance is based on coordination and information sharing between member states. Therefore, is has the potential to create a mutual control mechanism between the participating agents, with regards to both fundamental human rights and refugee law and rescue obligations.

Table 4: EC Strategic Priority Areas and MARISA

2.2.3. The Charter of Fundamental Rights of the European Union

The earlier EU treaties were thought of as more or less purely economic and did not include references to fundamental rights. Therefor 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.)

These fundamental rights should be a necessary requirement which could and should lead to drawing boundaries on what is and what is not acceptable in EC funded security research initiatives (CIES 2012).

In the context of various maritime operations aided by the MARISA 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 by sea**.** Important is also to note also the positive value ethics can bring to MARISA developments. There are various fundamental rights which MARISA promotes, both in the area of border control and SAR, but also in the domains of fisheries control, environment and customs. Ethics is not only a burden, but also possibility to create value in society – and to justify the existence of MARISA despite the challenges.

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 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 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 to access to documents
43 Right to access the European Ombudsman
44 Right to petition
45 Freedom of movement and residence
46 Diplomatic and consular protection

Justice
47 Right to an effective remedy and to a fair trial
48 Presumption of innocence and right to 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

Table 5: EU Fundamental Rights

To clarify the links between fundamental rights and maritime 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 maritime surveillance from which viewpoint the rights are analysed, the central column identifies the rights MARISA can promote, and finally the right column reveals the rights which may be violated by the use of MARISA if it is not designed and used ethically.

Aspect of maritime surveillance	**Rights which MARISA can promote**	**Rights to be protected/not to be violated**
Search and Rescue	(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.	(7) Privacy (8) Protection of personal data (21) Non-discrimination

	(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. (6) Right to life, liberty, and security. >Border control operations should not prevent individuals from the right to leave their country. In addition, the following other rights can also be relevant with refugees and asylum seekers since 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 (45) Freedom of movement	(7) Privacy and family life (8) Data protection All the rights which can be promoted (see the left column) can also be violated if refugees and migrants are sent back to their country of origin.
Fisheries control	(7) Right to property >Better surveillance of fish tracks. (16) Freedom to conduct business >Diminished need to aid in SAR. (31) Fair and just working conditions. >Not so much need for patrolling boats.	(7) Privacy (8) Protection of personal data
Customs	(16) Freedom to conduct 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	(17) Environment 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

Table 6: EU Fundamental Rights and MARISA

3. The Legal Framework for Maritime Surveillance Collaboration

The purpose of this chapter is to present and overview of the legal framework for maritime surveillance. Both legislation concerning border control, search and rescue legislation, and the framework for data management in the context of maritime surveillance are discussed. Finally, a legal framework and policy options elaborated in the EUCISE project will be discussed.

The subsections of the chapter are organised to match the organisation of the existing legislation, but even the proposal for a new regulation by the European Parliament and the Council on the European Border and Coast Guard has been taken into account in the subsections 3.2 and 3.3.

Legal issues concerning OSINT, Big data and AI are discussed separately, in Chapter 7.

3.1. The Schengen Borders Code (SBC)

The Schengen Borders Code 2016/399 is an EU regulation that sets out the rules on crossing the external borders of the Schengen area and the absence of border controls at the internal borders. Its key provisions contain regulation regarding e.g. checks on persons on external borders, entry conditions for non-EU or non-Schengen area nationals, and the conditions for temporary reintroduction of border controls at the internal borders in the (border-free) Schengen area. The SBC applies to all persons crossing the external borders of the Schengen area, including Romania, Bulgaria and Croatia that technically speaking are not yet Schengen countries. The SBC's is highly relevant for MARISA for instance because MARISA is likely to become a tool in the execution of Schengen border control.

Border control is in the interest of all Schengen countries: those at whose external borders it is carried out, but also those which have abolished internal border control. The preamble point (6) of the SBC sets out the intent behind the regulation: 'Border control should help to combat illegal immigration and trafficking in human beings and to prevent any threat to the Member States' internal security, public policy, public health and international relations' (SBC 2016). Hence, the aims behind border control are both humanitarian and safety-related.

As per the point (8) of the preamble to the SBC, border control comprises not only checks on persons at border crossing points and surveillance between those border crossing points, but also an analysis both of the risks for internal security and of the threats that may affect the security of external borders. Generally, external borders may be crossed only at border crossing points and during the fixed opening hours (Article 5). Due to the regular border crossings through official border crossing points are out of the scope of the MARISA project, border checks will not be discussed. (SBC 2016.)

Article 13 stipulates the implementation of border surveillance in more detail. The border guards shall use stationary or mobile units to carry out border surveillance. Surveillance may also be carried out by technical means, including electronic means. Surveillance shall be carried out in such a way as to prevent and discourage persons from circumventing the checks at border crossing points, and that unauthorised border crossings are always at risk of being detected. (SBC 2016.)

The SBC contains several provisions regulating the cooperation between different actors. Each member state shall ensure close and constant cooperation between its national services responsible for border control (SBC 2016, article 16.3). In addition to this, the member states are obligated to assist each other, maintaining close and constant cooperation with a view to the effective implementation of border control; *all relevant information* shall be exchanged (SBC 2016, article 17.)

According to article 17, operational cooperation and assistance between member states in relation to border control shall be managed and coordinated by the Agency established by regulation (EC) No 2007/2004. The Agency was originally known as *The European Agency for the Management of Operational Cooperation at the External Borders (of the Member States of the European Union)*, but its tasks have since been expanded and it currently goes by the name of *The European Border and Coast Guard Agency*, also known as *Frontex*. The role of Frontex as a manager and coordinator does not mean that it would have exclusive competence regarding the operational cooperation among the member states, however. The member states may, without prejudice to the competences of the Agency, continue operational cooperation with other Member States and/or third countries at the external borders, including the exchange of liaison officers, where such cooperation complements the action of Frontex. (SBC 2016.)

3.2. The Regulation on the European Border and Coast Guard (Frontex)

Frontex coordinates and organises joint operations and rapid border inventions to assist member states at the external borders, including in humanitarian emergencies and SAR operations at sea. To help identify migratory patterns as well as trends in cross-border criminal activities, Frontex analyses data related to the situation at and beyond EU's external borders. It monitors the situation at the borders and helps border authorities to share information with member states. The agency also carries out vulnerability assessments to evaluate the capacity and readiness of each member state to face challenges at its external borders. (Frontex WB.)

The key role of Frontex is to establish a technical and operational strategy for implementation of *integrated border management* (IBM) at Union level. According to article 5 (article 7.1 in the new proposal 'Regulation of the European Parliament and of the Council on the European Border and Coast Guard'), the responsibilities are shared as follows: 'The European Border and Coast Guard shall implement European integrated border management as a shared responsibility of the Agency and of the national authorities responsible for border management, including coast guards to the extent that they carry out maritime border surveillance operations and any other border control tasks' (FRONTEX 2016; EU/PROPOSAL 2018). The main relevance of the Frontex regulation (and the new proposal) stems from the fact that MARISA is a potential a tool to aid the execution of the integrated border management.

The content of the IBM and tasks of Frontex can be used as indicators what kind of information is required. In other words, they define the areas of interests what kind of information is needed and for which purposes to satisfy border authorities 'need to know'. It can also be concluded that implementation of the main tasks of Frontex are related to information exchange and analysis of data.

Article 10 in the current legislation (article 12 in the new proposal) stipulates an *obligation to exchange information.* In order to perform the tasks conferred on them by Regulation (EU) 2016/1624, in particular for Frontex to monitor the migratory flows, to carry out risk analysis and to perform the vulnerability assessment, Frontex and the national authorities responsible for border management and return, including coast guards to the extent that they carry out border control tasks, *shall exchange all necessary and accurate information in a timely manner*. It is noteworthy that obligation to exchange information is *limited to border control community*. The technical standards for information systems and software applications should be aligned with the standards used by eu-LISA for other IT systems in the area of freedom, security and justice. (Frontex 2016; EU/PROPOSAL 2018, article 10a.)

According to proposed Pre-article 28, Air border surveillance aims at detecting and monitoring such suspicious flights crossing or intending to cross EU external borders and performing related risk analysis with a view to triggering reaction capabilities by the competent authorities of the EU and the Member States. For this purpose, interagency cooperation at EU level should be promoted between the Agency, the network manager of the European air traffic management network (EUROCONTROL) and the European Aviation Safety Agency (EASA). Where relevant, Member States should be able to receive information on suspicious external flights and react accordingly. The Agency should monitor and support research and innovation activities in this area. (EU/PROPOSAL 2018.)

Articles 44-50 (articles 87-91 in the new proposal) contains general provisions on information exchange and data protection. According to Article 44 *Frontex may take all necessary measures to facilitate the exchange of information* relevant to its tasks with the Commission and the Member States and, where appropriate, the relevant Union agencies. It shall develop and operate an information system capable of exchanging *classified information* with those actors, and of exchanging *personal data* (referred to in accordance with Council Decision 2013/488/EU and Commission Decision (EU, Euratom) 2015/443 and 2015/444. (FRONTEX 2016; EU/PROPOSAL 2018.)

Frontex shall also facilitate and encourage technical and operational cooperation between Member States and third countries, within the framework of the external relations policy of the Union, including with regard to the protection of fundamental rights and the principle of non-refoulement. Article 3 in the new proposal state that fundamental rights, education and training, and research and innovation shall be horizontal components taken into account in the implementation of the European Integrated Border Management. This Regulation respects the EU Fundamental Rights and the Charter of Fundamental Rights of the European Union, in particular respect for human dignity, the right to life, the prohibition of torture and inhuman or degrading treatment or punishment, the prohibition of trafficking in human beings, the right to liberty and security, the right to the protection of personal data, the right of access to documents, the right to asylum and to protection against removal and expulsion, non-refoulement, non-discrimination and the rights of the child. (EU/PROPOSAL 2018.)

Frontex and the Member States shall comply with Union law, including norms and standards which form part of the Union acquis also when cooperation with third countries takes place on the territory of those countries. The establishment of cooperation with third countries shall serve to promote European border management and return standards. (FRONTEX 2016, article 54.1; EU/PROPOSAL 2018, articles 72-79.)

3.3. The EUROSUR Regulation

European Border Surveillance System (EUROSUR) is a common framework established by regulation (EU) No 1052/2013 for the exchange of information and cooperation between Member States and Frontex. It comprises all Schengen area countries and Bulgaria, Romania and Croatia. The establishment of EUROSUR was seen as necessary in order to strengthen the exchange of information and the operational cooperation between national authorities of Member States as well as with Frontex. The idea is that EUROSUR provides both national authorities and Frontex with the *infrastructure* and *tools* needed to improve their *situational awareness* and *reaction capability* at the external borders for the purpose of detecting, preventing and combating illegal immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants. (EUROSUR 2013, article 1; EU/PROPOSAL, article 18.)

In article 18 (Cooperation of the Agency with third parties) lists several relevant agencies with which it is obligatory for Frontex to cooperate and share information (EUROSUR 2013). All identified MARISA user communities are covered by Article 18 except the Defence community. However in the new proposal the list is more comprehensive (EU/PROPOSAL 2018, see article 69).

The EUROSUR Regulation establishes the EUROSUR framework and defines the operational and technical requirements for its functioning. According to article 4 (article 20 in the new proposal), EUROSUR consists of six components:

1) National coordination centres (NCC)
2) National situational pictures (NSP)
3) A communication network (a European situational picture including external border sections with corresponding impact levels in the new proposal)
4) An european situational picture (ESP); (Specific situational pictures in the new proposal)
5) A common pre-frontier intelligence picture (CPIP) (EUROSUR Fusion services in the new proposal)
6) Common application of surveillance tools. (integrated planning in the new proposal) (EUROSUR 2013; EU/PROPOSAL 2018.)

Each Member State designates, operates and maintains a national coordination centre which coordinates and exchanges information among all authorities with a responsibility for external border surveillance at national level, as well as with the other national coordination centres and Frontex (Article 5, article 26 in the new proposal). The national situational pictures (NSP), the European situational picture (ESP) and the common pre-frontier intelligence picture (CPIP) are produced through the collection, evacuation, collation, analysis, interpretation, generation, visulisation and dissemination of information. Each picture consists of three layers: an event layer, an operational layer, and an analysis layer. (article 8, articles 27-29 in the new proposal). Frontex shall establish and maintain a communication network in order to provide communication and analytical tools and allow for the exchange of non-classified sensitive and classified information in a secure manner and in near-real-time with, and among, the national coordination centres. (EUROSUR 2013, article 7; EU/PROPOSAL 2018, article 13.)

The EUROSUR Regulation includes also provisions about data protection. Any information sharing shall respect data protection and the fundamental rights. This limits the possibilities for an open sharing of data. In order to share personal data, the principle of *purpose limitation* applies, and the collected data can only be used for the same purpose. It is noteworthy that EUROSUR system is not, in principle, intended for the transmission of personal data. According to preamble (13) of Regulation (EU) No 1052/2013 'Any exchange of personal data in the European situational picture and the common pre-frontier intelligence picture should constitute *an exception* (for data protection in the new proposal, see articles 87-90). (EUROSUR 2013; EU/PROPOSAL 2018.)

According to article 18 (article 69 in the new proposal) information exchange between Frontex and the Union bodies and the international organisations shall be exchanged via communication networks that fulfil the criteria of availability, confidentiality and integrity. The handling of classified information shall comply with security rules and standards equivalent to those applied by Frontex. The Union bodies and the international organisations shall use information received in the context of EUROSUR only within the limits of their legal framework and in compliance with fundamental rights, including data protection requirements. (EUROSUR 2013; EU/PROPOSAL 2018.)

Article 20 (article 73 in the new proposal) guides cooperation with neighbouring third countries: Member States may exchange information and cooperate with neighbouring third countries. Information exchange and cooperation shall base on bilateral or multilateral agreements or through regional networks based on agreements. NCCs of the Member States are the contact points for the information exchange. The agreements shall comply with the relevant Union and international law on fundamental rights and on international protection. The exchange of personal data with third countries within the framework of EUROSUR system must be strictly limited to what is necessary for the application of this Regulation. (EUROSUR 2013; EU/PROPOSAL 2018.)

3.4. The Regulation on the Surveillance of External Sea Borders

Regulation (EU) No 656/2014 is an EU-regulation that establishes rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by Frontex. It obliges to render assistance to any vessel or person in distress at sea during a sea operation. In addition, Member states shall ensure that their participating units comply with that obligation, in accordance with international law and respect for fundamental rights. They shall do so regardless of the nationality or status of such a person or the circumstances in which that person is found. (EU 656/2014, article 9.)

As described above, Regulation (EU) No 656/2014 addresses readiness for SAR during border surveillance operations. In accordance with international law, every State must require the master of a vessel flying its flag, in so far as he can do so without serious danger to the vessel, the crew or the passengers, to render assistance without delay to any person found at sea in danger of being lost and to proceed with all possible speed to the rescue of persons in distress. Such assistance should be provided regardless of the nationality or status of the persons to be assisted or of the circumstances in which they are found. The shipmaster and crew should not face criminal penalties for the sole reason of having rescued persons in distress at sea and brought them to a place of safety. Article 9 regulates search and rescue situations addressing obligation of *duty of care* and by taking any measure necessary for the safety of the persons concerned, while avoiding taking any action that might aggravate the situation or increase the chances of injury or loss of life (EU 656/2014.)

Each Contracting Government undertakes to ensure that necessary arrangements are made for distress communication and co-ordination in their area of responsibility and for the rescue of persons in distress at sea around its coasts (EU 656/2014.)

3.5. Maritime CISE

3.5.1. Commission's Communication (2014) on CISE

In 2014, the Commission gave to the European Parliament and the Council the Communication, '*Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain'.* The document lays the ground for the Maritime CISE, enhancing information exchange between maritime surveillance authorities in the EU maritime domain. This has been one of the key strategic objectives of the Union under the Integrated Maritime Policy, and an important building block of the Maritime Security Strategy. (COM 2014.)

CISE (Common Information Sharing Environment) is a voluntary collaborative process in the European Union that seeks to enhance and promote information sharing between the authorities involved in maritime surveillance. It does not aim to replace or duplicate old information exchange systems and platforms, but to build on them. The goal is to increase the efficiency, quality, responsiveness and coordination of surveillance operations in the European maritime domain as well as to promote innovation for the prosperity and security of the EU and its citizens. However, Maritime CISE does not have any impact on the administrative structures of Member States, on the existing EU legislation in this field, or on the implementation of ongoing EU level initiatives, in particular not on those based on legal Union requirements. (COM 2014.)

The objective of Maritime CISE is to ensure that maritime surveillance information collected by one maritime authority and considered necessary for the operational activities of others can be shared and thus become subject to multiuse, rather than being collected and produced several times, or collected and kept for a single purpose. (CISE 2014) The information gathered could be either raw or unprocessed data which are formatted in a special way, or information derived from data that has been processed and taken a certain meaning. Secondly, the information itself can be 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. By moving towards a multipurpose use of data and by making current maritime surveillance systems interoperable, in this case it means that the information can be sent automatically from the system of one maritime surveillance authority to another, data collection will be a less time and resource intensive exercise and, in the best case scenario, authorities will always have the best available information on the situation at sea at their disposal.

Within maritime CISE, duplication of data collection efforts can be the indirect result of suboptimal co-operation between authorities. It may implicate the acquisition, maintenance and deployment of surveillance assets such as satellites and communication systems. In addition, enhanced information exchange could help avoiding that such resources are acquired in duplication, screen the same sea area twice, or collect the same information several times and carry out overlapping missions at sea. (COM 2014.)

The advantages of maritime CISE and its enhanced information exchange are following:

a) Enhancing knowledge and improving maritime situational awareness. Both can enhance prevention, preparedness and response to maritime security incidents related to cross border and organised crime (e.g. trafficking, illegal fishing, piracy, armed robbery, terrorism) maritime safety and illegal discharges or accidental marine pollution. Assessments involving Member State experts have clearly demonstrated that authorities manage maritime surveillance activities more effectively if all relevant information would be at their disposal during the planning and execution of operational activities. This could potentially lead to the reduction of such threats and risks by 30% on average. Pertinent examples would be information sharing between civilian and military authorities on the influx of migrants to the Schengen Area through the Mediterranean Sea; or that common routine surveillance and emergency management tools around a sea basin could be connected in one 'click' in case of emergency.

b) Substantial reductions in data collection efforts. Stakeholders have indicated that there is a large demand for additional data exchange in particular between civilian and military authorities and that over 40 % of the data collected in the EU is collected by several authorities at the same time, such as non-co-operative targets and ship identification information. (COM 2014.)

Initiatives to improve information exchange for the maritime domain have already been ongoing for some time. Basically, the progress has already been made through a number of legislative instruments at EU level that put in place systems serving different policy areas and, in some cases, going beyond one sector. In addition, the experiences made have shown that there is an added value for further cooperation. According to COM (2014) 451 final, one example is the operational use of the integrated maritime services (enhanced maritime awareness picture) provided by EMSA to FRONTEX and EFCA. It can be described as an inspiration for how cooperation at national level could be pursued. (COM 2014.)

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.)

3.5.2. The EUCISE2020 Project

This chapter partly reviews the legal framework of EUCISE2020 project. CISE is a project that seeks to reinforce a safe, secure and sustainable use of maritime space (aim) through information sharing among various user communities (components). It purports to bring together existing monitoring and tracking systems used by various user communities in order to establish a more inter-operable surveillance system, contributing to improvement in efficiency of MS' authorities and improve cost effectiveness. In general, EUCISE2020 involves horizontal data sharing and data exchanges within sectors and cross-sectors. Hence, it corresponds to the integrated management and integrated policy solutions.

Interim report of EUCISE2020 'The Development of CISE of the Surveillance of the EU Maritime Domain and their related impact assessment' addresses the mapping of user communities 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. Therefore, the chapter reviews the general legal framework referred in the interim report of EUCISE2020. The reviewed legislation presents the matters that have not yet discussed under Marisa project. Consequently, the review concentrates on the founding treaties of European Union as well as the principles of EU law. (CISE 2013.)

As a legal basis, the interim presents the principles of EU law laid down in the Treaty of on European Union (TEU) and Treaty of Functioning European Union (TFEU). The treaties set the legal mandate for possible EU policy and legislation for the CISE development. According to the interim report, the choice of appropriate legal basis for a measure has constitutional significance. Pursuant to the principle of conferral, as embodied in Art. 5 TEU (ex-Art. 5 TEC), the Union shall act only within the limits of the competences conferred upon it by the MS in the Treaties to attain the objectives set out therein. As a matter of principle, a measure should be founded on a single legal basis unless the examination of the measure reveals that it pursues a number of objectives or that it has several components, which are (1) inseparably linked and (2) without one being incidental to the other. Maritime policy does not fall under a single sector-based policy; it is based on a large number of legislative acts with legal bases in different provisions of both the TFEU and TEU. (CISE 2013.) For example, border control is defined in article 74 and 77 of TFEU, including the measures to ensure administrative cooperation between the relevant departments of the Member States in the area of freedom, security and justice and measures concerning border checks.

In the case where the all user communities should be embraced under a single framework of rules, would in principle be necessary to seek recourse to multiple legal base (CISE 2013). However, the existing legal framework nonetheless limits the possibilities to do so. As a matter of principle, TFEU and TEU competences may not be combined to provide a multiple legal basis for a single measure even if the measure pursues a number of objectives or has several components falling respectively within the policies governed by the TFEU and TEU, and where neither one of those components is incidental to the other. (CVRIA 2008.) This follows from the fact that the two systems have substantially different general characteristics: they provide for divergent legal instruments and envisage different decision-making procedures. Decision-making under the TFEU is often under co-decision, while the TEU provides for unanimous voting in the Council with minimal participation of the European Parliament. It is irrelevant whether in a specific case the TFEU and TEU legal basis contain incompatible legislative procedures. It is the sum of these differences, which makes it impossible to use TFEU and TEU legal basis simultaneously. (CISE 2013.)

According to the interim report, given that the defence user community has legal basis in the TEU and the remaining 6 in the TFEU, the following conclusions with respect to the implementation of CISE may be made:

Firstly, that it would not as a matter of principle be possible to adopt a measure founded both on a legal basis in the TFEU and TEU (for example a Council decision embracing all 7 user communities). The measure may on the other hand be split in parts so that part of the measure would cover the user communities embraced be TFEU, while the other would embrace the defence community, which is governed by TEU.

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.)

Interim report concludes that in the above-mentioned connection would be necessary to analyse in detail to which extent the proposed CISE legal framework seeks to implement objectives pursued by the common foreign and security policy, as governed in the TEU, and to which extent similar objectives may be implemented under TFEU policies. If one arrives at the conclusion that the CISE measure seeks equally to implement the common security and defence policy (i.e. foreign policy, Union's security and the progressive framing of a common defence policy) as well as the TFEU policies, the measure would in principle have to be split. In order to determine this question a detailed analysis of the aims and components of the proposed CISE legal framework will be necessary. (CISE 2013.)

The interim report of EUCISE2020 refers to EU Right to Act. According to the report, the verification of the EU Right to Act goes beyond the mere verification of the right of the EU to partake in the CISE development. According to the interim report, such an overall right must be established however, must also be followed by a more detailed definition of the precise scope of the EU Right to Act. The EU CISE action shall respect and manoeuvre within the TEU legal framework, allow MS to fulfil own policies according to Subsidiarity and opt-in/opt-out legal mandates. (CISE 2013.)

Firstly, the report refers to subsidiarity assessment as the CISE takes part of the EU regulatory trend based on transnational information networking (CISE 2013). The principle of subsidiarity is laid down in Article 5(3) of the Treaty on European Union (TEU) and Protocol (No 2) on the application of the principles of subsidiarity and proportionality. The general aim of the principle of subsidiarity is to guarantee a degree of independence for a lower authority in relation to a higher body or for a local authority in relation to central government. Principle of subsidiarity involves the sharing of powers between several levels of authority, a principle that forms the institutional basis for federal states. In the context of the European Union, the principle of subsidiarity serves to regulate the exercise of the Union’s non-exclusive powers. It rules out Union intervention when an issue can be dealt with effectively by Member States at central, regional or local level and means that the Union is justified in exercising its powers when Member States are unable to achieve the objectives of a proposed action satisfactorily and added value can be provided if the action is carried out at Union level. Under Article 5(3) TEU there are three preconditions for intervention by Union institutions in accordance with the principle of subsidiarity: (a) the area concerned does not fall within the Union’s exclusive competence (i.e. non-exclusive competence); (b) the objectives of the proposed action cannot be sufficiently achieved by the Member States (i.e. necessity); (c) the action can therefore, by reason of its scale or effects, be implemented more successfully by the Union (i.e. added value). (Panizza 2018.)

The interim report refers that the regulatory network approach is already on-going in several EU actors. For example, several EU agencies, (i.e. Frontex and EMSA) are related information networking and on that basis are relevant for the CISE. The EU transnational approach respects and utilises the existing national competences, legislation and administrative behaviours, and at the same time the EU transnational approach ensures the need for coordination and network facilitation at European level. Without the overall EU coordination, the various national differences would risk resulting in dysfunction. The role of the EU is actively to utilise and apply the national differences in coordinated manners. According to the interim report, the EU may provide the overall legal and institutional framework needed for successful CISE implementation. (CISE 2013.)

Secondly, the interim report refers to proportionality, as EU initiatives to enhance the benefits from sharing information do not go beyond what is necessary to achieve the objectives. The principle of proportionality seeks to set actions taken by EU institutions within specified bounds. Under this rule, the action of the EU must be limited to what is necessary to achieve the objectives of the Treaties (EUR-LEX Glossary). It means that the content and form of the action must be in keeping with the aim pursued. The principle of proportionality is laid down in Article 5 of the Treaty on European Union. The criteria for applying it are set out in the Protocol (No 2) on the application of the principles of subsidiarity and proportionality annexed to the Treaties. In the context of EU CISE, it means that the measures and means to achieve and implement the EU CISE development shall be defined gradually over time and based on a 'need be' basis. Such an approach takes into account the dynamic and evolving transnational nature of the CISE cooperation amongst MS and user groups (CISE 2013). In addition, the EU CISE instruments may in proportional manners correspond to such transnational needs and address primarily coordination and common direction. (CISE 2013.)

Thirdly, interim report refers that CISE will be built on existing legislation and the aim of revising measures to eliminate differences between Member States on the full exploitation of maritime surveillance data gathered by relevant actors in Member States. The EU CISE initiatives add the needed cross-sectoral coordination and facilitation for inter-operational data exchange required to develop the EU integrated maritime policy. According to the interim report, the CISE initiatives provide a coherent supplement to the already existing EU policy and legal framework. (CISE 2013.)

3.5.3. 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. 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. (CISE 2013.)

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. 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. (CISE 2013.)

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. 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. This framework would aim at embracing all user communities under one measure. (CISE 2013.)

4. Privacy and Data Protection Legislation

In this chapter, we present the main requirements and guidelines for MARISA regarding personal data processing, including both technical and organizational issues.

4.1. Background

Rapidly emerging technologies (such as smart phones and mobile applications, big data analytics, artificial intelligence, and the internet of things) and globalization have brought new challenges for the protection of personal data, and the scale of the collection and sharing of personal data has increased substantially during the past decades. New technology allows both companies and public actors to use personal data on an unprecedented scale to pursue their activities, and natural personas increasingly make personal information availably publicly and globally. In addition to the data explicitly provided by the data subjects themselves, personal data is nowadays often collected in an automatic manner by various gadgets and software we use, and is collected by various actors already from birth. Additionally, the economic and social integration in the EU has led to a massive increase in cross-border flows of personal data.

In order to ensure a consistent, high level of protection of personal data in the face of these changes, 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 data package comprises two main parts, both of which are relevant for MARISA:

1) Regulation (EU) 2016/679 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 (The General Data Protection Regulation / GDPR)
2) Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (The Data Protection Law Enforcement Directive / LED)

That the GDPR is a regulation means that it is a binding a legislative act that is enforceable in its entirety across the EU from the day it came into effect – in this case the 25th of May 2018**.** The LED, being a directive, is different in the sense that that it obliges the member states to achieve the results specified in the directive, but has to be incorporated in the national legislation, and leaves thus a little more leeway to the member states as to the exact formulations of the rules to be adopted. The deadline for the incorporation of the LED into national law was the 6th of May 2018. (GDPR 2016; LED 2016.)

The central difference between the GDPR and LED is that the latter sets out rules for criminal law enforcement authorities only, whereas the GDPR concern largely all other processing of personal data that falls under the scope of the union law. Processing by natural persons for purely personal purposes is the most notable exception to the application of the GDPR. As MARISA will likely be used for both law enforcement purposes and other activities (such as SAR), both documents' requirements are taken into account in this deliverable. Content wise there are some differences between the GDPR and the LED especially with regard to the principles and lawfulness of personal data processing and to the rights of the data subject. The responsibilities of register owners and data processors are quite similar in the two, however.

The GDPR applies to organizations located within the EU, but also to ones located outside of the EU if they offer goods or services to or monitor the behaviour of EU data subjects. It applies to all actors holding or processing the personal data of EU data subjects, regardless of the actor's own location. This is referred as the 'territorial scope'. The GDPR is applied always when personal data is processed wholly or partly by automated means, as well as when the data is not processed by automated means but forms or is intended to form a part of a filing system. This is referred to as the 'material scope'. (GDPR 2016, articles 2-3.)

The LED, as suggested by its name, applies to the movement and processing of personal data by competent authorities for law enforcement purposes – which fall outside the scope of the GDPR. 'The competent authorities' refers not only to stereotypical public law enforcement actors, but to any actor (public of private) entrusted with the right to exercise public authority and powers for law enforcement purposes. (LED 2016.)

Accountability

Accountability is one of the central game-changer approaches for this new era of data protection. The organisations that handle personal data are placed in the centre of the game with the requirement that they not only put in place technical and organisational measures to prevent the risks for and mitigate the effects of personal data breaches (which are defined in a really broad manner), but that they also be able to demonstrate their compliance to data protection authorities whenever requested. (GDPR 2016; LED 2016.)

The appropriate measures to enable compliance with the principle of accountability include, but are not limited to, documentation on what, how, for how long and for what purposes personal data is processed, the establishment of processes and procedures to tackle data protection issues, both when designing information systems and in the event of a data breach; the appointment of a Data Protection Officer that is be integrated in the organisation planning and operations, and many more.

Accountability is not about perfection, but about ensuring that the protective measures taken by data controllers both before, during, and after processing personal data or in the event of a breach are sufficient and reasonable with regards to the risks involved. This implies the necessity of a thorough risk assessment regarding technologies, their development and use processes as well as the business models. The decisions and processes taking place, including any information security incidents, must be documented appropriately.

The obligations regarding accountability are not one-off types of duties, but rather ongoing processes that must be reviewed, and, where necessary, updated. The development of new technologies or codes of conduct, for example, could mean that what is compliant today is no longer compliant tomorrow. Taking the accountability requirements seriously can help a controller to build trust with both authorities and individuals, to mitigate enforcement action and may even become a competitive advantage, as the awareness of data protection and privacy related challenges is constantly rising.

The Risk-based Approach

As a result of the GDPR and the LED, data protection is becoming increasingly risk-based and by design. According to both acts (GDPR article 24 & LED article 19), the controller is responsible for implementing appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the relevant regulations. This must be done in such a way that 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 are taken into account. This so-called risk-based approach, where organizations and companies are instructed to scale their protective measures to correspond to the risk levels in their data processing activities, is central in the GDPR and can be described as representing a shift from detailed bureaucratic requirements towards a more effective ‘compliance in practice’.

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.

For example, the requirement of ‘*accountability*’ can be fulfilled with very different means in different environments and organizations. The risk-based approach enables a high level of protection for personal data in all cases, while avoiding to over-regulate low-risk processing.

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 – as is the case in MARISA.

Filing system refers to any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (GDPR 2016, article 3). They are formed when data is collected of the area and persons through automated means such as optic electronic devices. Filing systems can form anywhere. Even a single sensor might have memory where personal data is stored. Even if it would be there a limited time, it still forms a filing system. It should be kept in mind that usually the administrators and developers have accounts inside the system or its components and thus access to data inside the system. *This renders a single administrator as a personal data processor.*

The Relevance for MARISA

The EU data protection reform has strong implications for MARISA system architecture, technical solution, and use. MARISA is not intrinsically interested in personal data but will use it as input in its data fusion analyses both directly (e.g. Twitter messages, high-resolution satellite images) and indirectly (e.g. AIS information). No such personal data is saved or stored in the system, however, which is why many of the new rights granted to the data subjects. in the legislation are less critical in the MARISA context.

However, the requirements for processing for controllers must be deeply intertwined in the MARISA solution both on the level of technology, user processes and business/governance/adoption models. The privacy governance model must take into account all forms of privacy related issues until there is concrete model on what the system does and how.

4.2. The Principles for Processing Personal Data

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. This can be understood to include maintaining an information security policy and executing it, as well as deciding what measures provide an appropriate level of security in each case.
7) Accountability: The controller shall be responsible for and be able to demonstrate compliance with all of the principles described above. (GDPR 2016, article 5; LED 2016, article 4.)

Accountability is perhaps the most important of the new requirements for controllers and processors. The GDPR and the LED both require that all data controllers are able to demonstrate their compliance with the obligations and principles described in the legislation (GDPR 2016, article 5(2); LED 2016, article 4 (4)). In the case of privacy violation, every controller must be able to demonstrate the level of compliance organization had before the violation, not just the actions or the acquired compliance level they reached after the violation.

Lawfulness of processing

When it comes to the processing of personal data under the GDPR, processing is lawful only when at least one of the justifying conditions specified in the regulation is met. Due to the heterogeneity of both MARISA data sources and the purposes behind data processing in MARISA, the relevant justifying conditions can vary a lot from case to case. The 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 (or in order to take steps prior to entering into a contract);
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 interest 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. (GDPR 2016; LED 2016.)

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.

Special Categories of Personal Data

Certain types of sensitive data are given a special status in the GDPR and LED. MARISA does not aim to handle such data, but it is nevertheless very much possible that data classified as sensitive could enter into the system via SOCMINT (e.g. if a Twitter comment contains sensitive information), high-resolution satellite images or similar.

All processing of personal data belonging to the special categories is prohibited as a rule, with the exceptions being cases such as when the data subject themselves has manifestly made the data public or 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. The special categories are the same in both the GDPR and the LED (articles 9 and 10, respectively):

1) Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership
2) Genetic or biometric data processed for the purpose of uniquely identifying a natural person
3) Data concerning health
4) Data concerning a person's sex life or sexual orientation.

4.3. The Rights of the Data Subject

The rights of the data subject are regulated in the chapter 3 in both the GDPR and the LED. 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. 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. However, since the raw data used as input to the analyses is not stored in MARISA most of these rights have little relevance for the project. (GDPR 2016; LED 2016.)

The only personal data saved in the system is that relating to the MARISA user accounts. From the perspective of data protection, handling such user credential data is relatively risk-free: the information tends not to be classified as sensitive, and the data subjects have given their explicit consent to the processing.

4.4. The Obligations of Data Processors and Controllers

‘Controller’ is 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. When two or more controllers jointly determine the purposes and means of processing, they are ‘joint controllers’. Joint controllers shall in a transparent manner determine their respective responsibilities for compliance under the GDPR and the LED. (GDPR 2016; LED 2016.) In MARISA, the controller is the Executive Board (the decision making body that has the highest level of authority in the project).

‘Processor’, is a (natural or legal) person, public authority, agency or another body, which processes personal data on behalf of the controller. Therefore, any of the consortium members in MARISA could have the status of a processor. The processor shall not process the personal data except on instructions from the controller, unless required to do so by EU law or member state law (GDPR article 29, LED article 23.)

The supervisory authorities for MARISA are the European Data Protection Board (former WP29), and the relevant supervisory authorities established by member states (GDPR 2016, articles 2-3; LED 2016, article 2.)

4.4.1. General Obligations

The controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the legislation. This obligation can be seen as following from the accountability principle. There are no specified instructions in either the GDPR or the LED on how the implementation is to be done: both instruct the controller to take into account 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 (GDPR article 24, LED article 19). This flexibility allows the efforts to be scaled to fit each individual context, and is a direct manifestation of the risk-based approach described above.

The controllers are only allowed to use processors that provide sufficient guarantees to implement appropriate technical and organisational measures; the use of a processor may in other words not lead to worse protection for personal data. The processors' processing must be governed by a contract or a comparable binding legal act that sets out the subject matter and duration of the processing, the nature and purpose of processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The processor shall not engage another processor without prior authorisation of the controller.

Data Protection by Design and by Default

Compliance with the data protection legislation requires the integration of safeguards into the processing, both at the time of the determination of the means for processing and at the time of the processing itself. This requirement is known as 'data protection by design and by default' in both the GDPR and the LED.

The risk-based approach can be seen also in these requirements: the controller is obliged to implement 'appropriate' techincal and organisational measures designed to implement data protection principles 'in an effective manner' and to integrate all 'necessary' safeguards into the processing. When evaluating the implementations to be performed, the controllers are instructed to take into account at least the state of the art in data protection, the cost of implementation and 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 posed by the processing. One example of a privacy by design and default-implementation could be the use of pseudonymisation to implement the principle of data minimisation (GDPR, article 25; LED 2016, article 20). See also chapter 5 for approaches concerning the practical applications of Privacy by Design/Default.

Records of Processing Activities and of Data Breaches

The obligation to create and maintain records of processing activities is imposed on both controllers and processors, under both the GDPR and the LED. This entails a written overview and documentation over the procedures of personal data processing. A long list of minimum requirements as to the contents of these records is found in the legislation, including for instance information about the controller/processor, the purposes of the processing, a description of the categories of data subjects and personal data, the categories of recipients to whom the personal data have been or will be disclosed. Where applicable, the record should also contain information about transfers to third countries or international organizations, time limits for storage and general descriptions of technical and organizational measures referred to in the section 'security of personal data' (below). The records shall be made available to the supervisory authority on request (GDPR 2016, article 30; LED 2016, article 24.)

Certain smaller organisations are exempted from the obligation to maintain records of their processing activities if the evaluated risks in their processing activities are low, the processing is only occasional, and does not include special categories of data. The exemption is, thus, rarely applicable; it is certain that MARISA and its stakeholders could not qualify for it.

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

When it comes to processing of personal data under the LED, keeping logs is compulsory. Logs must be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. It must be possible to establish the justification, date and time of any consultation or disclosure operations on the basis of their logs. Also 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

The purposes of logging are the verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings. These are also the sole purposes that the logs may be used for. Upon request, the controller and the processor shall make the logs available to the supervisory authority. (LED 2016, article 25.)

4.4.2. The Security of Personal Data

Security of processing

It is not only confidentiality and integrity that the legislation is concerned with; features such as resilience, reliability, and the ability to restore normal operations in the event of malfunction or similar are also emphasised in the GDPR and the LED.

The GDPR article concerning the security of processing does not provide any descriptions of general minimum measures for data protection, but instructs actors (both controllers and processors) to scale their protective measures to the likelihood and severity of the risks involved. ‘Appropriate technical and organisational measures’ considering the state of the art in data protection, cost of the implementation, and the nature, scope, context and purposes of processing, shall always be taken, but they might look different for different actors. Some suggestions for appropriate measures are, however, provided:

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

A similar requirement to take into account the state of the art, the cost of implementation, the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons is found also in the LED. The requirements to be given to controllers and processors are more concrete in the LED when compared to the GDPR. Following and evaluation of the risks involved, they are to implement measures designed to:

- Control access to equipment
- Prevent unauthorised reading, copying, modification or removal of data media
- Prevent the unauthorised input, inspection, modification or deletion of stored personal data
- Prevent the use of automated processing systems by unauthorised persons using data communication equipment
- Ensure that authorised users to automated processing systems have access only to the personal data covered by their access authorization
- 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
- 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
- Prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media
- Ensure that installed systems may, in the case of interruption, be restored
- 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.

Though the requirement to scale one’s efforts to match the risks and other situational factors provides flexibility in the implementation and application of the legislation, it could be hard to know what exactly constitutes ‘appropriate measures’. The preamble to the GDPR gives some guidelines as to how the assessment of data security risks should be done to comply with the legislation. Controllers should be able to mitigate the risks that might result e.g. from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (GDPR 2016, preamble point 83).

In order to best comply with these security requirements, all actors who process personal data should have the organizational and technological capability to notice and document breaches. A regular firewall or encryption as a preventive instrument is obviously not sufficient from a security point of view. Besides, firewall or encryption are not helpful in noticing data breaches caused by unauthorised or otherwise unlawful or wrong kind of processing activities.

It is also important that system data flows are documented and that data protection trainings are given for personnel with access to personal data. There should be a documented training program and maybe even tests to ensure that the personnel know the lawful processing principles of the personal data. If personnel have no periodically reported 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, and could include very different looking events, including instances of hacked data, but also e.g. lost, stolen or improperly disposed hardware or paper records to information mistakenly disclosed to unauthorised actors by staff members.

As described above, controllers have in certain cases an obligation to notify a specified supervisory authority about personal data breaches and to provide them with documentation about the breach. This must be done without undue delay and, where feasible, not later than 72 hours after having become aware of it. The only exception is when the personal data 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 personal data breach. The information to be included in the notification is regulated in the articles 33 (GDPR 2016) and 30 (LED 2016).

Also the data subjects that a data breach concerns generally have a right to be informed of a personal data breach that is likely to cause a high risk for their rights or freedoms without undue delay. 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.

4.4.3. 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 (GDPR Article 35; LED Article 27).

Considering that MARISA is a project where new technology to be used to monitor human action on an international scale is being developed, and that this technology, if misused, could threaten the fulfilment of numerous fundamental and human rights as well as other legal rights of the data subjects, it is obvious that a DPIA is mandatory for MARISA.

The DPIA according to GDPR shall contain at least:

1. A systematic description of the envisaged processing and its purposes, including the possible legitimate interests pursued by the controller

2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes
3. An assessment of the risks to the rights and freedoms of the data subjects
4. 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.

If a data protection officer has been designated, the controller shall seek her advice when carrying out the DPIA.

Prior consultation

The result of DPIA must be taken into account when planning control measures mitigating the risks. If controller is not able to mitigate the risks, it is obligatory to consult the supervisory authority before starting personal data processing activities (*'prior consultation'*). If the DPIA indicates that the processing would in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller is required to consult the supervisory authority prior to processing. (GDPR 2016; LED 2016.)

4.4.4. Data Protection Officer

Designation of a Data Protection Officer

When it comes to the controlling of personal data by competent authorities under the LED, the designation of a data protection officer is compulsory with few exceptions (LED 2016, article 32). Under the GDPR there are three cases in which a data controller is required to designate a data protection officer (DPO), all of which hold true for MARISA. The cases are:

1) If the processing is carried out by a public authority or body, except for courts acting in their judicial capacity,
2) If the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
3) 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. (GDPR 2016, article 37.)

The DPO may be a staff member of the controller or processor and may also fulfil other tasks and duties, 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. A group of undertakings may designate single DPO as long as the DPO is easily accessible from each establishment.

The Position and Tasks of the Data Protection Officer

The controller and processor shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data, and they shall support the DPO in performing her tasks by providing her with necessary resources, access to personal data and processing operations, and maintenance of her expert knowledge. The controller an processor are also responsible for ensuring that the DPO is not given any instructions regarding the exercise of her tasks, and that she is not dismissed or penalised for performing them. The DPO's tasks include at least the following:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
- to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with 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;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance
- to cooperate with the supervisory authority;
- to act 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.

The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

It is important to note that the DPO is not personally responsible for organization's GDPR / LED compliance; the controllers and processor are. DPO's role and responsibilities should be defined and documented for business model and it must be included in it. DPO will also have an effect on governance model where the roles and responsibilities of controller are defined in detail.

To answer to the requirements set out by the GDPR and the LED, as well as to reinforce awareness about Data Protection within the Project, MARISA has appointed a DPO and established a Data Protection and Ethics Team (DPET) that oversees the implementation of ethics and data protection at Consortium members' level.

4.4.5. Codes of Conduct and Certification

The GDPR includes provisions regarding the creation and approval of codes of conduct and the accreditation of different data protection certifications, seals and marks. The purpose of these tools is to facilitate the proper application of the GDPR and the demonstration of compliance. However, the mere adherence to a code of conduct or the obtaining of a certification, seal or mark does not in itself constitute proof for compliance with the GDPR.

Different associations and other bodies that represent categories of data controllers and processors can devise codes of conduct. One benefit with this is that it also allow for the specific features of the various industries and processing sectors to be taken into account. The national supervisory authorities or the European Data Protection Boad can approve and register them, and the Commission may decide that they have general validity within the union. Codes of conduct shall contain mechanisms that enable the mandatory monitoring of compliance with its provisions by the controllers or processors that undertake to apply it.

The establishment of data protection certifications, seals and marks is encouraged. Accredited certification bodies handle the issuing of such certifications, and the European Data Protection Board maintains a publicly available register of the certification mechanisms, seals and marks. The certifications shall be voluntary and available via a transparent process.

4.5. Transfers to Third Countries or to International Organizations

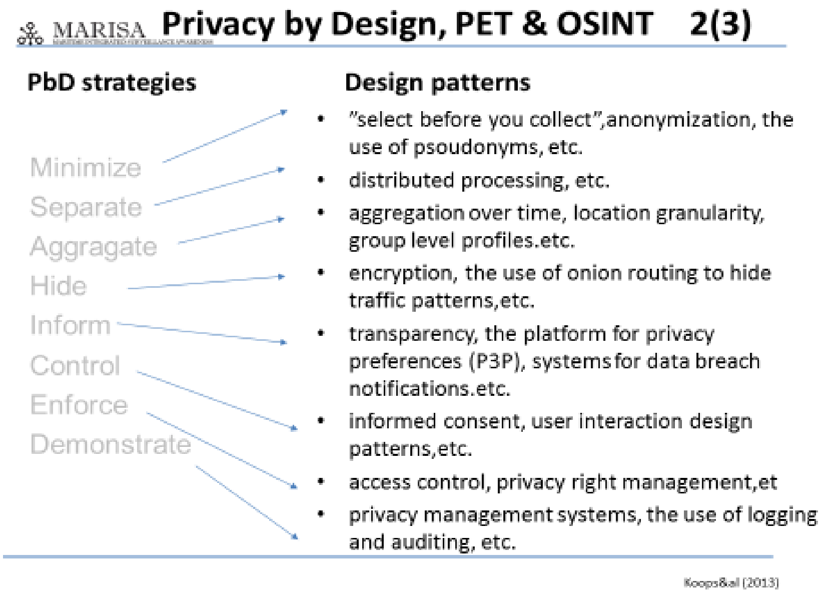
GDPR and LED also regulate the transfers of personal data to countries outside EU and to international organizations that don’t fit into the territorial scope of the regulation. No special permission is needed for the transfer if the Commission has decided the target country or organizations has guaranteed 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. (GDPR 2016, articles 45 &49; LED 2016, articles 35-40.)

5. Privacy by Design and Privacy Impact Assessment

5.1. Privacy by Design

Privacy by design (PbD) is an approach to systems engineering approach intended to ensure privacy protection from the earliest stages of a project and to be taken into account throughout the whole engineering process, not just in hindsight. The PbD concept is closely related to the concept of privacy enhancing technologies (PET) published in 1995. The concept is an example of value sensitive design that takes human values into account in a well-defined manner throughout the whole process. According to Antignac and Le Métayer (2014) research on PbD has focused on technologies rather than methodologies and on components rather than architectures. They advocate that PbD should be addressed at the architectural level and be associated with suitable methodologies, among other benefits, architectural descriptions enable a more systematic exploration of the design space. In addition, because privacy is intrinsically a complex notion that can be in tension with other requirements, they believe that formal methods should play a key role in this area. (Antignac & Le Metayer 2014) Kung (2014) continue the importance of architecture in designing a PbD system and provides an overview on how architectures are designed, analysed and evaluated, through quality attributes, tactics and architecture patterns. He also specifies a straw man architecture design methodology for privacy and present PEAR (Privacy Enhancing Architecture) methodology. Martin & Kung (2018) posit that for PbD to be viable, engineers must be effectively involved and endowed with methodological and technological tools closer to their mindset, and which integrate within software and systems engineering methods and tools.

Privacy by Design (PbD) is one of the key requirements in the European Data Protection Reform. It is included both in the GDPR and the LED. PbD refers to the philosophy of privacy protection from the early design state of technology. There are seven foundational principles of the 'Privacy by Design' approach: 1) Proactive not Reactive, Preventative not Remedial; 2) Privacy as the Default Setting; 3) Privacy Embedded into Design; 4) Full Functionality – Positive-Sum, not Zero-Sum; 5) End-to-End Security – Full Lifecycle Protection; 6) Visibility and Transparency – Keep it Open; 7) Respect for User Privacy – Keep it User-Centric. As Koops & al. (2013) argue, several PbD functionalities can be embedded in OSINT. The functionalities concern so called Privacy Enhancing Technologies. In the table there are summarised typical functionalities and correspondent PETs. (Koops 2013).



MARISA Privacy by Design, PET & OSINT 2(3)

PbD strategies

Minimize
Separate
Aggregate
Hide
Inform
Control
Enforce
Demonstrate

Design patterns

- ”select before you collect”,anonymization, the use of psoudonyms, etc.
- distributed processing, etc.
- aggregation over time, location granularity, group level profiles.etc.
- encryption, the use of onion routing to hide traffic patterns,etc.
- transparency, the platform for privacy preferences (P3P), systems for data breach notifications.etc.
- informed consent, user interaction design patterns,etc.
- access control, privacy right management,et
- privacy management systems, the use of logging and auditing, etc.

Koops&al (2013)

Figure 3: Privacy by Design Strategies and Design patterns (by Koops & al. 2013)

When it comes to the use of OSINT and Privacy Enhancing approaches, it will be end-users who determine to what extent PbD will be embraced. But platform provider at least has a responsibility to make sure that end-users are enabled to use PbD by allowing above functionalities (VIRTUOSO 2012a; Koops 2013.)

Furthermore, the VIRTUOSO report highlights two approaches as promising to explore in particular. One approach uses a policy mark-up language, such as XACML, to define Enterprise Privacy Policies, which determine appropriate data handling, including purpose specification of data collection, and data access policies. If all data processing within a system is described in data access and data handling policies and the actual personal data contain the appropriate metadata, a policy engine can then enforce the policies during runtime. The other approach is the concept of revocable privacy with spread responsibility. In that approach the combination of pseudonyms and secret sharing ensures that data subjects remain unidentified, unless two or more designated authorised persons give permission to de-anonymizing collected data. (VIRTUOSO 2011.)

Privacy by Design (PbD) Approaches
1. Revocable Privacy a) Spreading responsibility b) Self-enforcing architecture 2. Enterprise Privacy Policies and Technologies for Legal Compliance a) Purpose specification b) Legal basis or legitimate ground c) Collection and use limitation/data minimization d) Data quality e) Rights of data subject f) Security safeguards

Table 7: Privacy by Design approaches (by the VIRTUOSO Project)

Whether revocable privacy is a feasible approach for OSINT will depend on several factors: the nature of the investigation (e.g., whether it focuses on individuals or on objects or broader trends), the relevance for the investigation of mapping networks of individuals, the precision with which the identities of relevant individuals can be recognised by the system, and the stage(s) of the investigation in which recognisable individuals or connections between individuals need to be analysed. This requires an in-depth analysis for specific OSINT settings (VIRTUOSO 2012a.)

Enterprise Privacy Policies consist of data handling and data access policies. They specify the conditions under which certain personal data will be processed and for which purposes. If all data processing within a system is described in these policies - and the personal data contain the appropriate metadata - a policy engine can then enforce the policies during runtime. This can ensure that only authorised data requests are honoured for the right purposes (VIRTUOSO 2012a.)

In many respects, original PbD framework has been criticised as being a vague concept. To make its underlying goals more concrete, Colesky Hoepman & Hillen (2016) propose more specific privacy design strategies: 1) minimise: only collect that data which is strictly necessary, and remove that which no longer is; 2) hide: encrypt, pseudonymise, and take other measures that protect and obscure links between elements of data and their source; 3) abstract: reduce the granularity of data collected; combine or aggregate data from multiple sources so that the sources are no longer uniquely identifiable; 4) separate: store and access data only where it is used; process data at the source instead of centrally; 5) inform: explain to data subjects how their personal data is processed, and how profiles and automated decision-making based on their personal data work. A subject can only provide valid consent to data processing if they understand how their data is being processed; 6) control: allow data subjects to provide and revoke consent to process, and to access, correct, and delete their provided and derived data: 7) enforce: build technical and organizational measures that ensure the design decisions taken with regard to privacy are actually implemented, and log the actions of the systems; and 8) demonstrate: document, audit, and report on the operational and PbD processes. The first four strategies are more focused on data and the last four are about policies and the surrounding processes. Given these strategies, the PbD process could then ideally be implemented as follows (Van Aubel, et al., 2018): 'look at each project requirement, figure out what potential privacy impacts it has, and apply strategies to mitigate those impacts'. This iterative process should be repeated as the design becomes more detailed (Van Aubel et al. 2018) and the first step in each iteration involves performing a Data Protection Impact Assessment (DPIA).

5.2. Data Protection Impact Assessment

Where 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, the GDPR obliges the controller to carry out a Data Protection Impact Assessment (DPIA) prior to the processing. This is definitely the case with MARISA.

The purpose of a DPIA to identify and minimise data protection risks as the initial step of any new project. DPIA is a process designed to describe the processing, to assess its necessity and proportionality, and to help manage the risks that it involves. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the legislation. DPIA is, thus, a tool for building and demonstrating compliance. According to Coles, Faily and Ki-Aries (2018) DPIAs should be relatively cheap to implement with sufficient resources and tools. However, while there is advice on the legal requirements for DPIA and the elements of what practitioners should do to undertake a DPIA, there has been little prescription about how security and privacy requirements engineering processes map to the necessary activities of a DPIA, and how these activities can be tool-supported. (Coles, et al. 2018.)

Coles, et al. (2018) have studied existing Privacy Requirements Engineering approaches and tools to support carrying out DPIAs. The existing approaches capture the central elements of DPIA, but are lacking in two particular ways. First of all, more comprehensive prescriptions are needed to indicate what tools and techniques map to different stages of a DPIA. Secondly, such stages need to be adequately tool-supported, so that data input in one stage can be used to support reasoning and analysis in the subsequent others.

Their main contributions of Coles et al. (2018) are: 1) existing requirements 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; 2) demonstration how an exemplar for Security Requirements Engineering tools supports and helps reason about potential GDPR compliance issues as a design evolves; and 3) 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.

6. Challenges with the Legislation and Other Values

In this section we shed light on the ethical and societal dimensions of maritime surveillance operations aided by solutions such as MARISA. 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 MARISA. 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 MARISA 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, Jaendesboz 2011, 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 Surveillance 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 MARISA are similar to those of maritime surveillance in general. However, MARISA's more efficiency and capacity in maritime surveillance highlights the importance considering these challenges and opportunities not only when designing the MARISA technology, but also as part of its user processes and business modelling.

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

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

MARISA as a Part of CISE	Sufficient Privacy Enhanging Technologies. Technical challenges of OSINT, Big Data and Artificial Intelligence.	Unethical ways of using MARISA data in decision making, Organizational challenges with OSINT, BIG Data and AI	Unethical aims of using MARISA in maritime surveillance

Table 8: Ethics and MARISA's various compositions

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 MARISA 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, MARISA 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 MARISA 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 MARISA, 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 MARISA. At least the following issues are to be deliberated further:

- How could we deliver information provided by MARISA 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. 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 2951). 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.

MARISA 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 MARISA 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 (see https://www.hrw.org/report/2009/09/21/pushed-back-pushed-around/italys-forced-return-boat-migrants-and-asylum-seekers) Misconduct such as this will be a significant concern also in the development and use of MARISA.

In addition to the above challenges, diplomatic aspects need to be considered. The use of MARISA 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 MARISA 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 MARISA’s interoperability and compliance with EUROSUR and CISE covers also these ethical issues (not only technology).

- MARISA 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.

6.4. The Displacement Effect

It is to be expected that the use of MARISA 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': 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 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. (see http://frontex.europa.eu/trends-and-routes/eastern-mediterranean-route) 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 MARISA:

1) Before the implementation of MARISA, it is crucial to always make a feasibility study and a societal impact assessment for MARISA 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 MARISA are to be carried out for the purposes of e.g. risk analyses. If MARISA is sold stand-alone system instead of as part of the CISE ecosystem, this information sharing must be designed separately.

6.5. Human Collaboration, Technology and Information Sharing

To increase the Maritime Security actor's willingness to collaborate across disciplines, several ethical aspects need to be addressed in order to enhance trust not only towards MARISA 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 security related information does not lead to harsh or unsafe treatment of people or use of technology. These factors play a role also in MARISA, 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 MARISA. Factors related to the design of MARISA are likely to influence the level of acceptance the toolkit receives: the fact that the use of certain technologies in maritime 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 MARISA 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 MARISA 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 MARISA.

Several technologies are used among the MARISA 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 MARISA project.

MARISA 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 Alfresco and MARISA 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	

Table 9: MARISA Information Sharing

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.

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.

Table 10: Information Sharing Behaviour in General (by Xie 2011)

6.6. 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 behavior 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 every day 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. 2015.)

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. 2015.) 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 marine surveillance and SAR contexts.

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	This is the tendency of being influenced by information that is already known or that is first shown, 'first impression'.
Overconfidence 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.
Framing bias	This happens when we are influenced by the way in which information is presented rather than the information itself.
Omission bias	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.

Table 11: Examples of Cognitive Biases

6.7. 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 MARISA project (see also separate chapter on SIA).

6.7.1. 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).

6.7.2. 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).

6.7.3. 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.

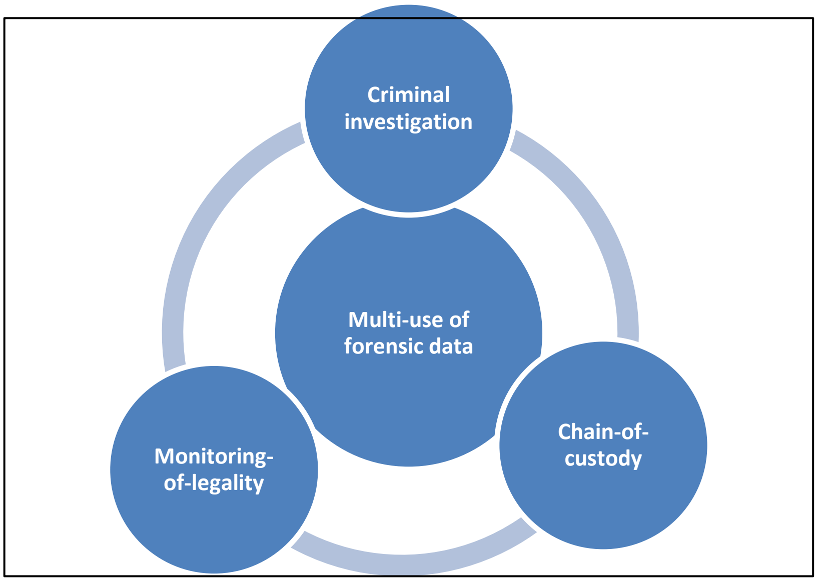


Figure 4: Multi-use of Law Enforcement Sensor Data

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).

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

Table 12: Stakeholders and their needs for LEA operations (by Rajamäki & al 2012)

6.8. The Misuse of MARISA 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 MARISA are the points three and four. If we move our focus from the MARISA project and its research to the proposed MARISA 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 MARISA provides (including also military tracks)
- The use of the MARISA solution for purposes which are un-ethical and out of the scope of original purpose

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

- By capturing the MARISA data when it is transformed from its data sources to the MARISA platform
- By hacking the MARISA platform and its data bases
- Due to the human information leakage when somebody having access right to the MARISA 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 MARISA technology and data transfer, on user processes and access rights and finally on the governance model of the MARISA solution, including the processors and controllers of the MARISA data (see the EU Data Protection regulation discussed later).

The misuse of the whole **MARISA solution** is strongly linked to the business/adoption models of the **MARISA**, and especially as stand-alone solution. The key question is that how we can make it sure that the **MARISA** 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 MARISA and their development during the MARISA 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 MARISA 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 MARISA.

7. OSINT, SOCMINT, Big Data and AI

In this chapter, a legal-ethical framework regarding the use of OSINT, SOCMINT and Big Data and AI in maritime surveillance is presented. Achievements in earlier projects (especially VIRTUOSO and MEDI@4SEC) are taken into consideration and discussed. In the last sub-section, we elaborate on the new ethical guidelines for trustworthy artificial intelligence, created by a high-level expert group on artificial intelligence, and published in April 2019.

7.1. OSINT

OSINT is intelligence collected from publicly available sources, including the internet, newspapers, radio, television, government reports and professional and academic literature (Glassman and Kang 2012). OSINT binds through a systematic analysis process as a tight and informative thematic entity the scattered information to be obtained from the open sources. During the last few years, the Internet and especially the channels of the social medium have revolutionised the ones which had significantly increased the amount of OSINT and information to be analysed. The basic character which networks a social medium has led to different graphic manners of representation in modern OSINT and for visualizations and for even the better identification of the connections of the matters.

OSINT has also been called ethical hacking, in other words hacking which does not break laws and it is used for good from the psychologist or physical manipulations for getting of the information. OSINT requires the knowledge of the network environment with a good performer, a comprehensive means selection and problem-solving skill. Ethical questions apply to the handling of the collected information. When collecting data from the persons, one must remember that the creation of person registers is tightly regulated. In the TOR network doxing is talked more often instead of OSINT even though sometimes the difference may be subtle. The words become a Doxing term, ´documents´ and ´docs´ and mean from the Internet from the different electric documents quarried by the personal data.

On the market there are numerous efficient network analysis tools some of which also are used by the LEAs. Wells & 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 prioritise 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 prioritises 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 (Wells & Gibson 2017).

The International and EU regulation for **OSINT** includes the regulations and conventions named in the table below (right column). But Even though international regulatory guidelines are available, specific allowances, prohibitions and exceptions mainly stem from national legislation. (Koops & al. 2013; VIRTUOSO 2011.)

Koops et. al. (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. European Data Protection Reform partly harmonises the general data protection regulation in EU countries (General Data Protection Regulation GDPR), but in case of law enforcement and crime prevention it still offers variation in the national level legislation (Law Enforcement Directive LED).

Hu (2016) identifies five key concerns relating to OSINT:

1) *The origin and intent of the intelligence can bias the data sample and create mislead analysis. Was the publicly available information initially cherry-picked to fit a certain narrative while the rest was discarded? What if the original source of the information was initially classified but subsequently obtained through hearsay?*
2) *The fact that information is unclassified does not mean that individuals or groups won't get hurt if that information is publicised. How can we ask questions to reflect the concerns of those reflected in the data, especially if it is not possible to get back in touch with that particular group? What trade-offs need to be made?'*
3) *Even when one dataset is de-identified, it is still possible to combine it with other datasets to re-identify an individual or group. Should we use these techniques to develop insights on individuals or groups? What if they are harmful to others? Are there best practices to follow, especially when the data involves particularly vulnerable groups?'*
4) *Many OSINT-related cases involve cleaning, organizing and analysing deluges of raw data. Algorithms, workbenches and machine learning can speed up this process significantly. Yet no technology platform is infallible, and the resulting analysis could have harmful consequences if it is wrong. How far should one rely on these methods? What's the balance between machine and human power? Are there common pitfalls to avoid, or ways to make explicit the decisions that have gone into analysing the data?'*
5) *Do we have a responsibility to share and publish some of this information more widely if it is in the public interest – even if doing so might harm individuals or groups? How can we maintain their trust while still making sure that no one gets hurt? How do we decide who we work with and when? How do we ensure that the rights of individuals reflected in our data are respected at all points of this process?' (Hu, 2016.)*

These key concerns are gathered in the table below (left column) together with corresponding regulation (right column).

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	European Fundamental Rights European Convention on Human Rights Cybercrime Convention EU Data Protection Regulation

Publicity and visibility	IPR legislation Liability Regulation of investigative agencies

Table 13: Legal and Ethical Framework for OSINT (by the VIRTUOSO Project)

Koops et al. (2013) considers the challenge of embedding PbD in OSINT carried out by law enforcement. Ideally, the technical development process of OSINT tools is combined with legal and ethical safeguards in such a way that the resulting products have a legally compliant design, are acceptable within society (social embedding), and at the same time meet in a sufficiently flexible way the varying requirements of different end-user groups. Koops, Hoepman and Leenes use the analytic PbD framework and they discusses two promising approaches, revocable privacy and policy enforcement language. The approaches are tested against three requirements that seem suitable for a ‘compliance by design’ approach in OSINT: purpose specification; collection and use limitation and data minimization; and data quality (up-to-datedness). For each requirement, they analyse whether and to what extent the approach could work to build in the requirement in the system. They demonstrates that even though not all legal requirements can be embedded fully in OSINT systems, it is possible to embed functionalities that facilitate compliance in allowing end-users to determine to what extent they adopt a ‘privacy by design’ approach when procuring an OSINT platform, extending it with plug-ins, and fine-tuning it to their needs. Therefore, developers of OSINT platforms and networks have a responsibility to make sure that end-users are enabled to use PbD, by allowing functionalities such as revocable privacy and a policy enforcement language. Even though actual end-users have a responsibility of their own for ethical and legal compliance, it is important to recognise that it is questionable whether all responsibility for a proper functioning and use of OSINT platforms can be ascribed to the end-users; and some responsibility for a proper functioning of OSINT framework in practice also lies with the developers of the platform and individual components. (Koops & al. 2013.)

7.2. SOCMINT

SOCMINT can be defined as the analytical exploitation of information available on social media networks. It identifies social media content as an opportunity and challenge for open source investigations [59]. For example, Twitter is a popular and widely used social media platform for microblogging or broadcasting short messages. Twitter has hundreds of millions of users worldwide, and they broadcast over every day 500 million messages, known as tweets, that may include text, images, and links (Glasgow, 2015). In crisis management, Twitter can act as a human sensor network for real-time event detection, but little attention has been paid to applying text mining and natural language processing techniques to monitor events in a multilingual setting and most of the work focusses on one single language only (Zielinski, 2013). According to some scholars, the surveillance of social media should be removed from the definition and discussion about OSINT and treated as an issue of its own (Wood 2016).

The concerns that Hu (2016) identifies relating to OSINT are also relevant to SOCMINT. However, the ability to monitor millions of social media accounts and hashtags in real time, and to then analyse and store this data, is a concern unique to social media. According to Wood (2016) we need to challenge the argument that SOCMINT is an inexpensive strategy with little impact on people’s privacy because it relies only on so-called publicly available (i.e. non-private) information. Social media does not easily fit into either the category of public or private. We would argue that it is instead a pseudo-private space, where there is an expectation of privacy from the state. (Wood 2016.) The grey zone is a space of transition where legitimate and legal methods pass into illegitimate and illegal methods but are neither specifically allowed nor specifically forbidden; and the ethics and morality of these methods are questionable (Podbregar, 2016).

MEDI@4SEC project identifies legal and ethical issues of SOCMINT 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 summarised in the table below (MEDI@SEC 2014a; MEDI@SEC 2014b):

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 enforces of the law, data controllers) 2)Fundamental rights of the citizens 3)Involvement of citizens in the provision of the public security **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	Difficulty to ensure transparency, accountability and non-discrimination. Without a democratically legitimised authority, citizens are driven by their own interpretations of the law and morality. 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

Table 14: Ethical and Legal Challenges of SOCMINT (by the MEDI@SEC project)

7.3. Big Data

Considering the potentially huge amount of data to store in MARISA concept, it is proposed to adopt an original 'Big data' approach (e.g. the Hadoop solution). In practice, 'Big Data' regroups a set of techniques/tools suitable for this storing and processing such datasets with, usually, a 'NoSQL' approach. The MARISA toolkit was built on the top of a big data infrastructure that provides the means to collect external data sources and operational systems products and to organise and exploit all the incoming data as well as all the data produced by the various services.

Big data means a large amount of information which with traditional methods would be found very troublesome and defective to be processed or visualised. Data science makes the analysis and use of the information in the sensible way possible. The use of OSINT in a professionally way requires a suitable trace analysis which is characteristic for Big Data. The amount of the information is huge through open sources and it is cheap to get it. The data science and Big Data help in the surveying, collecting, division and analysing of huge stores of information (Passos 2016, 392, 394-395).

Capabilities to gather, analyse, disseminate, and preserve vast quantities of data raise concerns about the nature of privacy and the means by which individual privacy might be compromised or protected. Anonymity overlaps with privacy, but the two are not identical. Likewise, the ability to make intimate personal decisions without government interference is considered to be a privacy right, as is protection from discrimination on the basis of certain personal characteristics (such as race, gender, or genome). Privacy is not just about secrets. Next, we look privacy challenges in four different dimensions of BDA: 1) data generation and collection, 2) data analysis, 3) use of data, and 4) technology and infrastructure behind data.

7.3.1. Data Generation and Collection

Data generation can be classified into active data generation and passive data generation: active data generation means that the data owner will give the data to a third party, while passive data generation refers to the circumstances that the 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 (Jain;Gyanchandani;& Khare, 2016). Individuals constantly emit into the MARISA environment information whose use or misuse may be a source of privacy concerns. Physically, these information emanations are of two types, which can be called 'born-digital' and 'born-analog.' Born-digital information is created by the individuals themselves or by a computer surrogate, specifically for use by a computer or data processing system. When data are born digital, privacy concerns can arise from over-collection. Over-collection occurs when a program’s design intentionally, and sometimes clandestinely, collects information unrelated to its stated purpose. Over-collection can, in principle, be recognised at the time of collection. Born-analog information arises from the characteristics of the physical world. Such information becomes accessible electronically when it impinges on a sensor such as a camera, microphone, or other engineered device. When data are born analog, they are likely to contain more information than the minimum necessary for their immediate purpose, and for valid reasons. One reason is for robustness of the desired 'signal' in the presence of variable 'noise' interconnection between the developed services develops meta-data from all data to be transmitted. Metadata are ancillary data that describe properties of the data such as the time the data were created, the device on which they were created, or the destination of a message. Included in the data or metadata may be identifying information of many kinds. It cannot today generally be asserted that metadata raise fewer privacy concerns than data.

The MARISA Toolkit has two relevant data sources: 1) data coming from the sensors, and 2) data coming from open sources. With regard to data coming from the sensors, these sensors are embodied in the operational environment of the Legacy Systems. Here Legacy Systems mean the previously existing end-users Maritime Surveillance systems in the National/Regional Coordination Centres or Coastal Stations to which MARISA Toolkit must establish some kind of communications. In these environments, owned by Participating Member State governmental entities, we can suppose that the data are used on the basis of need-to-know and need-to-share. Examples of those data from heterogeneous sources are radar and AIS tracks, AIS data validation, near real-time satellite detections and heat maps, integration of maps of most used routes (density maps) and traffic patterns, search and rescue risk maps, fusion of surveillance pictures information from end-users' operational environments.

MARISA services include three services (Twitter service, GDELT service and OSINT service) that collect open source information. Their main target is to extract and integrate maritime related safety and security events. OSINT service mainly collects its information via Twitter service and DGELT service. From data collection point of view, MARISA GDELT service may not have privacy concerns because professional journalists should have taken that issue into account when making news. However other ethical issues may arise, for example wealthier countries not only continue to attract most of the world news attention, they are also more likely to decide how other countries perceive the world (Guo & Vargo, 2017).

ln Twitter, several technical features and tweet-based social behaviors occur that might compromise privacy. Tweets are complex objects that, in addition to the message content, have many pieces of associated metadata, such as the username of the sender, the date and time the tweet was sent, the geographic coordinates the tweet was sent from if available, and much more (Glasgow, 2015). 'Most metadata are readily interpretable by automated systems, whereas tweet message content may require text processing methods for any automated interpretation of meaning' (Glasgow, 2015). 'Direct Messages' are the private side of Twitter and 'retweeting' is directly quoting and rebroadcasting another user's tweet. Someone might unintentionally or intentionally retweet private tweet to a public forum. Other behaviors include mentioning another user in one's tweet that is, talking about that user. According to Rumbold and Wilson (2018), when one puts any information in the public domain—whether intentionally or not—one does not waive one's right to privacy, but one can only waive one's right to privacy by actually waiving it.

7.3.2. Data Analytics

After data are collected, data analysis techniques (termed 'analytics') come into play and may generate an increasing fraction of privacy issues. By analytics, nonobvious and sometimes private information can be derived from data that, at the time of their collection, seemed to raise no, or only manageable, privacy issues. Data fusion occurs when data from different sources are brought into contact and new facts emerge. Individually, each data source may have a specific, limited purpose, but their combination may uncover new meanings. Such new information, used appropriately, may often bring benefits to individuals and society. However, the wide variety of potential uses for big data analytics raises crucial questions about whether our legal, ethical, and social norms are sufficient to protect privacy and other values in a big data world. (US Executive Office 2014a; US Executive Office 2014b.)

The 'brain' of MARISA is enhanced data fusion and analysis to improve marina surveillance as well as search and rescue with respect to response time and situational awareness. Because of data fusion in MARISA, privacy concerns may not necessarily be recognizable in born digital data when they are collected. Because of the signal processing robustness and standardization, the same is true of born analog data – even data from a single source (e.g., a single camera). When born digital and born analog data are combined with data fusion, new kinds of data are generated from data analytics.

Big data may be analyzed 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 behavior (Moallem, 2019). According to Wójtowicz and Cellary (2019), one of the most important carateristics of BDA is the paradigm shift, in which instead of discovering knowledge by searching for causality, one can discover it by searching for correlation: it is possible via BDA to learn with high propability what is happening, and even what will happen, but not why it happens or why it will happen. If a human programmer writes a program, another human programmer may inspect program code and find possible errors, but if a neural network is trained by peta-bytes of data, nobody is able to check whether a particular prediction is correct or not (Moallem, 2019).

Algorithms tell computers step by step how to solve a certain problem. However, predictive algorithms are often themselves unpredictable (Wójtowicz & Cellary, 2019). According to Rahman (2017), the first problem comes from algorithmic bias—AI algorithms being a reflection of the programmers' biases—may possibly give rise to the risk of false alerts by AI surveillance systems thus resulting in wrongful profiling and arrest; and the second problem is that AI profiling systems utilize historical data to generate lists of suspects for the purposes of predicting or solving crimes. ML techniques including neural networks run in two phases (the training phase and the prediction phase) and the 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 (Rahman, 2017).

7.3.3. The Use of Data

Data analysis does not directly touch the individual (it is neither collection nor, without additional action, use) and may have no external visibility. By contrast, it is the use of data (including born- digital or born-analog data and the products of data fusion and analysis) that can cause adverse consequences to individuals. Violations of privacy are possible even when there is no failure in computer security. If an authorised individual chooses to misuse data, what is violated is privacy policy, not security policy. Or, as we have discussed privacy may be violated by the fusion of data – even if performed by authorised individuals on secure computer systems.

An important ethical issue comes with automated policing. Automated discrimination is possible when augmented surveillance becomes more common. It intersects with the technical issues of unintended biases in algorithms and big data that could skew analyses generated by AI systems (Rahman, 2017). If a person is wrongly qualified as a potential terrorist, the consequences may be very severe (Wójtowicz & Cellary, 2019). If Big Data Analysis provides predictions with 99% accuracy, wrong predictions would concern over 5 million people in the EU, which population is 508 million. Big Data used by law enforcement will increase the chances of certain tagged people to suffer from adverse consequences without the ability to get back or even having knowledge that they are being discriminated (Matturdi, Zhou, Li & Lin 2014).

7.3.4. Infrastructure Behind Data

Data analytics requires not just algorithms and data, but also physical platforms where the data are stored and analysed. The related security services used for personal data are also an essential component of the infrastructure. Good cybersecurity enforces policies that are precise and unambiguous. On the other hand, compromised cybersecurity is clearly a threat to privacy. Privacy can be breached by failure to enforce confidentiality of data, by failure of identity and authentication processes, or by more complex scenarios such as those compromising availability.

Cloud computing is currently the most economic option of providing computing power and storage capacity. Privacy assurance can be successfully deployed in private clouds. Although stored data are encrypted and advances in homomorphic encryption, there is no prospect of commercial systems being able to maintain this encryption during real-time processing of large datasets (Wójtowicz & Cellary, 2019). The security and privacy for big data is not different from security and privacy research in general (Nelson & Olovsson 2016).

7.4. Trustworthy Artificial intelligence and MARISA

The High-Level Expert Group on Artificial Intelligence provided the AI Ethics Guidelines to the Commission in March 2019. The AI Ethics Guidelines forms 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. (AI-ETHICS 2019.)

The framework does not explicitly deal with the 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 (AI-ETHICS 2019) can be summarised from MARISA'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 developing, deploying or using the systems, and adapt it to the specific use case in which the system is being applied. (table below). 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.

1.Human Agency and Oversight

Fundamental Rights:

Did you carry out 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?
- 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)?

The Fall-back Plan and General Safety:

Did you ensure that your system has a sufficient fall-back 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/fall-back plans?
- Did you define and test fall-back 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, anonymization and aggregation?
Where a Data Privacy 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

A 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 Impacts:

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 it has 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?

Table 15: Trustworthy AI assessment list (by the AI ETHICS 2019)

8. Social Impact Assessment (SIA) for MARISA

This chapter contains a Societal Impact Assessment (SIA) for MARISA. The AI issues that have been raised and the way they have been handled in the project are analysed in the summary. The social impacts of MARISA were discussed for the first time already in the MARISA project proposal, and the first SIA was provided in the internal deliverable 'Ethical, Legal and Societal aspects of MARISA D2.3' in the autumn of 2017. Since values and opportunities have already been discussed thoroughly in the MARISA Grant Agreement and in the description of work, the focus in this SIA is laid on the societal barriers and challenges of MARISA.

8.1. 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 MARISA 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 MARISA Kick-off Meeting in May 2017, from WP2 end-user's workshops in July 2017, from literature provided by VIRTUOSO project, from Laurea networks and from Laurea Master level students of both Security, Social and Healthcare and Business. Finally there has been organised several possibilities for the partners to comment and contribute to the analysis.

8.2. 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. The column on the right explain the situation with the activities already performed and work still to be done.

Challenge	Activities needed	Activities performed	Work to be done
Justification of MARISA **>Way of life, fears and aspirations** **>Culture and community** **>political system** **>personal rights**			
People may feel suspicious and untrusting towards the MARISA technology and/or the authorities using it; concerns about MARISA 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. MARISA must substantiate that it is necessary in democratic society, and its use must be proportional to the justified goals.	The main characteristics of MARISA were presented to the User community and to the external experts, including a) the security requirements and b) the specific attention devoted to the data security aspects. In MARISA platform data is accessed through authenticated access to the network. Persistence of data is also guaranteed by the authentication module.	The next two MARISA Workshops (May 2019 and December 2019) will enforce those concepts defined and communicated earlier in MARISA workshops. Moreover, the MARISA Consortium will try to involve as many stakeholders as possible up to the end of the project.
MARISA 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.	Ethics issues have been a central focus throughout the first phase of MARISA. Those responsible for the different deliverables are in charge of the Ethical Compliance Check tables/of demonstrating how the ethical and societal guidelines for MARISA are taken into account (these documents can be found as Annexes in all the relevant MARISA deliverables). In addition, the MARISA Societal Impact Assessment (SIA) is updated and presented in this deliverable.	The same ethical governance model, which includes ethics compliance checks for each deliverable, continues till the end of the project.
The use of MARISA in e.g. the Mediterranean will probably cause a	The information sharing to border management authorities (Frontex) is essential to develop and maintain	Contacts have been taken with Frontex to promote information sharing and improve the overall	The contacts created shall be kept alive throughout the project.

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.	an awareness of the big picture of the situation and to react appropriately. In case MARISA is sold as stand-alone solution outside EUROSUR/CISE, any information sharing is to be organised so that the ethical and legal concerns relating to migration, human trafficking and smuggling are taken into account in an appropriate manner.	picture. MARISA was presented in the frame of a Border Security Workshop at Frontex premises in Varsaw, while Frontex representatives have been invited and participated to the User Community meetings and to the first MARISA Workshop.	
MARISA 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.	In order to capture the relevant operational needs and to validate the results, the MARISA concept, including the list of the data fusion services, were defined through a strong involvement of the user community. Two User Community meetings were held during the first year (Helsinki, Madrid), and a third meeting in December 2018 (Lisbon) before starting the second phase. The third meeting intended to review the original needs and improve the requirements and the operation scenarios as needed. The MARISA User Community included 'end user practitioners', partners, associates, maritime and surveillance experts.	Cultivate continuous end user communication and enhancement of the usability of MARISA.
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 MARISA's technical capacities is limited by laws and other 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 MARISA tire', and even make it obsolete from the start.	MARISA 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.. Various layers of ethics shall be implemented for the different MARISA 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 MARISA research and development, but for the future use of MARISA solution (unless the legislation will change, or the data fusion based on phenomena will be ready).	MARISA has not (and will not) use personal data or identify individuals although it processes personal data. The design of the technical solution and user processes have been based on the privacy by design (PbD) approach and other GDPR recuirements (such as data and purpose minimisation and storage limitation). As a result of this, the possiblity of a high risk personal data breach has largely been eliminated. In the first phase of the project, during the pilots, personal data were not be processed. Moreover, the toolkit Data Fusion services processing social media info (i.e Twitter Services) were not available for Phase 1 trials. Therefore, in all the phase 1 trials, there was no way to access and process personal data from social media. A paper describing data protection policy during the trials was provided as part of the pilot materials.	In order to assure that the Project is compliant with the GDPR also during the Phase 2, a Data Protection and Privacy Impact Assessment (PIA) will be performed before the second phase trials and during them. For any instance where compliance with the GDPR cannot be ensured during the pilots, simulated (fake) data will be utilised (e.g. social media data).
MARISA 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 MARISA solution shall be heard and implemented appropriately.	The MARISA Toolkit includes a number of services that help to plan SAR missions and help to optimise time use and other resources during SAR operations. These services deal with the location of vessels, risk analysis based on knowledge about previous incidents, sea and weather conditions, behavioural and predictive analysis of vessels. A scenario with a SAR incident was already designed and executed in the frame of the North Sea trial.	Additional SAR scenarios will be executed during the second phase with the involvement of the end users, in order to validate more in-depth related services providing anomalous behaviour capabilities, ship prediction and risk maps identification.
The use or MARISA 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).	This challenge has not been faced since no activities or actions have been accomplished on the specific aspects.	In the second phase the issue will be discussed with the appropriate organizations in order to ensure the respect of relevant laws.
Ethical issues in MARISA are linked to politics.	Lobbying/influencing political organizations.	No specific activities and/or actions have been carried out on this aspect.	The plan is to consolidate the MARISA adoption models in the early 2019 and, on that

			basis, define the preliminary Business Model for MARISA.
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 MARISA provides, 'Duty to render assistant' principle may bring more work the SAR organizations using MARISA.	When implementing MARISA, points of contact/national coordination centrals in the area MARISA 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 MARISA. Third countries in the sea in case should be seen as end-users of the MARISA 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.	MARISA Operational trials did not operate on the waters of third countries. The choice made in MARISA is not to deploy specific MARISA platforms or sensors and rather use the resources of the end-users in their daily operations. The principle 'MARISA does not envision operations which are not taking place with strict adherence to international maritime regulations' is embedded in MARISA code of conduct.	The principle 'MARISA does not envision operations which are not taking place with strict adherence to international maritime regulations' is to be taken into account in MARISA businesss model.
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.	A first training session was taken in order to show how to use the services dealing with the threaths detection and identification.	This aspect will be addressed more in depth in the second phase when the Level 3 services dealing with decision making and reaction capabilities will be available.
Cultural Differences and The Nature of ethics in Maritime Surveillance **>Culture and Community** **>Political Systems**			
Ethics is case-dependent. The ethical sensitivity of the decisions made with the help of MARISA 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 MARISA 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.	No activities or actions have been accomplished on the specific aspects. This challenge has not been faced in the first phase of the project.	This challenge is followed up during the second phase pilots.
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	Market research early enough (as part of the business model) to be able to adapt the features of MARISA 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	In the first phase, a preliminary definition of the MARISA adoption models was carried out, taking into consideration different legislation at EU and member state levels. The MARISA Operational trials cover different areas and operational needs (from the North Sea, to the Mediterranean Sea, including The	In the second phase, further work analysis is planned, with the active involvement of MARISA end-users in order to propose viable operational adoption models for proposed MARISA toolkit from one side, and to identify feasible business models for MARISA

on user processes and training, and finally to the business models.	trials. Lobbying and political influencing for synchronizing the legislation. Properly managed PR and communication and dissemination.	Balearic Sea, The Ionian and Aegean Seas, and The Strait of Bonifacio).	exploitation and dissemination.
Failure to share information due to the conflicting priorities in maritime surveillance .	Discussion and distribution of information.	The MARISA end users come from different countries, five end-users from The Netherlands, Spain, Italy, Greece and Portugal are involved as full partner. Continuous discussions have been held.	Continuous discussions have been planned also for the second phase.
Difficulties in the sharing of classified information due to the fact that confidentiality and integrity law are not developed at a central level.	Lobbying.	In the first phase no need of sharing classified information to exercise the MARISA toolkit.	In the second phase, there can be the need to validate the services with classified information (up to EU restricted). This will be discussed on a case-by-case basis with the MARISA end-users.
End-users are not forced to share information for internal policies Will every subscribing user of MARISA 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 MARISA governance model.	Preliminary activities for the definition of the adoption models have been carried out in the first phase. Existing constraints/limitations with regards information sharing among end-users are being identified and analysed in order to propose Common rules for collaboration under MARISA governance model. These activities led to the identification of a range of models for the MARISA governance.	This task will continue in the second phase and will be considered in the finalization of the MARISA exploitation plan.
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.	Trust building is an important task in of the MARISA User Community. Moreover, one of the MARISA drivers is the protection of data Fusion Products based on the 'need-to-share' approach, to guarantee access and distribution of data fusion results among relevant stakeholders. MARISA on the one hand will process a great amount of raw data of different types, on the other hand will produce a relevant number of data fusion products.	Particular care will be devoted to the definition of controlled mechanisms for the data distribution.
MARISA & Liability Issues **>Culture and Community** **>Political Systems** **>Personal Rights**			

Confidence of MARISA 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).	MARISA has transparent model with estimation for probabilities for different situations and sub-situations. All the data fusion services will elaborate data according to data transformation predefined chains that have been integrated in a transparent way. The small elaboration chains will always ensure a total control of results. Users will always use their legacy systems and will be able to compare MARISA decisional suggestions with their consolidated mission planning tools.	
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)	Ethical requirements/limitations are always taken into account from the user requirements to the design of the toolkit to the storage of data. Human is the loop. These challenges have also been tackled and will be tackled during the validation of the toolkit in the frame of the Operational Trials. The definition of the operational scenarios including using both simulated data and with a specific choreography with real vessels allows to detect at the maximum extent the wrong processing of the toolkit.	
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. MARISA 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.		The mission planning system still have to be designed and new requirements will be added for the service in order to do an accurate design of the functionalities of the service.
Privacy and Data Protection **>Political Systems** **>Personal Rights**			
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	MARISA 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	MARISA technical solution and user processes have been designed based on the privacy by design (PbD) approach and other requirements defined by the General Data Protection Regulation (GDPR). These solutions are defined more in detail the specific technical notes produced in the frame of the project. A DPO has been appointed to MARISA. A Data Protection and Ethics team has been established to oversee the implementation of the GDPR and the LED.	Privacy and data protection issues are needed to be discussed within the consortium constantly. An education session on Data Protection needs to be arranged at least once per year.

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.	MARISA will not be used to the identification of individual, but to the identification of phenomenon (e.g. terrorism) The data fusion technology concerning the above issue is to be investigated as part of the MARISA 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	The system has been designed to assist decision-makers in the maritime environment. It does not collect data on the individuals. The purpose of the system is to be used in border security and emergency situations, focusing on the information provided by the users and not the users' identity. This is explained in detail in the technical documentation. Anonymization is done.	
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 new data protection regulation has been analysed and all the activities are performed in compliance with the data protection regulation.	
The ethical constraints on length of personal data storage for such MARISA application may hinder the requested MARISA 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.	This was not the case during the first phase.	This will be considered also in the second phase. The constraints shall be considered in MARISA training and implementation materials.
Privacy and data protection of MARISA 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 MARISA project much more complicated than during the pilots.		Dimensions & principles of MARISA data protection solutions are included in MARISA code of conduct.	Guidelines for Marisa organizational solutions are to be embedded both to the business model/exportation deliverables, as well as in training material deliverables.
Challenges with OSINT and Big Data **>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?	Data Management is provided in the MARISA Data Model.	The MARISA services dealing with social media will be part of the second Phase.

How do we know that the data is reliable and relevant?			
Knowledge & information 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 MARISA OSINT professionals in the proper management of ope3n source information in MARISA 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.	*Done in the first phase (Data Management Plan, User and Training Manuals). The approach will be promoted as part of the dissemination actions (workshops, meeting) in order to involve also external organizations.*	Social media services will be developed in Phase 2. The issue will be carefully considered.
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.	Fusion algorithms are used to reduce the information load. HMI will display on demand data with an easy exclusion of data that are not of interest for the users. The toolkit and its HMI will prevent the overload of information to the users. During the first trial several recommendations have been received from the end users in order to enhance the usability of the toolkit.	In the second phase will be improved the usability but also the information architecture of the solution.
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.	User manual is provided within the training kit.	
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 MARISA implementation on necessary also from this point of view.	End-users in MARISA come both from military and civilian sectors. Both needs are taken into account.	To be done by those responsible for the trials.

Data Leakages and the Misuse of MARISA

>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.		Appears to not be applicable to MARISA.	
Diplomacy issue: how to use the data that inevitably include also military tracks?	Rules & regulation on the use of data.	Not applicable to MARISA. Follow rules and regulations.	
Lack of security> illegal usage of the system, abuse of the system, using MARISA data in DARK web Technical Information leakage: The data MARISA 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.	Security standards are part of the MARISA design, which is based on a 'need to share' approach. This guarantees access and distribution of data fusion results among relevant stakeholders.	
Human information leakage: MARISA 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.	This is a peculiarity of the MARISA toolkit design, that ensures information traceability.	User control, user roles nad logging will be used asap.
The MARISA 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 MARISA business models, proper regulation, control and licensing measures have to be taken into consideration. If MARISA technologies are used for any other operation than MS, then a special		Exploitation is part of the second phase. It will be taken into account.

	guidelines book including ethical restrictions of use should be created.		
The Value of MARISA for the End-users in the Long Run			
How can we make it sure that MARISA will be developed continuously based on end-user requirements and ethical/legal requirements after the project ends?	Continuous development of the MARISA should be embedded in the business model from the early beginning.		This will be part of the activities in the second phase. E.g. establishing a post MARISA consortium for further development and exploitation of MARISA toolkit.
Due to the capacity of MARISA 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 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?		This will be part of the activities in the second phase.
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.			This will be part of the activities in the second phase.
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 MARISA components. MARISA should be a flexible system with a scalable deployment.		This will be part of the activities in the second phase.
Software licenses might hinder efficient development. Same is with patents. Is this a problem in MARISA? Open standards should be used.	The use of open standards and source. No patents should be held by partners. National **MARISA** license that can be deployed locally by the national authorities. Use of permissive SW license.		This will be part of the activities in the second phase.
Scare availability of fundamental data to developers.	Use only open data. Start a political process.	Open data is used wherever possible.	This will be also part of the activities in the second phase.
Other Issues			
People say they do not	Mandatory written ethics, practical,	Ethics issues carefully considered	Considerations inside the

care about ethics. People don’t know they have ethics dots, and some are blurred?	principles in all projects and WP’s. Practical use-cases that stress the ethical issues and small brainstorming on it. Write and publish results.	throughout the project lifecycle. Task leader.	consortium continues during the second phase.
Low communication between the end-users and/or developers		End-users and developers are part of the User Community. Continuous discussions have been held.	End-users involved in all the Technical meetings also in Phase 2. Two MARISA Workshops are planned in Phase 2.
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.	Continuous exchange of information with the CISE experts.	CISE governance is going to be defined in the next months. Contacts will be kept alive.
Understanding that ethics is not only a challenge, but also a possibility.	Understanding ethics as a driver for development and value creation.	Ethics issues have been fully considered during the development and validation.	Ethical issues will be considered also during the second phase.

Table 16: MARISA SIA

8.3. Summary

Justification of the MARISA in general can be supported by good communication and information sharing, by system transparency and accountability, by data security, by strong collaboration with various stakeholders, as well as by having ethics as a guide during the whole project life span – and afterwards.

Tension between the right for security and other ethical/legal issues calls for various activities related both to the technology (data fusion, privacy by design, various layers of ethics regulation), to the user processes and training, to the business/governance model (joint operation plans with third countries in the area, definition of national contact points before implementation), to MARISA user communities (collaboration also with SAR people and with third countries)as well as to various tasks needed in MARISA project (lobbying and influencing political organizations, collaboration with CISE.

Nature of ethics and cultural differences means that role of the communication user training is important, as well as conducting a market research as part of the business model. In addition, defining the rules for the collaboration as part of the business/governance model is one way of mitigating the differences. On the system level modularization and customization is needed in order to manage e.g. various layers of ethics in the system. Furthermore, lobbying and political influencing is needed in order to harmonise the legislation.

Liability issues calls for good quality of the data and data fusions, triangulation, transparency and accountability, as well as lobbying in order to remove obstacles concerning the use of certain data. The most important issue is however to keep in mind that it is always the human who makes the final decisions, not the machine.

Privacy and data protection requirements are crystallised in the EU data protection Reform. They concern both the technology, user processes and business/governance model. Designing MARISA data fusion in such a way that identification is on the level of phenomena instead of person is essential, as well as pseudonymisation.

Information management and human decision-making calls for both good information management and good understanding and training on ONSINT, human decision making and the biases and blind spots of cognitive processes. Development of smarter collection systems are needed to ensure adequate data are collected in the right time, in the right format, and for the right circumstances. The use of a broad range of analytic techniques to identify and resolve biases, e.g. assumption surfacing, red teaming, post-mortem analysis is also needed. In addition, rules and regulation on the use of data are needed for situation where user have a dual role (both civilian and military).

Data leakages and misuse of MARISA means that various activities are to be taken both on the level of technology and security, user processes and rules, as well as on business model level including proper regulation.

Furthermore, to make it sure that **the value of MARISA for the end-users in the long rung** calls for both economic and technical and ethical sustainability of the solution. Continuous development should be embedded in the business model, and the whole development should from the early beginning be based on open standards and without patents.

9. The Ethical Dimensions of MARISA

The purpose of this chapter is to present a checklist of ethical requirements and a Code of Conduct for MARISA. Taken together, these documents summarize the ethical framework for MARISA, including its development, deployment and use.

9.1. Ethical Requirements

The current ethical requirements for MARISA are presented below in the form of a table. The list was originally created in the autumn 2017 (for the deliverable 'Ethical, Societal and Legal Aspects of MARISA d2.3') but has now been clarified and updated and includes also the status reports for implementation. It will be a living document until the end of the MARISA project. The categories and classifications used in the table are explained below.

Importance of the requirement:	**Type of requirement**	**Substance of the requirement:**
Essential	(ethical) Awareness	MNGMT Management
Important	(ethical) Analysis	ETHICS Ethics
Interesting	(any kind of) Activity	UC User community
Desirable		AM Adoption model
		BM/GM Business/governance model
		TECH Technology
		TRAIN Training
		DISS Dissemination
		PILOT Piloting
		ALL

Table 17: Categories used in the MARISA Ethical Requirments -table

GENERAR REQUIREMENTS FOR MARISA DEVELOPMENT AND ETHICAL AWARENESS (updates to original requirements clarified with grey text)	**TYPE& LINKS TO WP'S**	**Status (including corresponding UR's)**
MARISA-G1) Take ethics and societal challenges seriously; concerning both technology, user processes, and business/governance model, including information management.	*Essential Awareness* *All*	*Ethics check has been an obligatory activity in each deliverable, and ethical issues have been on the agenda in several meetings. The check-list for Trusthworthy AI has also been taken into use in MARISA.*
(MARISA-G5) 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* *All*	*Privacy and Data Protection have been a specific topic during various MARISA meetings. In addition to D2.6 and D2.13 also technical notes on the issues have been provided by Ethics Manager and Data Protection Officier.* *The Privacy by Design (PbD)-approach and other requirements defined in the GDPR are used as a basis for designing the MARISA technical solution and user processes.* *MARISA governance and business models are based upon the GDPR and the organizational requirements set for the Controller and Processors of the data These activities are performed in parallel with the design of the technology and user processes.* *In the second phase it will be evaluated the GDPR compliance of the project at different steps through checks at the end of any relevant phase and on specific*

		deliverables. Moreover, a Privacy and Data protection Impact Assessment (DPIA) is conducted in Phase 2 on the newly developed MARISA services, based on Social Media Data, as well the infra-services related to user access rights and management available. The DPIA is performed by utilizing the PIA toolkit provided by CNIL.
MARISA-G6) The GDPR requires effective and clear governance model. This should be created for both the development phase and the final MARISA solution, and be integrated into the MARISA business/adoption model(s). A Data Protection Officer shall be nominated.	*Essential Activity* *PILOT WP7*	*DPO has been nominated for MARISA project and Controller during the MARISA project is the consortium jointly.* *A data protection team, including a data protection officer, was formed in early 2019.*
(MARISA-G7**)** Define the flows of personal in the MARISA solution. 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) Original G-7 is modified by moving risk analysis of personal data from G-9 here as risk analysis and DPIA.	*Essential Activity* *PILOT WP7*	*Description of the data flows is provided in the technical documentation (D3.x, D4.x and D5.x) and verified during the Phase 1 pilots. The same approach will be followed in phase 2.* *Data Protection and Privacy Impact Assessment (DPIA) work started during the first phase by figuring out risks in first phase pilots (>no risks, since only data in which persons can be identified is AIS data with the possibility for indirect identification). Potential risks concern the configuration in Phase 2 on the newly developed MARISA services, based on Social Media Data, as well the infra-services related to user access rights and management.*
(MARISA-G23 + G24 + G26) Consider that the GDPR applies already during the pilot. Communicate openly about data protection issues, challenges and needs already during the pilot. One alternative is to use fake data. If using real-life data is necessary, the reasons for this must be elaborated. Any personal data should be anonymised or irreversibly pseudonymised as soon as it is recognised as personal data. If this cannot be done (e.g. with photographs and indirectly identifying personal characteristics), the data should be stored only for as long as strictly necessary for testing the prototype. Avoid the processing such photos and videos due to the sensitive nature of such data.Original tree separate requirements are merged.	*Essential Activity/Awareness* *PILOT WP7*	*Simulated data mainly used in the first pilots. In the second phase, the use of real data is envisaged to ensure an effective validation of the toolkit. EM and DPO will be involved.* *Open communication about data use was taken care of during the first execution of the operational trials and so it will be in the second phase* *Real-life data will be used in the second trial execution taking into account ethics guidelines and ensuring GDPR compliance.*
(MARISA-G2) Follow up on the legal framework for information sharing, management and data protection.	*Essential Analysis* *ETHICS WP2*	*First analysis was done as part of D2.6. Updating is done as part of this deliverable D2.13.* *The new regulation forEuropean Border and Coast Guard) is still on the process. It is important to follow it up until it will be finalized and accepted.*
MARISA-G16) Perform a societal/ surveillance impact assessment (SIA) to secure that MARISA is compliant with ethics and legislation.	*Essential Analysis* *ETHICS*	*First analysis was done as part of D2.6. Updating is done as part of the deliverable D2.13.*

	WP2	
(MARISA-G19) 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* *UC, AM/BM WP2, WP8*	*This desirable requirement is not possible to implement in the frame of the MARISA R&D project and its original scope.* *In the final business/governance model and/or exploitation plan this recommendation is important to consider as one potential activity/service related to each new MARISA implementation.*
(MARISA-G20) Include SAR people in the user community: their needs are as important for MARISA as everyone else's.	*Essential/ Important Activity* *UC, AM,BM WP2*	*The MARISA end-users include SAR people. They are part of the User Communities that also include external experts. The user requirements have been defined taken into account their needs as well.* *Same approach is relevant in MARISA's various user communities and Business/Adoption Models in the future.*
(MARISA-G21) Recognize third countries in the sea as both end-users of MARISA, and as partners in solving shared problems with the help of new technology.	*Desirable/ Essential Activity* *MNGMT UC, AM,BM WP1, WP2*	*The MARISA Advisory Board include a representative from a third country. The point will be addressed during the MARISA workshops and the Advisory boards.* *This issue is relevant also in the various future User Communities and Business/Adoption Models of MARISA.*
(MARISA-G22) Lobby/influence political organizations on data protection issues and other legislation that is essential for MARISA, as well as on data availability across countries.	*Desirable Activity* *MNGMT WP1*	*Not done yet. It will be discussed in the Executive Board. Anyway it doesn't seem a priority at this stage.*
MARISA-G27) 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.	*Essential Awareness* *UC WP2*	*Belonging practitioners and partners to different countries, this issue and any potential difference in copyright rules is addressed during the User Community and technical meetings.*
MARISA-G11) 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.	*Important/ Essential Activity* *Training, AM, BM WP2,WP8*	*Done in the set of manuals (administration manual and user manual) discriminating the responsibilities of service providers (i.e. developers) and practitioners (i.e. end-users)* *Essential in the future Business/Adoption Model.*
MARISA-G12) Practice transparency about MARISA 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* *DISS WP8*	*Done in the first phase (refers to the communication and dissemination plan), Web-site implemented and available. The communication and dissemination activities will be even more in the second phase.*
(MARISA-G9) 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	*Essential Activity* *Piloting, AM/BM WP7, WP2, WP8*	*Not done yet. IPR assessment planned in phase 2, starting from the definition of the D8.6 (Exploitation plan)* *This is also a task to be performed as part of each MARISA implementation. (>MARISA business model and exploitation, MARISA adoption Model). See also MARISA Code of Conduct in D2.13.*

risk management procedures. Original G-9 is modified by moving data protection issues in G-7.		
(MARISA-G13) 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.	*Desirable/ Essential Activity* *PILOT BM/AM WP7,WP2, WP8*	*It seems not a priority during the MARISA R&D project and its pilot use of social media data.* *This is essential to take into account at in the organizational requirements in the final business/governance model and/or exploitation plan (see B-9)..See also MARISA Code of Conduct in D2.13.*
(MARISA-G14) Perform an explicit legal Duty of Care before utilizing any Big Data or Artificial Intelligence (AI). 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). Original G-15 is modified by adding also AI into text. S	*Desirable/ Essential Activity* *PILOT BM/GM WP7, WP8*	*This will performed before second phase pilots?.* *This is essential to take into account at in the organizational requirements in the final business/governance model (>B-9). See also MARISA Code of Conduct in D2.13.*
MARISA-G15) Conduct external reviews and audits concerning the analysis of Big Data and the use of Artificial Intelligence (AI). 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. Original G-15 is modified by adding also AI into text.	*Desirable/ Essential Activity* *PILOT BM/GM WP7, WP8*	*DPO nominated for MARISA project. External reviewes could be part of one of the two MARISA workshop planned in the second phase. See also B-9.* *External reviews and audit are essential services needed to enable ethical use of big data and AI in MARISA. This has to be explained in organizational requirements of MARISA as part of MARISA business/governance model. See also MARISA Code of Conduct.*
SPECIFIC REQUIREMENTS FOR MARISA TECHNOLOGY DEVELOPMENT & ITS USER MANUALS		
(MARISA-G8) 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)	*Essential Activity* *TECH, TRAIN WP2-WP8*	*This is done as documented in the MARISA Design document and in the technical documentation. The full set of Privacy Enhancing Technologies (including access rights, anonymization etc) will be validated during the second phase pilot.* *This has also impact on MARISA training material.* *MARISA_UR_GEN_05, MARISA_UR_GEN_65, MARISA_UR_GEN-70* *all the MARISA _UR_ACCESS SERVICES*
(MARISA-T1) 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. Original T1 and T8 are merged.	*Essential Activity* *TECH WP3-WP5*	*This requirement is translated into several requirements in the technical baseline. Specific KPIs have been defined to monitor the fulfilment of the functionalities during the validation. Rules can be configured by the users. Refers to technical documentation (D3.x, D4.x, D5.x)* *MARISA_UR_GEN_55, MARISA_UR_GEN_60*

		various MARISA_UR_DF1 requirements *The AI-checklist will also be used in order to investigate the transparency issues in MARISA.*
(MARISA-G3 and T3) Put priority to the transparency and accountability of MARISA and its information management. Transparency is mandatory for both the MARISA system and the processing of data, as it serves the interests of accountability. > GDPR Original G3 and T3 are merged since they are overlapping a lot.	*Essential Activity* *TECH, TRAIN WP3-WP5, WP8*	*A Privacy Organization Model of the Project is defined complying with the Accountability principle set forth in art. 30 of the GDPR (e.g. mapping the processing, assigning Data Protection responsibilities etc.) The set of technical documents (D3.x, D4.x, D5.x) provides all the information about the MARISA toolkit with different levels of details* *MARISA_UR_GEN_55, MARISA_UR_GEN_60* *various MARISA_UR_LEVEL 1-4 SERVICES*
(MARISA-G10) 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)	*Essential Activity* *TECH, TRAIN, DISS WP3-5, WP8*	*Done in the first phase (Data Management Plan, User and Training Manuals). The approach will be promoted as part of the dissemination actions (workshops, meeting) in order to involve also external organizations* *This has impact also on technology!*
(MARISA-T2) 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. (see also PR)	*Essential Activity* *All*	*Human is always in the loop*
(MARISA-T4) 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 TECH WP3-WP5	*Needs clarification during the second phase of MARISA. This recommendation is related e.g. to data protection requirements.* *MARISA_UR_GEN_15 is linked to this requirement*
(MARISA-T5) 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 Activity* *TECH, TRAIN WP3-WP5, WP8*	*Access control capabilities are part of the second phase. It will be discussed during the technical meetings*
(MARISA-T6) Modularity of the MARISA 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 Activity* *TECH WP3-WP5*	*Modularity is one of the main drivers of the MARISA toolkit design as it can be evaluated in the technical documents. It will support different models for the exploitation of the system* *MARISA_UR_GEN_15 is linked to this requirement* *MARISA_UR_GEN_20*
(MARISA-T7) 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 Activity* *TECH*	*This requirement is taken into account in the algorithm selection and in their implementation. It has been already verified during the operational scenarios.* *How about the use of dark internet?*

	WP3-WP5	*various MARISA_UR_DF1-4 requirements*
(MARISA-T9) 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 Activity* *TECH WP3-WP6?*	*The MARISA toolkit design ensures information traceability through an extensive use of logs and reporting.* *MARISA_UR_GEN_92, MARISA_UR_GEN_94*
(MARISA-T10) Compliance with EUCISE2020 network should be implemented.	*Important Activity* *TECH WP3-WP5*	*It is confirmed. MARISA data model is compliant with CISE data model. The EUCISE 2020 adaptors have been implemented. In the second phase, the MARISA toolkit will interface the EUCISE2020 nodes* *MARISA_UR_GEN-45*
(MARISA-T11) Specific security standards are to be followed up to the EU restricted level (TBC).	*Essential Activity* *TECH WP?*	*It is done according to the Security Advisory Board guidelines and requirements. Specific deliverables have been identified that can potentially include EU-restricted information. The Security Advisory Board assess the list of deliverables and the dissemination level up to the EU-restricted level* *MARISA_UR_GEN-05*
(MARISA-T12) A vast array of analytic techniques to identify and resolve biases, (e.g. assumption surfacing, red teaming, post-mortem analysis, etc) is encouraged.	*Interesting Activity* *TECH WPX?*	*This will be discussed during the second phase of MARISA. See also G-5 on biased decision making and cognition.*
(MARISA-T13/U1) The quality of data is to be investigated both automatically and manually when first transferring it as well as in each use case.	*Essential Activity* *TECH, TRAIN, AM/BM*	*This is out of scope in the MARISA validation and, hence, in the MARISA R&D project. The requirement will be taken into account during the exploitation by implementing a software layer that automatically analyze the quality of data.*
MARISA-T14 When applicable, deploy even additional technical solutions to cope with the data protection legislation and other requirements.	*Essential Activity* *TECH WPx?*	*See e.g. MARISA UR_GEN-75* *The need for additional technical solutions (-if needed) can be identified after the PIA based on MARISA in the second phase. (e.g. rights of data subjects are not essential in MARISA context).*
MARISA-T15: Trustworthy Artificial Intelligence requires that algorithms are secure, reliable as well as robust enough to deal with errors or inconsistencies. New requirement	*Essential Activity* *TECH* *WP3-6*	*The analysis of MARISA services utizing AI will be performed with the help of this checklists.*
SPECIFIC REQUIREMENTS FOR USER PROCESSES AND TRAINING MATERIAL		
(MARISA-U1/T13) The quality of data is to be investigated both automatically and manually when first transferring it as well as in each use case.	*Essential Activity* *TRAIN,*	*The first version of the training kit was already delivered in Phase 1. The second and final version will be delivered in Phase 2 (D8.12, M28). The training and the user manuals will be verified during the execution of the Operational trials.*

	TECH *WP3, WP8*	
(MARISA-U2) 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. MARISA 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.	*Essential Awareness* *TRAIN* *WP8*	*The users will be always in the loop, the toolkit will support decision making and planning being the final decision lies on the end-users. This is clearly explained in the training and user manuals*
(MARISA-U3) Adopt the check and balance approach to avoid data leakages and mis-use of it.	*Essential Activity* *TECH, GM/AM* *WPx?, WP2?*	*This has to be discussed during the Phase 2*
(MARISA-U4) Proper user training on ethical decision making is needed because of the inherent biases in cognitive processing and because ethics and legislation are case/country dependent even in our pilot countries	*Essential Activity* *TRAIN* *WP8*	*Training sessions were already carried out in the first phase with the support of the training kit and so it will be done in the second phase.* *This should also be part of the future MARISA adoption/business – models. (see B-6)*
(MARISA-U5) Organise specific education on data protection, OSINT and social media, where also the ethical and legal challenges included (privacy, stigmatization, dual roles, etc.)	*Essential Activity* *TRAIN* *WP8*	*This will be taken into account during the second phase. One of the MARISA Workshop could include a specific session on the subject* *This should also be part of the future MARISA adoption/business –models (see B-6).*
(MARISA-U6) Develop end-user specific Codes of Conducts where the ethical principles for the use of MARISA are defined (includes the pilots).	*Essential Activity* *ETHICS* *WP2*	*First MARISA code of Conduct will be provided in Final Ethics Deliverable d2.13.*
MARISA ADAPTION/BUSINESS MODELS (in the future)		
(MARISA-B1) The continuous development of the MARISA services together with the end-users and stakeholders shall be embedded in the business model from the beginning to ensure that MARISA is up to date regarding ethical and legal requirements also in the future.	*Desirable Activity* *BM* *WP8*	*This issue will be addressed in the MARISA exploitation Plan (d8.6, M22) and in the MARISA exploitation Plan and Uptake Mechanisms (D8.7, M34). See also MARISA code of conduct in D2.13.*
(MARISA-B2) 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 model of MARISA.	*Important Activity* *BM* *WP8*	*The MARISA Business Model will be defined in the second phase on the MARISA Exploitation Plan (D8.6, M22) and in the MARISA Exploitation Plan and Uptake Mechanisms (D8.7, M34). See also MARISA code of conduct in D2.13.*
(MARISA-B7) Considering Service Logic (SD) in designing alternative business	*Important*	*Issue to be discussed with the consortium. See also B9.*

models for MARISA and its various component is highly recommended, as it supports the holistic approach to MARISA where not only technology, but also services are included. Furthermore, it lowers the investment costs for users. This is a new recommendation not identified in d2.6	*Activity* *AM/BM* *WP2, WP8*	
MARISA-G28) 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?)	*Desirable Activity* *AM/BM* *WP2, WP8*	*This is an issue which is clearly addressed in the exploitation plan. MARISA appointed the Innovation Manager taking care of IPR issues and patents ownership*
MARISA-B3) If MARISA 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.'	*Essential Activity* *BM* *WP9*	*This issue will be addressed in the MARISA Exploitation Plan (D8.6, M22) and in the MARISA Exploitation Plan and Uptake Mechanisms (D8.7, M34)*
(MARISA-B4) Market research, which is an essential part of the business model, must be conducted early on to enable the successful adaptation of MARISA in each local context. This includes conducting a Societal Impact Assessment (SIA) as well as an evaluation of the legal and ethical frameworks for MARISA in each operating environment.	*Essential Activity* *AM/BM* *WP2, WP8*	*The MARISA Business Model will be defined in the second phase in the MARISA Exploitation Plan (D8.6, M22) and in the MARISA Exploitation Plan and Uptake Mechanisms (D8.7, M34). See also MARISA code of conduct in D2.13. Also work with Adoption Model.*
(MARISA-B5) Organizational activities concerning Data Protection must be applied as part of the governance model for each new implementation of MARISA. Conducting a light PIA before the implementation is essential. Original B5 is splitted, the second par is now B9. PIA is also added here.	*Essential Activity* *BM/GM* *WP8*	*The final ethics deliverable D2.13 provides basic guidelines the organizational activities. These are to be embedded in MARISA exploitation/business modelling and in training material. See also MARISA code of conduct in D2.13.*
MARISA –B8) Information must be shared with border management authorities (i.e. Frontex) in all MARISA implementations, even when MARISA is sold as a stand-alone solution. This is essential for the border control authorities to be able to maintain a holistic situational awareness and to e.g. avoid the displacement effect. New requirement coming from original B5.	*Essential Activity* *AM/BM/GM* *WP2, WP8*	*The MARISA Business Model will be defined in the second phase in the MARISA Exploitation Plan (D8.6, M22) and in the MARISA Exploitation Plan and Uptake Mechanisms (D8.7, M34). Also adoption model?*
(MARISA-B9) It is essential for ethical compliance that the following activities are performed in each MARISA environment:	*Essential Activity*	*This is part of the business modelling and exploitation plan and linked to the idea of service logic. (see B7). See also MARISA code of conduct in D2.13.*

- Defining a Social Media Strategy - Defining an explicit legal Duty of Care, including external reviews - Audits of Big Data and AI components (see g13-g15) This text is reframed and splitted from original B5	*BM/GM* *WP8*	
(MARISA-b6) Ethics management and training concerning the use of MARISA in decision making must always be included in the business model.	*Essential Activity* *AM/BM/GM* *WP2, WP8*	*The MARISA Business Model will be defined in the second phase in the MARISA Exploitation Plan (D8.6, M22) and in the MARISA Exploitation Plan and Uptake Mechanisms (D8.7,M34). See also MARISA code of conduct in d2.13.*

Table 18; MARISA Ethical Requirements

9.2. MARISA Code of Conduct

The values and principles discussed in the previous sub-section form the fundamental ethical framework for the MARISA system as well as its user guidelines and business and adoption models.

These principles are summarised in the 'MARISA code of conduct', which can be found below. When applying these principles in specific user community contexts, they are to be further specified and integrated into other existing codes of conduct.

MARISA Code of Conduct

This Code of Conduct is designed for end-users, decision makers and developers of MARISA. It establishes 8 points of principles which should be taken into consideration when deploying, using and developing MARISA solution.

1 The Justification of MARISA is Based on Ethical Grounds

The adoption of new Maritime 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. MARISA is no exception to this. It is therefore vital that its use can be justified on ethical grounds: MARISA must respect fundamental rights and other applicable legislations, regulations and values. An ethically conscious approach is important also to enable the sustainable competitiveness of MARISA 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 MARISA, as well as on decision making and the future governance and business models of MARISA. 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.

MARISA 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.

2 The Humanitarian Imperative and the Rights of the People at Sea

Duty to Render Assistance is the hallmark of SAR regulation**.** MARISA 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 need to be respected, regardless of their origin or nationality. The information MARISA 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. MARISA enables an effective identification vessel on high seas and even on the territorial waters of third countries. It is therefore technically possible that MARISA 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 MARISA is to prevent the creation of such processes.

3 Moral Division of Labour in Maritime Surveillance and SAR

MARISA provides improved Marine 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 maritime surveillance should be discussed.

States enjoy sovereignty in their coastal waters. Any use of MARISA 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 shall be seen as MARISA end users and as true partners in solving shared problems with new technology

4 Value for End-users Involvement

Providing improvements in maritime awareness, MARISA 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 MARISA development also after the MARISA 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 MARISA technology.

5 Transparency, Liability and Human Decision Making

AI systems like MARISA 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 Surveillance and SAR must always be made by the competent human decision makers - computer systems such as MARISA can only have an assisting role in operational decision making.

6 Privacy and Data Protection

Privacy and data protection measures must be embedded in the MARISA technology so that compliance is achieved with both the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). MARISA Procurement Strategies/Adoption Models and Training material in turn provide guidelines for organizational arrangements to ensure data protection. A Data Protection Impact Assessment (PIA) is a compulsory be part of each MARISA 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, especially of those in a vulnerable position (e.g. refugees, victims of human trafficking), must always be protected when MARISA technology and information is used and available. Sensitive MARISA 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.

7 Data management and organizational arrangements and part of MARISA 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 MARISA 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).

8 Robustness, Accountability and Learning

AI systems like MARISA 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 MARISA 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 MARISA shall be provided. Transparency and on the accountability of MARISA and its information management and use must be prioritised. Feedback is welcome and addressed.

Table 19: Initial MARISA Code of Conduct

10. Final Remarks

The requirements coming directly from maritime law enforcement, search and rescue, and other actors in maritime security cover only a fraction of all the legal, ethical and societal aspects that relate to MARISA, its components, development and use. A comprehensive ethical and legal framework is thus vital to ensure that the solution is truly sustainable.

Applied ethics cannot be treated as a mere legitimising tool of 'ethics approval' but must be seen as a way of putting critiques to work. The MARISA technology and architecture, MARISA user processes and decision-making, and the future governance- and business models of MARISA are all liked with numerous legal, ethical and societal questions. Three sets of challenges and opportunities in particular come into prominence:

1) Ethical and legal issues relating to OSINT and big data
2) Ethical and legal issues relating to privacy and data protection, and
3) The tensions between different rights and values, such as freedom and security, that are likely to become more pronounced as a result of new security technologies

Each of these challenges has implications for the MARISA technology itself, but even more so for the MARISA business, governance, and adoption models. It is a given that all aspects of MARISA must be compatible with the requirements set by fundamental and human rights and other applicable legislation, principles and values. Compliance is only the starting point, however: MARISA can, and should, be designed and used to actively promote the fulfilment of these rights and values. A holistic ethical approach is, in the long run, also beneficial for the main objects of the project, as it helps to alleviate the worries and suspicions about new technology and to make the solution better prepared for future developments in legislation and society as a whole.

With this ethics approach we have seek to not only prevent and minimise the ethical risks associated with MARISA, but also to maximise the solution's benefit to society.