D1.1 Ethical and Legal Framework: Initial Assessment Report

corosect.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101016953

Author(s)/Organisation(s)	KU Leuven
Contributor(s)	ATOS, CERTH, ENTOCYCLE, AGVR, ENTOMOTECH, FSH, HSEL, ICF, TECNOVA, UM, NASEKOMO, OAM (Contribution in the form of answering a questionnaire)
Work Package	Work Package 1
Delivery Date (DoA)	30 June 2021
Actual Delivery Date	29 June 2021
Abstract:	This deliverable is the first report on the legal and ethical framework in the CoRoSect project, covering a relatively wide spectrum of domains that are applicable to the project with a focus on data protection and privacy, liability, and ethics. It maps the relevant sources and delivers a high-level description of the applicable legal and ethical legal framework, together with its potential constraints for the project's applications and procedures.

Document Revision History			
Date	**Version**	**Author/Contributor/ Reviewer**	**Summary of main changes**
01.04.2021	0.1	Laurens Nijs	Table of Content and Initial Input
21.05.2021	0.2	Laurens Nijs, Halid Kayhan, Burcu Yaşar	Continuous Input
05.06.2021	0.3	Halid Kayhan, Burcu Yaşar	Continuous Input
07.06.2021	0.4	Halid Kayhan, Burcu Yaşar	Final draft for review
07.06.2021	0.5	Anton Vedder	Internal Review (KUL)
09.06.2021	0.6	Halid Kayhan, Burcu Yaşar	Revision
17.06.2021	0.7	Rico Möckel, Juho Mäkiö	Internal Review (UM and HSEL)
17.06.2021	0.8	Burcu Yaşar	Implementation of reviewers' comments
25.06.2021	0.9	Alex Papadimitriou	Quality Review
25.06.2021	1.0	Burcu Yaşar	Final Editing

Dissemination Level		
PU	Public	**x**
PP	Restricted to other programme participants (including the EC Services)	
RE	Restricted to a group specified by the consortium (including the EC Services)	
CO	Confidential, only for members of the consortium (including the EC)	

Funding Scheme: Innovation Action (IA) ● Topic: H2020-ICT-46-2020
Start date of project: 01 January, 2021 ● Duration: 36 months

CoRoSect Consortium			
Participant Number	**Participant organisation name**	**Short name**	**Country**
1	UNIVERSITEIT MAASTRICHT https://www.maastrichtuniversity.nl/	UM	NL
2	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS https://www.certh.gr/	CERTH	GR
3	HOCHSCHULE EMDEN/LEER https://www.hs-emden-leer.de/en/	HSEL	GER
4	LUONNONVARAKESKUS https://www.luke.fi/	LUKE	FIN
5	OULUN AMMATTIKORKEAKOULU OY - OULU UNIVERSITY OF APPLIED SCIENCES https://www.oamk.fi/fi/	OAMK	FIN
6	FUNDACION PARA LAS TECNOLOGIAS AUXILIARES DE LA AGRICULTURA http://www.fundaciontecnova.com/	TECNOVA	ES
7	KATHOLIEKE UNIVERSITEIT LEUVEN https://www.kuleuven.be/kuleuven/	KU LEUVEN	BEL
8	ATOS IT SOLUTIONS AND SERVICES IBERIA SL https://atos.net/en/	ATOS	ES
9	ROBOTNIK AUTOMATION SLL http://www.robotnik.es/	ROB	ES
10	AGVR BV www.agvegroup.com	AGVR	NL
11	NASEKOMO AD https://nasekomo.life/	NASEKOMO	BG
12	ENTOMOTECH SL http://entomotech.es/	ENTOMOTECH	ES
13	ENTOCYCLE LTD https://www.entocycle.com/	ENTOCYCLE	GB
14	SOCIETA AGRICOLA ITALIAN CRICKET FARM SRL https://www.italiancricketfarm.com/	ICF	IT
15	INVERTAPRO AS https://www.invertapro.com/	INVERTAPRO	NOR
16	FIELD LAB ROBOTICS BV https://www.fieldlabrobotics.com/	FLR	NL
17	FoodScale Hub https://foodscalehub.com/	FSH	RS
18	AgriFood Lithuania DIH https://www.agrifood.lt/	AFL	LT
19	CENTRO INTERNAZIONALE DI ALTISTUDI AGRONOMICI MEDITERRANEI http://www.iamb.it/	CIHEAM	IT

Table of Contents

List of tables

List of figures

List of Abbreviations and Acronyms	
AI	Artificial Intelligence
AGV	Automated Guided Vehicle
Art.	Article
API	Application Programming Interface
CoRoSect	Cognitive Robotic System for Digitalized and Networked (Automated) Insect Farms
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
ECHR	European Convention on Human Rights
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EP	European Parliament
EU	European Union
Expert Group on Liability	Expert Group on Liability and New Technologies
GDPR	General Data Protection Regulation
HLEG AI	The High-Level Expert Group on Artificial Intelligence
ICO	UK Information Commissioner's Office
ICT	Information and Communications Technology
UN	United Nations
WP	Work Package

Executive Summary

This deliverable (D1.1: Ethical and Legal Framework: Initial Assessment Report) provides a high-level description of the legal and ethical framework that will be applicable to the CoRoSect project, as well as to the subsequent technological applications that are to result from the project. It maps the relevant sources in a wide range of areas, including data protection and privacy, safety, liability, and ethics, together with their potential constraints for the project's applications and procedures. A considerable part of the existing framework consists of ethical principles and guidelines. Ethical principles, including human oversight, transparency and accountability should be fully respected in the design and development of AI-based technologies. In addition, the existing legal framework on product safety and liability applies to the CoRoSect project, although the application of the relevant rules to specific technologies are not always clear due to the uncertainties and specificities involved in the AI-based technologies. Furthermore, European Union (EU) data protection law provides a legal framework that also applies to the CoRoSect. AI robots, for the purpose of performing and improving their functions, process vast amounts of data, often by covert means (e.g. sensors and cameras), thus creating risks for the individuals' rights to respect for private life and to the protection of personal data (Art. 7 and 8 Charter of Fundamental Rights of the EU). Therefore, adherence to the General Data Protection Regulation (GDPR) and, especially, its requirements for data protection by design and by default, are crucial. Although it is not completely clear at this stage what types of personal data will be processed within the CoRoSect framework, a preliminary analysis has shown that personal data will be collected and processed through cameras and sensors. These activities will fall under the material scope of the GDPR. Lastly, all the ethical requirements related to research under Horizon 2020 Programme must always be applied to ”achieve real research excellence”.

1 Introduction

Food security represents one of the main challenges of the 21st century. A potential sustainable solution to this uncertain future can be found in insect farming. Insects are a valuable food source for farming animals. However, research, innovation, farming protocols development and standardization, and public awareness campaigns on insects as food and feed are dramatically needed. This is where Cognitive Robotic System for Digitalized and Networked (Automated) Insect Farms (CoRoSect) joins the conversation. CoRoSect will provide a novel robotization concept enabling up-scaling and optimizing a number of insect production facilities utilizing state-of-the-art robotization and artificial intelligence (AI) technologies. The basic solution is to enable to set up dynamic work cells, where a single human worker is aided by several robots, AI, and smart sensors across the stages of insect production.

This deliverable is the first report on the legal and ethical framework in the CoRoSect project, covering a relatively wide spectrum of legal domains that are applicable to the project as well as to the subsequent technological applications that are to result from the project. As indicated in the title of this report "Legal and Ethical Requirements", the deliverable's primary goal is to map the main areas of concern and to deliver a high-level description of the applicable ethical and legal framework, together with its potential constraints for the project's applications and procedures.

This deliverable aims to be as broad as possible with regard to the technologies involved. The jurisdictional scope of this deliverable is international law and law of the European Union (EU). The national laws of each country will not be analysed due to the language limitations of the authors. It will be nevertheless stated when diverging national implementations can be expected, where applicable. If the regulation of the relevant areas and questions is reserved for individual countries (for example when directives are left to be transposed by Member States or where legal acts leave a broad margin of discretion to Member States or treaty signatories), the specific national regulation would need to be analysed and addressed separately by members of the consortium or other stakeholders.

This deliverable will touch upon several legal and ethical questions raised by the CoRoSect project. Issues analysed will be related to, among others, AI and liability, privacy and data protection and research ethics concerning human participants and insects.

It is important to note that while this deliverable will provide a first overview of the requirements for legal and ethical compliance, on the one hand, it will provide the basis for subsequent deliverables within Work Package 1 (WP1) of the CoRoSect-project, on the other. This deliverable (D1.1 Ethical and Legal Framework: Initial Assessment Report) is the result of the first Task within WP1.

The second chapter of this deliverable (**Artificial intelligence governance – A European perspective**) provides a general overview of the governance model of AI in Europe. The chapter first provides a brief explanation about the notion of AI and second analyses the current and future legislative efforts on AI in Europe. The third chapter (**Legal Framework on Safety and Liability)** outlines the legislative framework that deals with the aspects of safety and liability. It provides a brief overview of the recent studies and policy documents that address these aspects in the context of emerging technologies at the EU level. It further outlines the concepts of civil liability with a focus on product liability.

The fourth chapter (**Data Protection and Privacy**) provides a high-level description of privacy and data protection and cybersecurity rules applicable to the CoRoSect project. To perform and improve their functions, AI robots process vast amounts of data, often by covert means (e.g. sensors and cameras), threatening individuals' rights to respect for private life and to the protection of personal data (Art. 7 and 8 CFREU). Therefore, adherence to the General Data Protection Regulation's (GDPR) data quality principles and its requirements for data protection by design and by default are crucial. Considering that the accumulation of personal data makes such systems vulnerable to attacks and breaches, security concerns and their mitigation through technical and organisational measures are likewise relevant.

The fifth and final chapter (**Research Ethics**) identifies the most important ethical considerations. EU institutions have repeatedly advocated the development of human-centric AI, premised on shared EU values and principles, especially dignity, autonomy, and self-determination. Such values and principles likewise extend to the deployment stage. On a daily basis, human-robot interaction might be fraught with morally problematic effects, for example, robot deception or exercise of authority. In the long run, the introduction of robots into the workplace might significantly affect the labour market, replacing and not just complementing human workers. The application domain of such AI-enabled automation is no less important: automating an industry whose goal is to "feed the world's population while respecting future generations" needs and expectations in terms of food security, safety and sustainability" warrants particular ethical scrutiny.

The methods used in the writing of this deliverable are as follows:

i. In the first step, as a preparatory phase, the authors analysed the CoRoSect project's concept and technologies.

ii. As a second step, the authors identified all the legal domains containing rules, that might restrict or otherwise affect the Consortium's activities. To put themselves in the position to make this assessment, a preliminary questionnaire or "Q & A" was created. The questionnaire aimed to support the compliance of the Consortium partners' activities by providing guidance on what issues need to be addressed and also to support the formulation of legal and policy recommendations on the automation of insect rearing farms in the EU. Its purpose was to provide WP1 (Ethical, Legal and Social Implications (ELSI) of human-robot collaboration in industrial automation) with accurate and up-to-date information on all matters that might be relevant for the identification of the applicable legal framework and to assess potential ethical considerations. The questionnaire included some key questions regarding: technology being used and developed; extent of decision-making by smart algorithms; data processing and collecting activities as well as data flows; ethical considerations of AI, human participants in research activities and insect farming. To streamline the project's activities KU Leuven (WP 1 Leader) worked together with CERTH which is responsible for CoRoSect's Data Management Plan (DMP – proposal 2.2.1.5.). KUL and CERTH bundled questions on data flows and data protection, making compliance more efficient.

iii. In a third step the questionnaire's answers were analysed. They allowed to gain much more knowledge on technical implementation of the CoRoSect project and were used in

the preparation of this deliverable. However, it should be noted that the technologies envisaged to be developed and/or deployed may change in the course of the CoRoSect project due to the ongoing processes of the project. An important reason for this may be interoperability issues between those technologies: for instance, in case two envisaged technologies cannot function together properly, there may be a need to use different technologies to achieve the desired outcome. Overall, the responses collected to these questions are key to know as to whether and which type of personal data will be processed and what ethical issues may arise. This deliverable provides a preliminary analysis. Any further analysis will be provided in the D1.2 (Ethical and Legal Requirements Specification Report).

2 Artificial intelligence governance – A European perspective

2.1. The concept of Artificial Intelligence

In order to analyse the European rules on artificial intelligence, a good understanding of the notion of AI is key. AI refers to the ability of a computer or machine to have, or to mimic, human-like intelligence. A machine will be considered as AI when it is able to perform certain capabilities typically performed by the human mind, based on learning from examples and experiences (in the form of data sets), such as recognizing objects, understanding, and responding to language, making decisions and solving problems or even combining all these capabilities into entire actions, such as driving a car.[1]

AI is a widely used term which covers a broad variety of computing technologies, even remotely, resembling human intelligence. Within the circle of what is called AI, we find Machine learning. Machine learning refers to an AI application that learns by itself. This way the application will learn to perform the task, which it was designed to do, in a better and more efficient way. Finally, there is Deep learning. Deep learning is a subset of machine learning. Deep learning applications will also learn on itself to perform certain tasks, but without any human intervention (See Figure 1).

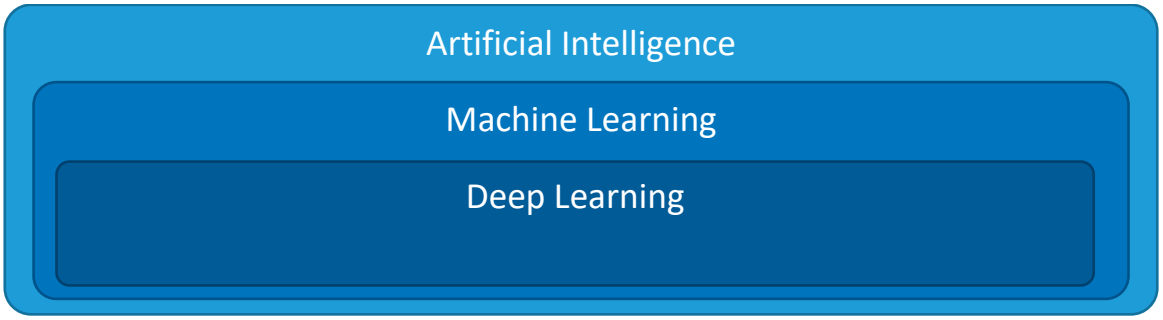

Figure 1: The relationship between AI, machine learning and deep learning

AI has different types of applications, going from speech recognition to virus and span prevention to household robots. Particularly relevant for the CoRoSect project is an application called “Image recognition”, also known as “computer vision” or “machine vision”. These terms refer to the ability of a system to identify and classify objects, shapes, people, writing within still or moving images. The system processes images acquired from an electronic camera, just like the vision system in the human brain processes images derived from the eye.[2]

CoRoSect wants to implement this technique enabling an automated selection of insects at certain stages in the insect farming process. However, this is not the only AI application suggested by the CoRoSect end-users. The use-case requirements also identify the need for speech recognition in order to process cricket sound waves and the need for automated transportation using AGV’s.

On a more theoretical level a distinction has to be made between two types of AI: strong AI and weak AI. Strong AI is general artificial intelligence, meaning that it actually reflects human intelligence in

[1] IBM Cloud Education, Artificial Intelligence (AI), 3 June 2020, https://www.ibm.com/cloud/learn/what-is-artificial-intelligence, accessed 04 June 2021.
[2] M. NIXON and A. AGUADO, *Feature Extraction and Image Processing for Computer Vision*, 2019, London (UK), Elsevier Science & Technology, 1.

general, in its entirety. As to this day strong AI still remains theoretical, with no real-life applications. Weak AI refers to an AI application trained to perform specific tasks. Also called narrow AI, this type of artificial intelligence is already quite common in our everyday lives, think of Amazon's Alexa, self-driving cars or IBM Watson.

2.2. Legal and ethical framework on Artificial Intelligence

In this part of the deliverable an analysis will be made of the current and future legislative efforts on Artificial Intelligence in Europe. The European Commission's (EC) approach on Artificial Intelligence centres around excellence and trust. The European Union started working on a strategy on AI in 2018. The high-level idea of the initial approach was to create a fair, open and democratic, but nevertheless competitively sustainable climate for AI development in Europe.[3] This idea would be realised through the adoption of a concrete strategy plan, and the designation of an expert group aiming at developing guidelines and recommendations on the development of AI.[4]

The first steps in this development date back to the 10th of April 2018, when the EU Member States signed a Declaration of cooperation on Artificial Intelligence (AI).[5] This was the first step towards officially joining forces and engaging in a European approach.[6] The adoption of the declaration was an important event since many new technologies, including AI, require a cross-border approach, as stressed by Andrus Ansip, the Vice-President for the Digital Single Market and Mariya Gabriel, Commissioner for Digital Economy and Society: "In Europe, any successful strategy dealing with AI needs to be cross-border. A large number of Member States agreed to work together on the opportunities and challenges brought by AI. That is excellent news. Cooperation will focus on reinforcing European AI research centres, creating synergies in R&D&I funding schemes across Europe, and exchanging views on the impact of AI on society and the economy. Member States will engage in a continuous dialogue with the Commission, which will act as a facilitator".[7]

The Declaration was signed by Austria, Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, UK, Norway and later joined by Romania, Greece, Cyprus and Croatia.

---

[3] P. VAN DEN SPIEGEL and B. BOGAERT, "EU strategic plan on Data and AI
The data strategy and the White Paper on AI unveiled", *KPMG Insights*, https://home.kpmg/be/en/home/insights/2020/02/ta-eu-strategic-plan-on-data-and-ai.html, accessed 04 June 2021.

[4] EC, *Factsheet: Artificial Intelligence for Europe*, 25 April 2018, https://digital-strategy.ec.europa.eu/en/library/factsheet-artificial-intelligence-europe, accessed 04 June 2021.

[5] Declaration of cooperation on Artificial Intelligence of 10 April 2018, https://ec.europa.eu/jrc/communities/sites/default/files/2018aideclarationatdigitaldaydocxpdf.pdf, accessed 04 June 2021.

[6] EC, *EU Member States sign up to cooperate on Artificial Intelligence*, 10 April 2018, https://digital-strategy.ec.europa.eu/en/news/eu-member-states-sign-cooperate-artificial-intelligence, accessed 04 June 2021.

[7] EC, EU Member States sign up to cooperate on Artificial Intelligence, 10 April 2018, https://digital-strategy.ec.europa.eu/en/news/eu-member-states-sign-cooperate-artificial-intelligence, accessed 04 June 2021.

By giving their approval these countries agreed to some fundamental ideas on the further development of AI in Europe, among others:

1. Work towards a comprehensive and integrated European approach on AI to increase the EU's competitiveness, attractiveness and excellence in R&D in AI.
2. Build awareness and foster the development of AI in a "European AI Alliance".
3. Exchange of views, information, best practises, data and cooperation between member states.

On the 1st of June 2018 the next level of initiative was taken: The High-Level Expert Group on Artificial Intelligence (HLEG AI) was appointed, which is crucial to the development of AI legal and ethical framework. It helps stimulate a multi-stakeholder dialogue, gathers participants' views and reflects them in its analysis and reports.[8] The key takeaway is that the HLEG AI has published four deliverables on AI policy in the EU.[9] These deliverables and the overall work of HLEG AI constitute the core of the current legal and ethical framework on AI in Europe. They are the basis for the initiatives taken by the Commission and its Member states, such as the White Paper on AI. The mandate of the HLEG AI ended in July 2020.

2.2.1. The High-Level Expert Group on Artificial Intelligence

The European Commission appointed a group of experts to provide advice on its AI Strategy. During the first year of its mandate, the HLEG AI worked on two main deliverables:

1. Ethics Guidelines for Trustworthy AI
2. Policy and Investment Recommendations for Trustworthy AI.

In July 2020, when its mandate ended, the expert group published two more deliverables:

1. The final Assessment List for Trustworthy AI (ALTAI)
2. Sectoral Considerations on the Policy and Investment Recommendations.

In what follows this deliverable will have a detailed look at each of the 4 policy documents and their principles.

2.2.1.1. Ethics Guidelines for Trustworthy AI

The HLEG AI presented the "Ethics Guidelines for Trustworthy AI" on 8 April of 2019.[10] In the introduction the expert group explains why AI is important for the future development of our society. It stresses that AI should not be seen as an end to itself, but a means to 'increase human flourishing, thereby enhancing individual and societal well-being and the common good, as well as bringing progress and innovation. In particular, AI systems can help to facilitate the achievement of the United Nations' (UN) Sustainable Development Goals, such as promoting gender balance and tackling climate change, rationalising our use of natural resources, enhancing our health, mobility and production

[8] EC, *Call for a High-Level Expert Group on Artificial Intelligence*, 9 March 2018, https://digital-strategy.ec.europa.eu/en/news/call-high-level-expert-group-artificial-intelligence, accessed 04 June 2021.
[9] A link to these four policies can be found here: https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai, accessed 04 June 2021.

[10] EC, *Ethics guidelines for trustworthy AI*, 8 April 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, accessed 04 June 2021.

processes, and supporting how we monitor progress against sustainability and social cohesion indicators.[11]

In this context the HLEG AI makes clear that AI should be human-centric, and that there is a need to balance the incredible opportunities with the risks it inherently poses. To put it briefly, they want to maximise the benefits of AI systems while at the same time prevent and minimise their risks.

The silver lining of the guidelines is trust. The HLEG AI wants to create a framework to ensure and scale Trustworthy AI. This notion refers to, not only the AI systems themselves, but relates to all actors and processes that are part of the socio-technical context of the system. Trustworthiness of an AI system comes down to **three components**, which should be met throughout the system's entire life cycle.[12] The HLEG AI considers each of these components necessary to achieve Trustworthy AI. Nevertheless, they are not sufficient in itself.

1. It should be **lawful**, complying with all applicable laws and regulations;
2. It should be **ethical**, ensuring adherence to ethical principles and values; and
3. It should be **robust**, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm.

The HLEG AI indicates that they prefer a situation of harmony, but they do realise that tensions may arise between the three components. Moreover, they stress that each situation has a different problems and solutions. In that regard the example given is an AI music recommendation system that clearly does not raise equal ethical concerns compared to an AI system suggesting critical medical treatments.

Lawful AI

The lawfulness simply refers to legally binding rules governing development and use of AI on international, European and national level. As mentioned before, there is no AI-specific regulation yet, nevertheless there are several other sources of primary and secondary EU law applicable to artificial intelligence (such as GDPR and the Product Liability Directive[13]) and both international and national laws. Moreover, depending on the sector, sector-specific rules may be applicable as well.

The HLEG AI guidelines do not give any further clarification on what these rules are. To put if differently, the expert group does not provide any legal advice, but simply stresses that the legal rules remain mandatory to comply with and that they must be duly observed.

Ethical AI

AI systems are required to follow ethical norms in order to be considered trustworthy. These are especially relevant since the positive law might encounter difficulties adapting to technological developments. Where legislation lacks speed to keep up with new technologies, a situation of which AI is an accurate example, ethics fills the gap.

---

[11] ibid., p. 4.
[12] ibid., p. 5.
[13] Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, *OJ L* 210, 7 August 1985.

Robust AI

AI systems are expected to be both technically and socially robust. Robustness refers to a situation where society and individuals can trust AI systems not to cause any unintentional harm. The HLEG AI makes clear that such systems should perform in a safe, secure and reliable manner, and safeguards should be foreseen to prevent any unintended adverse impacts.[14]

The Expert group continues by outlining the structure of their guidelines. The document is divided into 3 chapters, starting at a more abstract level of guidance (Chapter 1 - the foundations of Trustworthy AI), to more concrete assessment instructions (Chapter 3 - Assessing Trustworthy AI). The Figure 2 below provided by the HLEG AI gives an overview of the framework[15]:

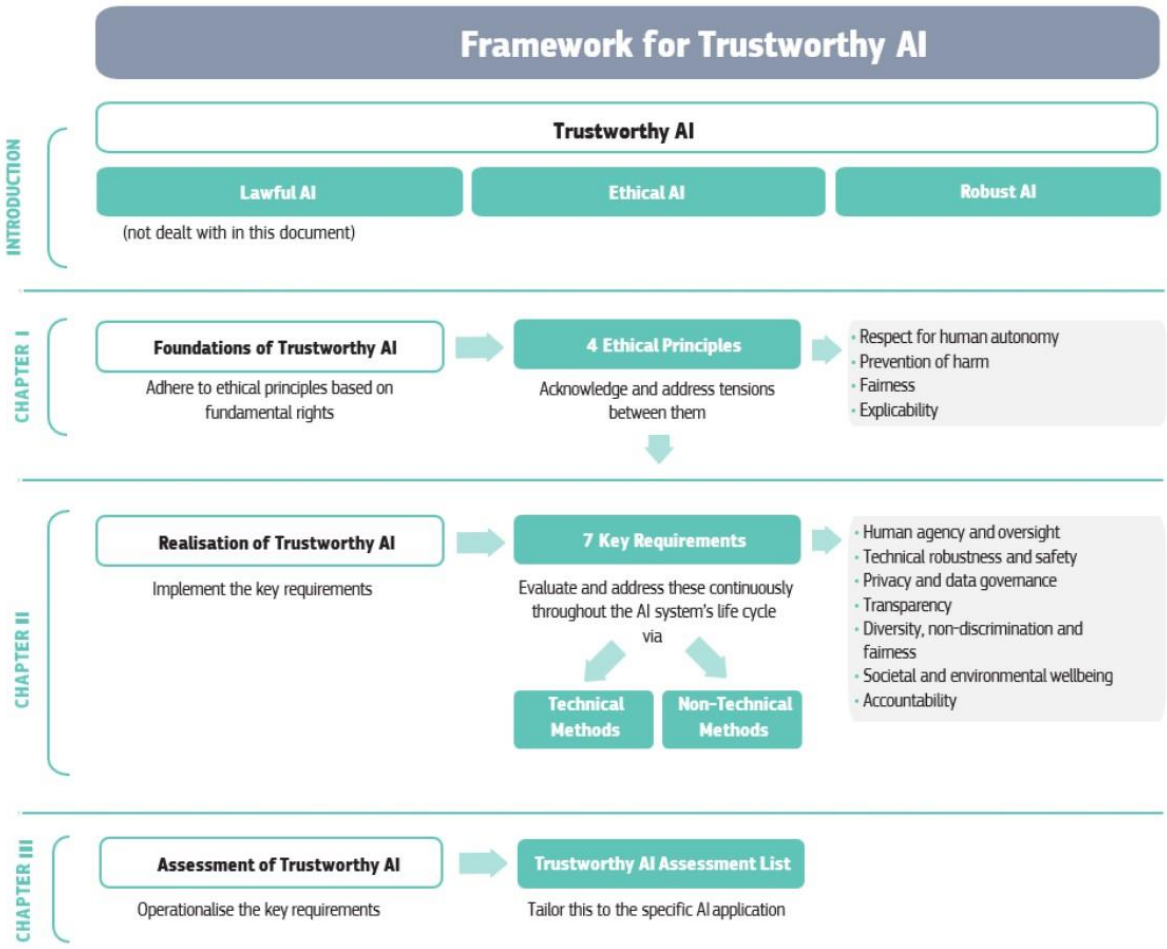

Figure 2: The guidelines as a framework for Trustworthy AI

The first chapter sets out the **foundations of Trustworthy AI** (See Figure 2). It prescribes four ethical principles, based on fundamental rights. The main goal of AI ethics is to identify concerns relating to

[14] ibid., p. 7.
[15] ibid, p. 8.

quality of life, human autonomy and freedom of individuals in a democratic society, and how AI can help improve these aspects of an individuals' life.

The foundation is first of all to be found in the EU and international treaties on fundamental rights. These rights are united by one common idea, namely "respect for human dignity". This is also called a human-centric approach, meaning that "the human being enjoys a unique and inalienable moral status of primacy in the civil, political, economic and social fields". [16] Underneath these fundamental rights four ethical principles can be identified. These principles, or rights, are generally the subject of legally binding rules in the EU. To put it differently, EU members states have to comply with these four principles because, by means of EU and international human rights treaties, the principles are legally enforceable. However, there is more to the story than enforceable rights (lawful AI). Ethical reflection allows for a better understanding of the relationship between the development, deployment and use of AI systems on the one hand and fundamental rights and their underlying values on the other hand.

The four ethical principles are rooted in fundamental rights. The HLEG AI stresses that they are specified as ethical imperatives, meaning that AI developers should always strive to adhere to them. Nevertheless, these principles are to a large extent already reflected in current legal frameworks. There is an overlap between lawful AI and ethical AI. The idea is that while many legal obligations reflect ethical principles, adherence to ethical principles goes beyond formal compliance with existing laws.[17]

1. The principle of respect for human autonomy

Humans must be able to keep full and effective self-determination over themselves when interacting with AI systems and should be able to partake in the democratic process. Humans cannot be manipulated, coerced, deceived, conditioned or herd by AI systems. On the contrary, AI systems are expected to support, empower, and even augment human skills. Human oversight over work processes in AI systems should be secured, as consequence of the human-centric approach.

2. The principle of prevention of harm

Human dignity as well as mental and physical integrity should be carefully protected. Therefore, AI systems are required to be technically robust and should operate in a safe and secure way. This to avoid AI systems causing harm or adversely affect human beings. The HLEG AI stresses to pay more attention to specifically precarious situations concerning vulnerable persons, or asymmetries of power such as employer – employee and government – citizens relations.

3. The principle of fairness

The development, deployment and use of AI systems must be fair. Fairness is understood by the HLEG AI to have a substantial and a procedural dimension. Procedural fairness refers to giving people a possibility to contest and to seek effective redress against decisions made by AI systems and by the humans operating them. In practice this dimension implies that the accountable entity is identifiable, and that the decision-making process is explicable. Substantial fairness refers to protection against unfair bias, discrimination, and stigmatisation.

---

[16] ibid., p. 10.
[17] ibid., p. 12.

4. The principle of explicability

AI systems should be transparent and open, with explainable decisions. If not explainable, the aspect of procedural fairness becomes meaningless. If people do not know what is happening and how it is happening, they cannot seek redress. However, it is not always possible to explain how an AI system (for example, deep learning algorithms) comes to a certain decision. This is situation is referred to as a black-box. The HLEG AI clarifies that is not a black-and-white story, "the degree to which explicability is needed is highly dependent on the context and the severity of the consequences if that output is erroneous or otherwise inaccurate".[18]

The HLEG AI indicates that tensions may rise between these principles. Therefore, one needs to establish the "methods of accountable deliberation" to deal with these issues. Problematic situations may especially arise in relation to the principles of human autonomy and prevention of harm. The example given is an AI system which helps to combat crime, but therefore, due to surveillance activities, infringes liberty and privacy.

In a final note the HLEG AI recognizes the fact that it concerns mere abstract ethical prescriptions which do not always offer a straightforward solution. The approach to deal with ethical considerations cannot be intuitive, but should be rational and evidence-based.

The second chapter of the guidelines shifts to the **practical implementation of "Trustworthy AI"**. Building on the previously identified foundational principles the expert group sets out 7 requirements to achieve Trustworthy AI. These are applicable to the various stakeholders throughout the AI systems' life-cycle: developers, deployers, end-users and broader society. The HLEG AI provides a definition for each of these groups.[19]

Developers are understood as "those who research, design and/or develop AI systems". This group should implement the 7 requirements in the design and development process of the AI system.

Deployers refers to "public or private organisations that use AI systems within their business processes and to offer products and services to others".

End-users are "those engaging with the AI system, directly or indirectly". Broader society simply refers to others affected by AI systems, directly or indirectly. These two groups are entitled to be informed and should be able to request the requirements to be upheld.

<u>The list of 7 requirements:</u>

There is no hierarchy between the requirements, meaning that they are all equally important. Nevertheless, the importance may differ depending on the practical use-case at hand. Special attention should be given to AI system affecting individuals, implying that for instance for mere industrial applications the implications are less severe.

[18] ibid., p. 13.
[19] ibid., p. 14.

1. Human Agency and oversight

This first requirement is related to the ethical principle of respect for human autonomy stating that AI systems should support human autonomy and decision-making. Human agency and oversight are two separate notions.

Human agency refers to the ability of users to make informed autonomous decisions regarding AI systems. This requirement translates into an information obligation towards the individual: ”They should be given the knowledge and tools to comprehend and interact with AI systems to a satisfactory degree and, where possible, be enabled to reasonably self-assess or challenge the system.” In practice this is closely linked to Art. 22 of the GDPR.[20] Human agency aims at avoiding AI systems to unfairly manipulate, decept, herd and condition individuals.

Human oversight refers to the involvement of human in the AI’s decision-making process, thereby preventing that the AI system would undermine human autonomy or cause adverse effects. There are three different mechanisms to achieve human oversight: human-in-the-loop (HITL), human-on-the-loop (HOTL), human-in-command (HIC). The HLEG AI defines these notions as follows:

- HITL refers to the capability for human intervention in every decision cycle of the system, which in many cases is neither possible nor desirable.
- HOTL refers to the capability for human intervention during the design cycle of the system and monitoring the system’s operation.
- HIC refers to the capability to oversee the overall activity of the AI system (including its broader economic, societal, legal and ethical impact) and the ability to decide when and how to use the system in any particular situation.[21]

Once again, the degree of human oversight needs to be assessed in relation to the specific use-case. However, as a general rule, the less human oversight over an AI system, the more extensive testing and stricter governance is required.

2. Technical robustness and safety

Technical robustness is closely linked with the ethical principle prevention of harm. It is a requirement referring, in general, to reliability and safety of AI systems. The physical and mental integrity of humans should be ensured. In order to achieve this result, the expert group identifies four different aspects. First of all, the results of an AI system should be reproducible and reliable. Moreover, the system should be accurate, referring to its ability to make correct judgements. The third aspect is the requirement to have a fallback plan in place. A fallback plan could be seen as a switch off-button in case of problems, making sure that a human operator intervenes before continuing their actions. The higher the risk, the more crucial such safety measures will be. The final component of this second requirement is resilience to attack and security, referring to the protection of the AI system from attacks against both software and hardware.

[20] Art. 22 GDPR is the right not to be subject to a decision based solely on automated processing when this produces legal effects on users or similarly significantly affects them.
[21] EC, *Ethics guidelines for trustworthy AI*, 8 April 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, accessed 04 June 2021, p. 16.

3. Privacy and data governance

Linked to the principle of prevention of harm, this requirement encompasses two components. Privacy as a fundamental right and adequate data governance. On the one hand compliance with the legislation on privacy and data protection will be required. On the other hand, the quality and integrity of the data used in the AI system are to be guaranteed. The latter is of particular importance in the context of AI since the quality of the data sets used is paramount to the performance of AI systems. Social biases, inaccuracies, mistakes in data sets are inclined to magnify (exponentially) when using self-learning algorithms. Moreover, the expert group stipulates that protocols should outline who can access data and under which circumstances.

4. Transparency

AI systems are expected to be transparent about the data, the system and the business model.[22] The expert group considers transparency to encompass "traceability, explainability and communication". Traceability which essentially comes down to a detailed documentation of the processes of an AI system, will increase explainability. Explainability refers to being able to explain the technical processes of AI systems as well as the related human decisions. A stakeholder should be able to understand why the AI system makes a certain decision, especially when affecting individuals' lives. Communication has a more specific meaning in this context. The HLEG AI clarifies that an AI system must be identifiable as such. Humans must be in a position where they know they are interacting with an AI system.

This requirement is linked to the ethical principle of explicability.

5. Diversity, non-discrimination and fairness

Mainly referring to the avoidance of unfair biases, this requirement finds its foundation in the principle of fairness. One of the major concerns when using AI systems are biases rooted in the training-datasets. The HLEG AI warns that "the continuation of such biases could lead to unintended (in)direct prejudice and discrimination against certain groups or people, potentially exacerbating prejudice and marginalisation" and that "harm may result from the intentional exploitation of consumer biases by engaging in unfair competition".

In practice not only the datasets can suffer from biases, but also the way in which AI system are developed, i.e. the way in which algorithms are programmed. In order to address this potential risk, a good oversight process should be put in place. Moreover, a diversified hiring strategy (people from different backgrounds, cultures and disciplines) will be required.

6. Societal and environmental wellbeing

The ethical principles of fairness and prevention of harm imply that the interests of broader society are to be taken into account throughout the AI system's life cycle. The idea is that AI systems should benefit all human beings including future generations. Therefore, AI systems should be sustainable and environmentally friendly; the impact of these systems on our individual social relations must be

[22] ibid., p. 18.

considered carefully; the same goes for the impact on society at large and democracy (think about influencing elections).

7. Accountability

The final requirement is complementing the other requirements. Accountability requires to put in place mechanisms to ensure responsibility for AI systems and their outcomes. The expert group stipulates that this encompasses auditability, minimisation, and reporting of negative impact. Nevertheless, it acknowledges that trade-offs between these requirements will sometimes be inevitable. The HLEG AI attaches great importance to the rational and methodological manner within in the state of the art, to deal with such trade-off. Moreover, mechanisms should be in place allowing individuals or groups to seek redress, creating a crucial element of trust.

Auditability refers to the evaluation of algorithms, data and design processes by internal and external auditors. Minimisation is the idea where the potential negative impact of AI systems must be kept to a minimum. Reporting plays an important role here. Therefore, protection of whistle-blowers and other organizations (like NGOs or trade unions) is key when expressing their concerns about certain AI systems.

Realisation of Trustworthy AI

The next step in the process of realizing Trustworthy AI is implementing the abovementioned requirements. Implementation is a story of both technical and non-technical methods (See Figure 3).

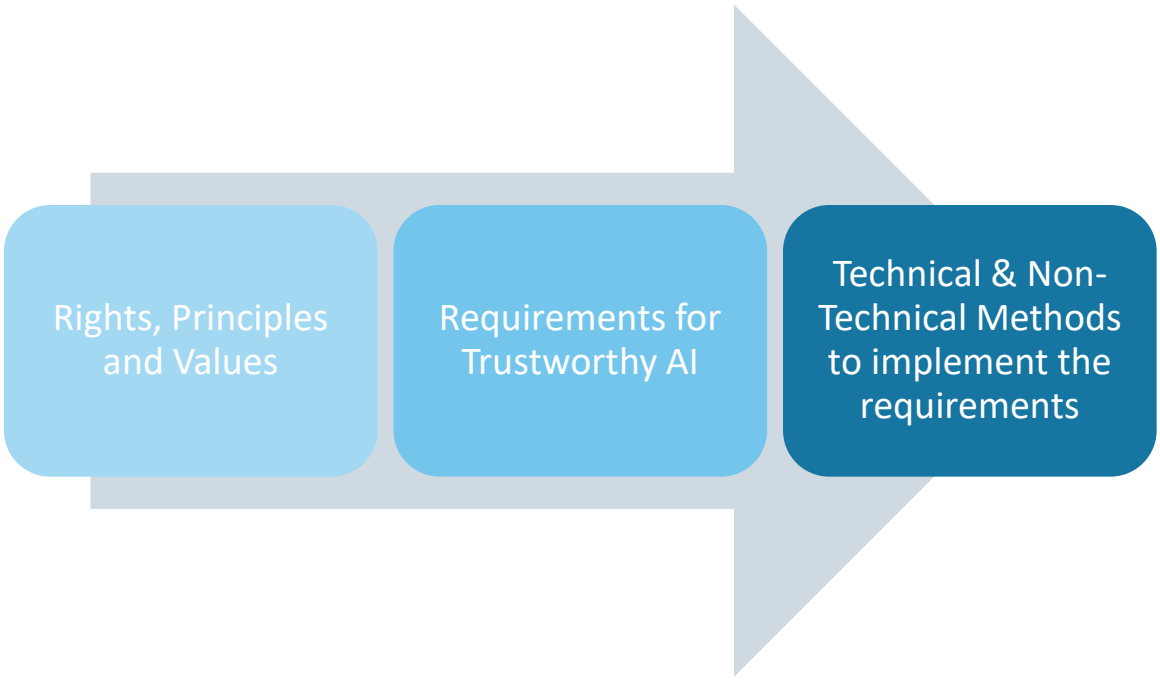

Figure 3: Realising Trustworthy AI throughout the system's entire life cycle.[23]

[23] ibid., p. 20.

Since the scope of this deliverable is limited to the identification of the applicable framework for the CoRoSect project, there will be no in-depth analysis of the technical and non-technical methods. Such analysis will however fall within the scope of deliverable D1.2.

Table 1 below gives an overview of the proposed methods:

Technical methods	Non-technical methods
Architectures for Trustworthy AI	Regulation
Ethics and rule of law by design (X-by-design)	Codes of conduct
Explanation methods	Standardisation
Testing and validating	Certification
Quality of Service Indicators	Accountability via governance frameworks
	Stakeholder participation and social dialogue
	Education and awareness to foster an ethical mind-set
	Diversity and inclusive design teams

Table 1: An overview of the proposed methods of Trustworthy AI

Assessing Trustworthy AI

The third chapter of the HLEG AI guidelines contains the so-called Assessment list for Trustworthy AI. This assessment list is directed towards developers and deployers of AI systems and should allow them to operationalise the requirements for trustworthy AI from the second chapter. However, the list does not reflect legal compliance. Compliance with the relevant legislation (called lawful AI) is yet to be achieved. To put it differently: compliance with the assessment list does not guarantee legal compliance.

The expert group indicates that organizations should implement the list into existing governance mechanisms (or create new ones). It is a good practice to give the implementation attention at the highest level of the management structure as well as on operational levels (legal, HR, compliance, procurement…).[24] The list does not provide answers to all questions that might rise. The core idea is that the assessment needs to be in relation and in proportion to each specific use-case. The list encourages reflection on how Trustworthy AI can be operationalised by an organization.

The guidelines contain an initial version of the assessment list. Anno 2021, the relevant version is the final version of July 2020.[25]

Examples of opportunities and critical concerns raised by AI

In the last section the guidelines tackle some specific situations.[26] The HLEG AI provides three examples of AI opportunities and five situations where critical concerns towards the use of AI can be expressed. The first category concerns societal challenges where the EU encourages to use AI in order

[24] ibid., p. 25.
[25] EC, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment, accessed 04 June 2021.
[26] EC, *Ethics guidelines for trustworthy AI*, 8 April 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, accessed 04 June 2021, p. 30-35.

to treat/solve them more efficiently. Often these challenges are also reflected in the UN Sustainable Development Goals.[27]

1. Climate action and sustainable infrastructure
2. Health and well-being
3. Quality education and digital transformation

Particularly relevant for CoRoSect is the idea of creating sustainable infrastructure since insect farming might represent a potential sustainable solution for food security in the 21st century. CoRoSect will provide innovation in the field of robotization and artificial intelligence. This would allow scaling and optimizing insect production facilities, providing more sustainability.[28]

- As the CoRoSect project concerns the use of AI-based technologies, Ethics Guidelines for Trustworthy AI is applicable to the design, development, and the use of these technologies.

On the other side of the spectrum there are AI applications which give rise to (severe) concerns. Usually this concerns situations where one of the conditions for Trustworthy AI is violated. Therefore, there is great likeliness that the situation does not only contradict the AI guidelines, but moreover constitutes an infringement of positive law (such as the GDPR).

1. Identifying and tracking individuals with AI
2. Covert AI systems (referring to the phenomenon that individuals do not know or are not able to find out that they are interacting with an AI)
3. AI enabled citizen scoring in violation of fundamental rights
4. Lethal autonomous weapon systems (LAWS)
5. Potential longer-term concerns

- At first sight the CoRoSect project does not seem to fall under the scope of these situations, at least not directly. Nevertheless, important aspects to keep in mind is informing people working with AI systems about the fact that they are collaborating with an artificial intelligence application and the overall long-term consequences of the AI system.

Conclusion and glossary

HLEG AI concludes its findings by summarizing the key elements of the AI ethics guidelines in the conclusion. At the end of the guidelines, a glossary was added. This glossary provides a definition of some highly relevant notions such as AI system or Bias.

2.2.1.2. Policy and Investment Recommendations for Trustworthy Artificial Intelligence

The second document from the hand of the HLEG AI concerns 33 recommendations which aim at guiding Trustworthy AI towards sustainability, growth and competitiveness, inclusion, while

[27] United Nations (UN) Sustainable Development Goals, https://sustainabledevelopment.un.org/?menu=1300, accessed 04 June 2021.
[28] CoRoSect Proposal, 2.

empowering, protecting and benefiting human beings.[29] The recommendations are directed at EU institutions and EU Member States, following a sector-specific approach (Society at large; Private sector; Public sector; Europe's research and academia). Even though some of the above-mentioned areas are relevant for the CoRoSect project (research, private sector), the recommendations only provide high-level, normative guidelines for authorities.

- From the CoRoSect perspective the document can serve as a valuable insight in the rationale behind other, more tangible rules on AI both at EU as well as on national level.

2.2.1.3. Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment

The European AI strategy continues with a self-assessment list, presented on the 17th of July 2020. This list is the final version of the list initially proposed in the AI ethics guidelines of 2018. It was reviewed by 350 stakeholders in 2019.[30] The foundation for the assessment list are the 7 key requirements for Trustworthy AI, as defined by the Ethics Guidelines, namely:

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

The ALTAI helps to operationalise these requirements by means of a (more) practical checklist. [31] It is intended for self-evaluation purposes[32], and exists in two formats: a paper-based version and an online tool for self-assessment. The list is made out of questions which are best answered, according to the expert group, by a multidisciplinary team of people (including AI designers and developers, data scientists, procurement specialist, front-end staff, legal specialist and management). There are four questions relating to compliance with fundamental rights, followed by a separate chapter for each of the seven requirements. Finally, once again, a (more extensive) glossary of some key notions is provided.

- The ALTAI is also relevant for the CoRoSect project. Part of these questions have already been answered by the consortium's partners in the questionnaire made by KU Leuven and CERTH under their first deliverables. The second deliverable (D1.2 Specification of Ethical and Legal Requirements) will further analyse ALTAI in light of the specified CoRoSect use-cases.

---

[29] HLEG AI, *Policy and Investment Recommendations for Trustworthy Artificial Intelligence*, 26 June 2019, 6, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60343, accessed 04 June 2021.
[30] EC, *Pilot the Assessment List of the Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/futurium/en/ethics-guidelines-trustworthy-ai/register-piloting-process-0, accessed 04 June 2021.
[31] EC, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, 17 July 2020, https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment, accessed 04 June 2021.
[32] HLEG AI, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, 17 July 2020, 3, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342, accessed 04 June 2021.

2.2.1.4. Sectoral Considerations on Policy and Investment Recommendations for Trustworthy AI

On the 23th of July 2020, HLEG AI delivered a final guiding document, the so-called Sectoral Considerations for Trustworthy AI. These sectoral recommendations built on the 2019 Policy and Investment Recommendations and focus on three sectors: public sector, healthcare, and manufacturing and IoT (Internet of Things).[33]

- The CoRoSect project has no actual connection to those specific areas, implying that the project falls outside the scope of the 2020 sectoral recommendations.

2.2.2. European Commission

The European Commission is the main institution in the AI strategy of the EU. However, until very recent the Commission did not take too much action yet. During the course of the period 2018 – 2020 the Commission delivered only one report, the White Paper on AI. Nevertheless, it was the Commission who played an important role by setting up the European AI Alliance and by appointing the HLEG AI. In fact, European Commission presented the HLEG AI's Ethics Guidelines for Trustworthy AI as guidelines that are "central" to the European approach to the governance of AI. In April 2021 the Commission presented a legislative proposal on AI. This is the first major step towards an actual – hard law – regulation of artificial intelligence in the EU.

The Table 2 below provides the timeline of the important milestones of the European AI strategy.[34]

[33] HLEG AI, *Sectoral Considerations on Policy and Investment Recommendations for Trustworthy AI*, 23 July 2020, https://futurium.ec.europa.eu/sites/default/files/2020-07/Sectoral%20Considerations%20On%20The%20Policy%20And%20Investment%20Recommendations%20For%20Trustworthy%20Artificial%20Intelligence_0.pdf, accessed 04 June 2021.

[34] EC, *Strategy for Artificial Intelligence (updated 2021),* https://digital-strategy.ec.europa.eu/en/policies/strategy-artificial-intelligence, accessed 04 June 2021.

April 2021	Fostering a European approach for Artificial Intelligence
April 2021	Legislative proposal on AI
April 2021	Updated Coordinated Plan on AI
April 2020	Impact Assessment
October 2020	2nd European AI Alliance Assembly
July 2020	Inception Impact Assessment
July 2020	Public Consultation - White Paper on Artificial Intelligence
July 2020	Final Assessment List on Trustworthy AI (ALT AI) of the HLEG AI
July 2020	Sectoral Recommendations of Trustworthy AI of the HLEG AI
February 2020	White Paper on AI : a European approach to excellence and trust
December 2019	Piloting of Assessment list on Trustworthy AI
June 2019	1st European AI Alliance Assembly
June 2019	Policy and Investment recommendations of HLEG AI
April 2019	Communication: Building Trust in Human Centric Artificial Intelligence
April 2019	Ethics Guidelines for Trustworthy AI
December 2018	Coordinated Plan on AI (Communication on " AI Made in Europe" - Press Release)
December 2018	Stakeholder Consultation on draft Ethics Guidelines for Trustworthy AI
June 2018	Launch of the European AI Alliance
June 2018	Set up of the High-Level Expert Group on AI (HLEG AI)
March 2018	Press Release on AI Expert Group and European AI Alliance
April 2018	European AI Strategy (Communication: Artificial Intelligence for Europe – Press Release)
April 2018	Staff Working Document: Liability for emerging digital technologies
April 2018	Declaration of cooperation on Artificial intelligence

Table 2: The timeline of the important milestones of the European AI strategy

Pink: the four deliverables of the High-Level Expert Group on AI

Blue: the two regulating deliverables of the European Commission and the Coordinated plan on AI, followed by an updated version anno 2021.

1.2.2.1. Coordinated Plan on Artificial Intelligence (2018)

The Coordinated plan on AI has been updated very recently, therefore it seems relevant to introduce the initial coordinated plan.[35] Published on the 7th of December 2018, the Coordinated Plan on AI was meant as a high-level document on the development and use of AI made in Europe. The idea was to create an eco-system stimulating AI innovation within Europe. The EC states as follows: "Overall, the ambition is for Europe to become the world-leading region for developing and deploying cutting-edge, ethical and secure AI, promoting a human-centric approach in the global context".[36] The plan builds

[35] EC, *Coordinated Plan on Artificial Intelligence of 7 December 2018* (Annex to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions), COM(2018), 795 final.
[36] ibid., p. 1.

on the "Declaration of cooperation" of April 2018 signed by the member states, illustrating their ambition to collaborate in the area of AI.

The Coordinated Plan contains eight points of action:

1. Strategic actions and coordination

This part of the coordinated plan refers to the three pillars, already discussed in the introduction of this chapter: boosting the EU's technological and industrial capacity; preparing for socio-economic changes brought about by AI; ensuring an appropriate ethical and legal framework. Moreover, it confirms that the EC has task the HLEG AI to draft AI ethics guidelines, and has tasked an Expert Group on Liability and New Technologies to assist on the Product Liability Directive's implementation. One of the more ambitious statements is to increase the investment in AI in the period 2018-2020 to at least EUR 20 billion.

2. Maximising investments through partnerships

The Commission is aware of the fact that collaboration is needed between the European institutions, the member states and the private sector. Once again this translates into provision of funds, among others through the H2020 program. Moreover, it aims at putting up Public-Private Partnerships (PPP) and creating a European Innovation Council to support disruptive innovation.

3. Market approach

The Commission acknowledges the importance of research and innovation and of transferring those research activities to industry. The EC identifies three steps in that process: building up research excellence; establishing world-reference testing facilities and accelerating AI take-up through Digital Innovation Hubs. These goals are supported by some concrete numbers on planned investments.

4. Skills and life-long learning

The concern of the EC is that talent, which is an essential element for AI development, needs to be attracted and safeguarded within the EU. Knowledge on information and communications technology (ICT) related topics, should be promoted and stimulated in general.

5. Common European Data Space

Since datasets are essential for training smart algorithms, the Commission stresses the importance of international data flows, within the limits of the EU regulations. Where personal data are processed, the GDPR will be applicable (See Chapter 4 Data Protection and privacy).[37] Where the transfer concerns non-personal data the Regulation on the free flow of non-personal data applies to cross-border data flows in the EU.[38] Of particular interest are: identifying public data sets (for training AI applications); implementation of interoperable data and meta-data formats and development and deployment of standardised Application Programming Interface (API).

[37] 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), *OJ L* 119, 4 May 2016.
[38] Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L* 303, 28 November 2018.

6. Ethics by design and regulatory framework

The commission tasked the HLEG AI to draft ethics guidelines and a European AI Alliance for consultation. A key principle in this context is "ethics by design" implying that "ethical and legal principles are embedded in AI products and services right at the beginning of the design process".[39] Moreover, the Commission will assess whether the existing legislation is fit for tackling new challenges raised by AI. Another key principle will be security by design, whereby cybersecurity, the protection of victims and the facilitation of law enforcement activities should be taken into account from the beginning of the design process.[40]

7. AI for the public sector and international cooperation

The core idea of both (which are separate) action points is cooperation. The Commission reiterates how AI can ameliorate many aspects of the public sector and improve efficiency in public services. To achieve these smarter AI-enabled solutions for all levels of governance, the Commission wants Member States to contribute in an EU-wide exchange of best practises and data, joint procurement of AI solutions. In line with this the Commission stresses that the development of AI will benefit from international cooperation. The EU will promote the AI ethics guidelines internationally, but Member States are requested to, individually, align bilateral outreach efforts.

1.3.2.2. Updated Coordinated Plan on Artificial Intelligence (2021)

The updated version of the Coordinated Plan has been published on the 21st of April 2021.[41] The 2021 review of the Coordinated Plan is considered the next step in creating "EU global leadership on trustworthy AI".[42] The Commission puts forward three general points of action:

1. Accelerate investments in AI technologies to drive resilient economic and social recovery facilitated by the uptake of new digital solutions;
2. Act on AI strategies and programmes by implementing them fully and in a timely manner to ensure that the EU reaps the full benefits of first-mover adopter advantages; and
3. Align AI policy to remove fragmentation and address global challenges.

The review proposes four key sets of proposals for the EU and the Member States aimed at facilitating the European approach to AI and stimulating new opportunities for/with AI technologies (See Table 3 below). The document is consistently structured: on each topic the Commission provides an "Overview of actions taken", reflecting upon what has been achieved in the last years. This is then

[39] EC, *Coordinated Plan on Artificial Intelligence of 7 December 2018* (Annex to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions), COM(2018), 795 final, p. 17.
[40] ibid., p. 8.
[41] EC, *Press Release Coordinated Plan on Artificial Intelligence 2021 Review*, 21 April 2021, https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review, accessed 04 June 2021.
[42] EC, *Coordinated Plan on Artificial Intelligence 2021 Review of 21 April 2021* (Annexes to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence), COM(2021) 205 final, p. 2.

followed by an "Outlook", giving some future perspective on AI development and deployment over the next years.

Enabling conditions for AI development and uptake in the EU	Make the EU the place where excellence thrives from the lab to the market	Ensure that AI works for people and is a force for good in society	Build strategic leadership in high-impact sectors
• Acquire, pool and share policy insights • Tap into the potential of data • Foster critical computing capacity	• Collaborate with stakeholders through, e.g. the European Partnership on AI, Data and Robotics and expert groups • Build and mobilise research capacities • Provide an environment for developers to test and experiment (TEFs), and for SMEs and public administrations to take up AI • Support the funding and scaling of innovative AI ideas and solutions	• Nurture talent and improve the supply of skills necessary to enable a thriving AI eco-system • Develop a policy framework to ensure trust in AI system • Promote the EU vision on sustainable and trustworthy AI in the world	• Bring AI into play for climate and environment • Use the next generation of AI to improve health • Maintain Europe's lead: Strategy for Robotics in the world of AI • Make the public sector a trailblazer for using AI • Apply AI to law enforcement, migration and asylum • Make mobility safer and less polluting through AI • Support AI for sustainable agriculture

Table 3: An overview of key policy objectives outlined in the Updated Coordinated Plan on AI[43]

From the perspective of CoRoSect both the initial as well as the reviewed version of the Coordinated Plan have little practical meaning. The Commission outlines the high-level policy mostly aimed at informing the public/stakeholders on the initiatives taken, urging the Member States to take action, and providing a basis for European and international cooperation. Noteworthy is that the Reviewed Coordinated Plan has become much more extensive since 2018. Since CoRoSect is a cross-border project, notice should be taken of national AI strategies (if adopted).[44]

Countries that have published a national AI strategy: Bulgaria, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Hungary, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Spain and Sweden.

Countries still working on a national AI strategy: Austria, Belgium, Croatia, Greece, Ireland, Italy, Romania and Slovenia.

1.3.2.3. White Paper on AI: a European approach to excellence and trust (2020)

The European Commission establishes some policy options to achieve trustworthy AI while respecting fundamental rights and values of EU citizens.[45] That is the overall subject of the White Paper on AI which is structured in two building blocks: an ecosystem of excellence and an ecosystem.

On the one hand the White Paper encompasses the policy framework. This part sets out measures to align efforts at European, national and regional level. The Commission aimed at achieving an

[43] See ibid., p. 6, 16, 27 and 37.
[44] ibid., p. 59.
[45] EC, *White Paper on Artificial Intelligence*, 19 February 2020, COM(2020) 65 final, 2-3 , commission-white-paper-artificial-intelligence-feb2020_en.pdf, , accessed 04 June 2021.

ecosystem of excellence throughout the entire development and deployment process. This part similar to what is set out in the Coordinated Plan on AI as the Commission stresses the same points of action.

On the other hand, the White Paper tries to create an ecosystem of trust. Here the Commission retakes many elements set out in the HLEG AI Ethics Guidelines, such as the human-centric approach and the seven requirements for Trustworthy AI. This part of the paper focusses on compliance with EU rules and fundamental right, with specific attention for AI systems posing a high risk. This idea of differentiation between AI systems posing little risks and high-risk systems is coming back in the recently published proposal for the Artificial Intelligence Act.

The White Paper on AI stresses the importance of creating an actual legal framework on AI in Europe. The Commission opened the dialogue by means of a public consultation of Member States civil society, industry and academics.[46] In April 2021, having received and analysed all feedback, the EC publishes a proposal for an "Artificial Intelligence Act".

1.3.2.4. Artificial Intelligence Act

The 21st of April 2021 the European Commission proposed the first ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally.[47] The Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) is very extensive (108 pages). This deliverable tries to capture the essence of the proposed act. Figure 4 below provides a brief overview of the Artificial Intelligence Act.

[46] EC, *White Paper on Artificial Intelligence: Public consultation towards a European approach for excellence and trust, Consultation Results*, 17 July 2020, https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence, accessed 04 June 2021.

[47] EC, *Proposal of 21st April 2021 for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts*, COM(2021) 206 final, https://ec.europa.eu/newsroom/dae/redirection/document/75788, accessed 04 June 2021.

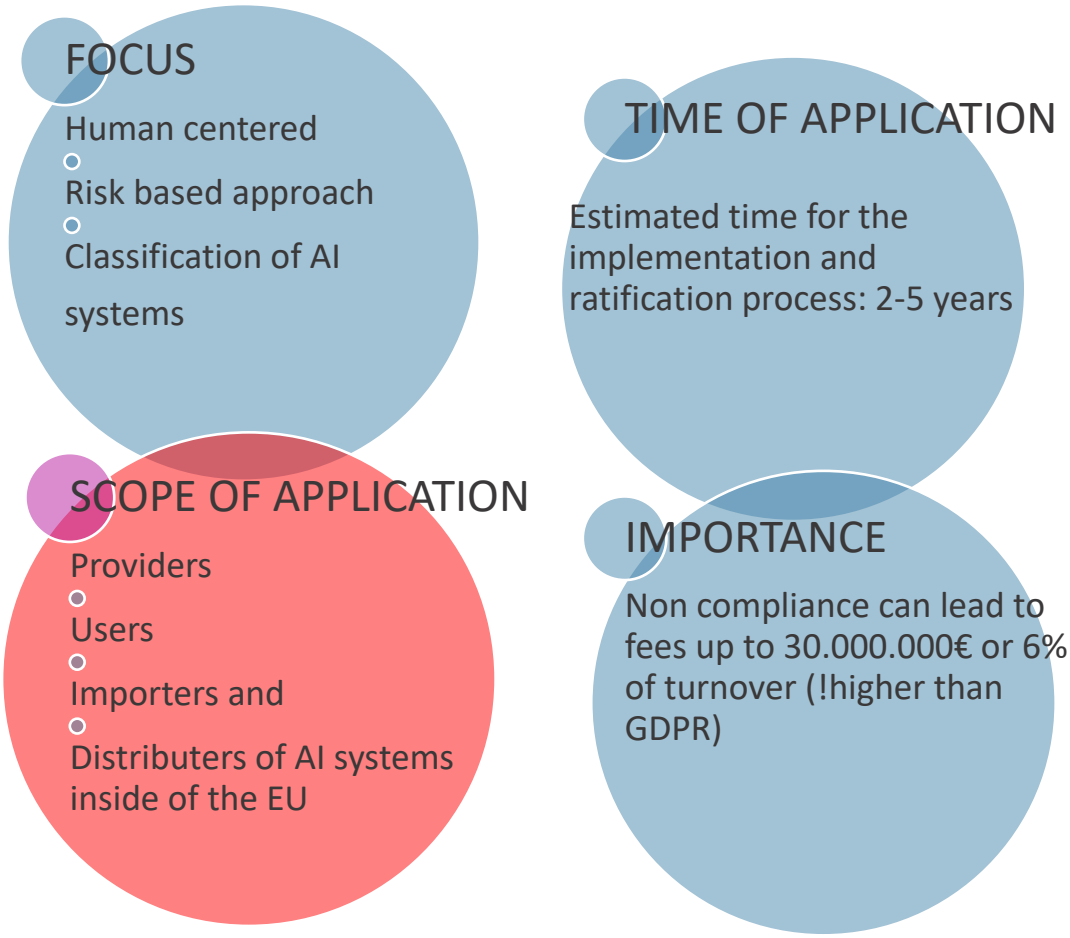

Figure 4: An overview of the Artificial Intelligence Act[48]

The AI Act aims at providing a legislative framework for dealing with AI in the future. It fosters collaboration and a level playing field between EU Member States and protecting citizens' fundamental rights; it enforces quality throughout the AI life cycle; it emphasises the ethical application of AI. The Act expresses the intention to achieve these goals by creating and implementing a single standard across the EU, ensuring legal certainty and implementing a public EU databases containing high-risk AI practises. The overall tension the proposal tries to handle is driving innovation on the one hand, while also mitigating the risks of AI on the other.

Moreover, it is noteworthy that the sanctions on violating the proposed regulation are severe, even more severe than the GDPR's Art. 83.[49] Infringements (of Art. 5 and Art. 10) of the proposal can lead to penalties up to 30M EUR or 6% of global annual turnover. In comparison: the highest penalty under the GDPR leads to an administrative fine of 20M EUR or 4% of the annual turnover.

[48] Deloitte Germany (Risk Advisory), *Artificial Intelligence Act*, May 2021, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Deloitte%20TAI%20DE%20-%20Artificial%20Intelligence%20Act.pdf, accessed 04 June 2021, p. 2.
[49] Art. 83 GDPR puts forward the general conditions for imposing administrative fines.

Lack of compliance with other provisions of the AI Act may result in a fine of 20M EUR or 4% of the global annual turnover. Lastly, when incorrect or misleading information is submitted to the relevant authorities, the proposal imposes a fine up to 10M EUR or 2% of the global annual turnover.[50]

- The scope of application of the AI Act is defined as "providers, users, importers and distributers of AI systems inside of the EU", implying that the Artificial Intelligence Act will undoubtfully be applicable to the CoRoSect project since the project involves both development and deployment of AI systems.
- Even though the AI Act is just a first proposal, meaning that a lot of its provisions can (and probably will) change, the European Commission gives a clear indication of where it wants to go with their AI policy. CoRoSect should keep in mind that the bar is set at a high level with serious financial repercussions, and that it is not unlikely a final version of the AI Act will exist by the time the 3-year project ends.

Scope of application

Art. 3 is a list of 44 definitions relevant to the proposal. The first definition might be the most relevant at this point since it defines what an "artificial intelligence system" or "AI system" is. According to the proposal an AI system concerns "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".[51]

Translated into "AI models" this would cover:[52]

1. Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
2. Logic and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
3. Statistical approaches, Bayesian estimation, search, and optimization methods.

According to recital 6 of the Artificial Intelligence Act "the notion of AI system should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments" and "AI systems can be designed to operate with varying levels of autonomy and be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded)." The idea behind this approach is to future-proof the

[50] Art. 71 of the Proposal of 21st April 2021 for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, COM(2021) 206 final, https://ec.europa.eu/newsroom/dae/redirection/document/75788, accessed 04 June 2021, (Artificial Intelligence Act).
[51] ibid., Art. 3.1.
[52] According to Risk Advisory Department of Deloitte Germany, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Deloitte%20TAI%20DE%20-%20Artificial%20Intelligence%20Act.pdf, accessed 04 June 2021.

definition of AI by making it so technologically neutral as possible to anticipate and include machine learning, deep learning, hybrid systems as well as not yet known or developed techniques.

Moreover, AI systems, in some specific situations, should also fall within the scope of the Act even when they are "are neither placed on the market, nor put into service, nor used in the Union".[53]

Art. 2 of the proposal defines the scope of application of the regulation. The regulation is suggested to apply to:

a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;

b) users of AI systems located within the Union;

c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union.[54]

When a high-risk AI system is a product or systems falling under the scope of some particular directives/regulations, only Art. 84 of the AI Act would apply.[55] It concerns the acts listed in the Table 4 below, which are not applicable for CoRoSect:

Regulation (EC) 300/2008	Civil Aviation Security
Regulation (EU) No 167/2013	Approval and market surveillance of agricultural and forestry vehicles
Regulation (EU) No 168/2013	Approval and market surveillance of two- or three-wheel vehicles and quadricycles
Directive 2014/90/EU	Marine equipment
Directive (EU) 2016/797	Interoperability of the rail system
Regulation (EU) 2018/858	Approval and market surveillance of motor vehicles and their trailers, as well as systems, components and separate technical units intended for such vehicles
Regulation (EU) 2018/1139	Civil Aviation - establishing a European Union Aviation Safety Agency
Regulation (EU) 2019/2144	Approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users.

Table 4: List of acts to which only Art. 84 of the Articifial Intelligence Act apply.

[53] Artificial Intelligence Act, Recital 11.
[54] ibid., Art. 2.1
[55] ibid., Art. 2.2.

The Artificial Intelligence Act shall not apply to:[56]

- AI systems developed or used exclusively for military purposes;
- Public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States;
- Purely private, non-commercial use[57].

Types of AI systems

A final observation with regard to applicability concerns the types of AI systems. The silver lining of the proposal is that it differentiates AI systems based on their potential for hazards and risks, enclosing a risk-based approach. Four types of AI systems classified by the Artificial Intelligence Act are outlined in the Figure 5 below.

[56] ibid., Art. 2.3 and 2.4.

[57] Deloitte Germany (Risk Advisory), *Artificial Intelligence Act*, May 2021, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Deloitte%20TAI%20DE%20-%20Artificial%20Intelligence%20Act.pdf, accessed 04 June 2021, p. 6.

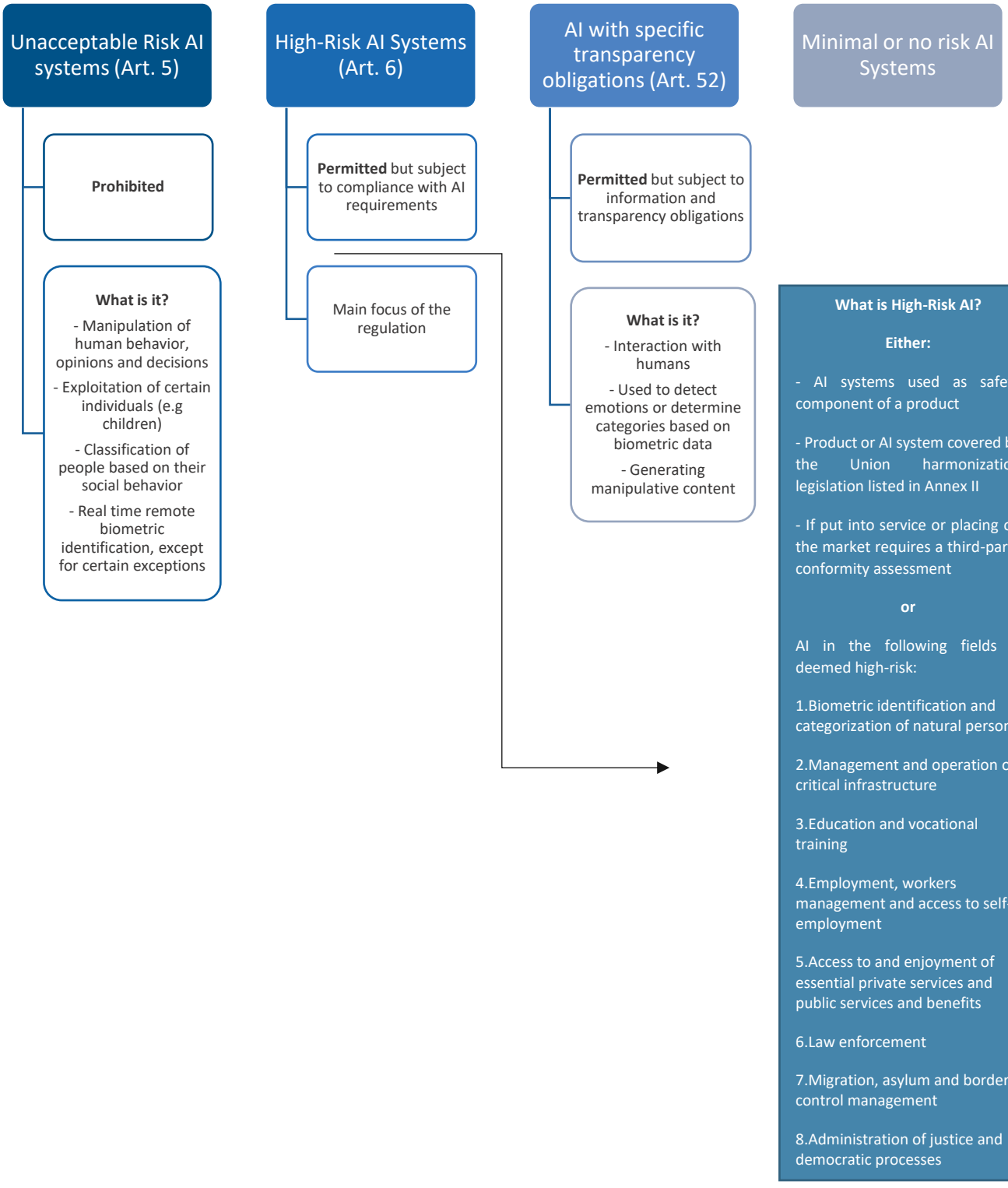

Figure 5: An overview of four types of AI systems classified by the Artificial Intelligence Act[58]

[58] Deloitte Germany (Risk Advisory), *Artificial Intelligence Act*, May 2021, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Deloitte%20TAI%20DE%20-%20Artificial%20Intelligence%20Act.pdf, accessed 04 June 2021, p. 7.

The term of "High-Risk AI System" is not defined, but the proposal indicates in Articles 6 and 7 the criteria to be used to determine whether a system should be considered high risk.[59] Art. 6 refers to products or components that are covered by existing EU product safety legislation that is listed in Annex II to the Proposal. This Annex II refers to legislation going from civil aviation safety to marine equipment. Art. 7 refers to the AI systems from Annex III, ranging from biometric identification to the administration of justice and democratic processes.

Regarding the list of high-risk AI systems of Art. 6, please note that not every AI system in the fields mentioned is necessarily high-risk. Moreover, the list shall be updated regularly (12 months – Art. 84). When an AI system is considered to be a High-Risk AI system, the system will be subject to stringent quality standards and several monitoring requirements (Risk Management, Data Governance, Record Keeping, Technical Documentation, Human Oversight, Transparency, Robustness, Accuracy and Cybersecurity).

This recently published proposal for an Artificial Intelligence Act is highly relevant for all AI-driven applications, systems, methods, techniques developed and used within CoRoSect.

- Based on the proposal of the Artificial Intelligence Act, the following could be (preliminary) concluded in the context of CoRoSect:

  1. CoRoSect both develops and uses "systems" which are included in the definition of an "Artificial Intelligence System" of Art. 3.1.

  2. CoRoSect falls within the scope of application of the proposal (Art. 2). At first sight the projects' partners will either be "providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country (a)", either "users of AI systems located within the Union (b)". The Artificial Intelligence Act applies to CoRoSect.

  3. CoRoSect does not fall under the categories only governed by Art. 84 of the proposal, nor does it concern "military purposes" or "public authorities and international organisations using AI systems for reasons or justice or law enforcement".

  4. CoRoSect makes use of different types of AI (image recognition analysis, autonomous vehicles, sound recognition…). A detailed answer in the "AI and Ethics" questionnaire under WP1 (T1.1) allows to identify the exact technologies. Concerning the type of AI system:
     - CoRoSect does not include "unacceptable risk AI systems" (Art. 5).
     - CoRoSect does not include "high-risk AI systems" (Art. 6). However, the exact scope of Annex II and Annex III is not entirely clear yet and needs to be monitored carefully. For example: we are faced with an ongoing discussion on remote

[59] J. TIELEMANS, A look at what's in the EU's newly proposed regulation on AI, *Iapp* 2021, https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/, accessed 04 June 2021.

biometric identification. The EPDS immediately issued a statement that the current proposal is not strict enough when it comes to facial recognition.[60]

- CoRoSect includes "human-robot collaboration". Therefore Art. 52 on "AI with specific transparency obligations" is applicable. Of particular importance is paragraph 1 "Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence".
- CoRoSect includes "Minimal or no Risk AI systems". These are permitted without restrictions.

[60] EDPS, *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary - Press Release*, 23 April 2021, https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en, accessed 04 June 2021.

3 Legal framework on safety and liability

A fundamental principle in the EU is that all products put on the market should be safe. As deficiencies in the products may have serious consequences on individuals, including on their health, physical and mental well-being, product safety constitutes one of the public policies of the EU. The established legal framework on safety at EU level therefore aims to ensure that all products and services operate safely, reliably, and consistently.[61] Legal safety framework is complemented by the liability framework at the EU and national level, which requires the damage having occurred to be remedied efficiently. A robust and reliable safety and liability framework protects the individuals' rights and public interest, promotes business incentives for innovation by providing legal certainty, as well as creating trust for products and services on the market.[62]

Emerging technologies creates uncertainty as to whether and how the existing legal framework should apply to them because "AI, the IoT and robotics are transforming the characteristics of many products and services."[63] Therefore, safety and liability issues in the context of new technologies, particularly AI, have been subject to a fair amount of recent studies and policy documents within the EU. In 2016, one of the first such document has been published as an independent study, which was requested by the European Parliament's (EP) Committee on Legal Affairs.[64] It addressed the main ethical challenges in relation with robotics and was followed by other studies and recommendations by the European Parliament.[65]

In March 2018, European Commission set up an "Expert Group on Liability and New Technologies" (Expert Group on Liability) with a mandate to support the European Commission by providing expertise on the applicable framework and assisting in the development of a new framework[66]. The Expert Group on Liability is divided in two sub-groups[67]:

1. Product Liability Directive Formation, tasked with addressing issues arising from the Product Liability Directive

---

[61] EC, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, 19 February 2020, COM(2020) 64 final, https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf, accessed 04 June 2021, p. 1.

[62] ibid.

[63] ibid.

[64] N. NEVEJANS, *European Civil Law Rules in Robotics*, October 2016, https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf, accessed 09 June 2021.

[65] T. EVAS, *A common EU approach to liability rules and insurance for connected and autonomous vehicles: European Added Value Assessment*, 2018, https://op.europa.eu/en/publication-detail/-/publication/df658667-20f1-11e8-ac73-01aa75ed71a1/language-en, accessed 09 June 2021; EP, *Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)),* 16 February 2017, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html, accessed 09 June 2021.

[66] O. DHEU, EU report on AI, new technologies and liability : key take-aways and limitations, 9 January 2020, https://www.law.kuleuven.be/citip/blog/eu-report-on-ai-new-technologies-and-liability-key-take-aways-and-limitations/, accessed 09 June 2021.

[67] Register of Commission Expert Groups and Other Similar Entities, *Expert Group on liability and new technologies (E03592)*, https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3592, accessed 09 June 2021.

2. New Technologies Formation, tasked with developing principles and guidelines to adapt the applicable laws to new technologies.

In November 2019, Expert Group's New Technologies Formation published its report "Liability for Artificial Intelligence and other emerging digital technologies", providing its main findings on civil liability challenges raised by digital technologies, and proposing recommendations with regard to adapting current legal mechanisms.[68] Subsequently, European Commission published the document "Report the safety and liability implications of artificial intelligence, the internet of things and robotics" in February 2020.[69] It is followed by an independent study commissioned and published by the European Parliament in July 2020[70], and a resolution adopted by the European Parliament in October 2020, which requests from the European Commission to submit to the European Parliament a regulation proposal on liability for the operation of AI-systems.[71]

The key issues and concerns regarding safety and liability have been raised by the above-mentioned studies and policy documents. It has been generally acknowledged that the existing safety and liability framework in the EU applies to the products and services integrated with emerging digital technologies such as AI and robotics, albeit with shortcomings. New Technologies Formation of the Expert Group on Liability opines that the "liability regimes in force in the Member States ensure at least basic protection of victims whose damage is caused by the operation of such new technologies".[72] However, it further notes that "the specific characteristics of these technologies and their applications – including complexity, modification through updates or self-learning during operation, limited predictability, and vulnerability to cybersecurity threats – may make it more difficult to offer these victims a claim for compensation in all cases where this seems justified."[73] If therefore concludes that the EU and national liability regimes may need to be amended to ensure a fair and efficient allocation of liability.

In order to address the challenges involved in the AI and robotics, it is crucial to understand the existing safety and liability regime in the EU. This chapter will therefore provide information on the applicable safety and liability legislation in the EU and a preliminary analysis on its applicability to CoRoSect. An in-dept analysis on the applicability and special issues concerning AI-based technologies and robotics will be further discussed in the D1.2 Ethical and Legal Requirements Specification Report. This chapter will firstly provide the safety framework that has not been already covered in the previous chapter, and secondly the fundamental underpinnings of liability, especially product liability.

---

[68] Expert Group on Liability and New Technologies (New Technologies Foundation), *Report on Liability for Artificial Intelligence and other emerging digital technologies*, 2019.
[69] EC, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, 19 February 2020, COM(2020) 64 final.
[70] A. BERTOLINI, *Artificial Intelligence and Civil Liability,* European Parliament, July 2020.
[71] EP, *Civil liability regime for artificial intelligence European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence,* (2020/2014(INL)), 20 October 2020.
[72] Expert Group on Liability and New Technologies (New Technologies Foundation), *Report on Liability for Artificial Intelligence and other emerging digital technologies*, 2019*,* p. 3.
[73] ibid.

3.1. Safety

EU product safety framework plays a key role in safeguarding the health and safety of consumers, workers, users and the protection of environment. The framework includes legislation on general product safety[74], as well as legislation addressing specific sectors and products (e.g. medical devices, marine equipment). It aims to addresses the risks such as mechanical and electrical risks to ensure that a product is safe and any potential damages and injuries can be avoided.[75] It also addresses the "use of the product", which is a relevant issue for ensuring safety.[76] For instance, based on a risk assessment carried out in relation with the machinery design and construction, manufacturers are required to consider the limits of the machinery, including "the intended use" and any "foreseeable misuse" of the machinery that is being designed or constructed.[77]

Generally, those who are placing their products in the EU/European Economic Area (EEA) market should ensure the following:

- Only safe products should be placed in the market
- Consumers should be informed about the risks involved in the product
- Any dangerous products should be traced and removed from the market

Cybersecurity may also be a factor that concerns the safety of the product and its users. Although cybersecurity threats are not generally addressed by the mandatory provisions of the EU safety framework, some specific legislation includes provisions on security measures. This is, for instance, the case in Regulation on Medical Devices.[78] The European Union Regulation (EU) 2019/881 Cybersecurity Act also establishes a voluntary cybersecurity certification framework for ICT products and services. In the following pages, Machinery Directive and the Cybersecurity Act are further examined.

3.1.1. Machinery Directive

The Machinery Directive of 2006 is one of the main legislations governing the harmonisation of essential health and safety requirements for machinery in the EU.[79] It aims at promoting free movement of machinery within the single market while guaranteeing a high level of protection for EU workers and citizens. The Machinery Directive has a "new approach" to regulation, providing a combination of mandatory health and safety requirements and voluntary harmonised standards. It is

[74] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance), *OJ L 11,* 15 January 2002.
[75] EC, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, 19 February 2020, COM(2020) 64 final, https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf, accessed 09 June 2021, p. 6.
[76] ibid.
[77] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) *OJ L* 157/24, 9 June 2006 (Machinery Directive), Annex 1.
[78] Regulation (EU) 2017/745 of the European Parliament and the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.
[79] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) *OJ L* 157/24, 9 June 2006 (Machinery Directive).

therefore relatively flexible to technological developments in the digital era.[80] The Machinery Directive **only applies to products that are to be placed on the European Economic Area (EEA) for the first time**.

The Machinery Directive was published on 9 June 2006 and came into force on 29 December 2009. It was amended by the Directive 2009/127/EC of the European Parliament and of the Council of 21 October 2009, with regard to machinery for pesticide application, and by the Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles, among others. The Machinery Directive is implemented by the national laws of the member states of the EEA, which include all members of the EU, and Norway, Iceland and Liechtenstein.

The Machinery Directive applies to machinery as well as interchangeable equipment, safety components, lifting accessories, chains, ropes, webbing, removable mechanical transmission devices and partly completed machinery.[81] Machinery is defined as[82]:

- An assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application,
- An assembly referred to in the first indent, missing only the components to connect it on site or to sources of energy and motion,
- An assembly referred to in the first and second indents, ready to be installed and able to function as it stands only if mounted on a means of transport, or installed in a building or a structure,
- Assemblies of machinery referred to in the first, second and third indents or partly completed machinery which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole,
- An assembly of linked parts or components, at least one of which moves and which are joined together, intended for lifting loads and whose only power source is directly applied human effort

Machinery that is covered by more specific legislation is excluded from the scope of application. This includes agricultural and forestry tractors[83], motor vehicles and their trailers[84] and certain electric and electronic products such as household appliances or office equipment.[85] As some other safety legislation within the EU, the Machinery Directive requires machinery to be labelled with a "CE

[80] EC, *Machinery*, https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence accessed 04 June 2021.
[81] Machinery Directive, Art. 1.
[82] Machinery Directive, Art. 2(a).
[83] Directive 2003/37/EC of the European Parliament and of the Council of 26 May 2003 on type-approval of agricultural or forestry tractors, their trailers and interchangeable towed machinery, together with their systems, components and separate technical units and repealing Directive 74/150/EEC, *OJ L* 171, 9 June 2003.
[84] See Council Directive 70/156/EEC of 6 February 1970 on the approximation of the laws of the Member States relating to the type-approval of motor vehicles and their trailers *OJ L* 42, 23 February 1970; Directive 2002/24/EC of the European Parliament and of the Council of 18 March 2002 relating to the type-approval of two or three-wheel motor vehicles and repealing Council Directive 92/61/EEC.
[85] Machinery Directive, Art. 1(2)(k).

conformity" marking before being placed on the market and put into service. The CE marking is the standard indicator in the EU which provides a declaration of the manufacturer that their product placed on the market conforms with the health and safety requirements. Manufacturers are responsible for ensuring that CE marking is affixed to the machinery in a visible, legible, and indelible form, health and safety requirements for machineries are fulfilled and appropriate procedures are put into place to ensure quality assessment.[86]

- As a preliminary analysis, the Machinery Directive seems to be applicable to the CoRoSect Project. The relevant health and safety requirements should be respected, and appropriate procedures should be put into place to ensure quality assessment.

3.1.2. Cybersecurity Act

Cybersecurity Act introduces a common cybersecurity certification framework for ICT products, services and processes within the EU.[87] It also strengthens the EU Agency for cybersecurity (ENISA), granting it a permanent mandate, and providing it with more resources and new tasks. ENISA will have a key role in setting up and maintaining the European cybersecurity certification framework, by preparing the technical ground for specific certification schemes. ENISA will also provide public information on the certification schemes and the issued certificates through a dedicated website.[88]

Increased digitisation and connectivity increase cybersecurity risks, thus making governments, businesses, and individuals more vulnerable to cyber threats. In order to mitigate those risks, the Cybersecurity Act aims to provide a comprehensive set of measures that can be implemented at the earliest stages of the design and development of the ICT products, services or processes. Potential cyber security risks should be reduced by design and development processes to ensure that the products, services and processes remain secure throughout their lifecycle. "Security-by-design" can ensure product safety and security, by anticipating and minimizing the impacts of potential cyber-attacks.[89] In addition, "security by default" should be ensured in the design and development of the ICT products, services and processes. It requires that the users receive a default configuration with the most secure settings possible.[90] Security by design and by default are two of the security objectives that the European Cybersecurity scheme aim to achieve.[91]

The cybersecurity certification framework will provide comprehensive set of rules, technical requirements, and standards under EU-wide certification schemes. ICT products and services that have been certified in accordance with the relevant scheme will be deemed to be compliant with the specified requirements.[92] The certificates will be recognised in all EU Member States, avoiding the risks arising from the fragmentation and barriers between different certification schemes at national

---

[86] Machinery Directive, Art. 5.
[87] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certificationand repealing Regulation (EU) No 526/2013 , PE/86/2018/REV/1, *OJ L* 151, 7 June 2019 (Cybersecurity Act).
[88] ibid., Art. 50.
[89] ibid., Recital 12.
[90] ibid., Recital 13.
[91] ibid., Art. 51(i).
[92] ibid., Art. 56(1).

level. The cybersecurity certification will be principally voluntary unless required by the EU law or the relevant national laws.[93] European Commission is mandated to regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme should be mandatory. The European Commission will carry out the first assessment by 31 December 2023, and the subsequent assessments in every two years.

On 26 March 2021, ENISA published the outcome of the public consultation on the first draft of the cybersecurity certification candidate EUCC scheme. If approved, the EUCC will serve as a successor to the existing ICT products certification schemes operating under the SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement).[94]

- There is currently no established cybersecurity scheme resulting from the Cybersecurity Act that is applicable to the CoRoSect. Although cybersecurity schemes will be adhered to on a voluntary basis, any relevant cybersecurity requirements should be fulfilled and any relevant measure addressing and mitigating the cybersecurity risks should be put in place.

3.2. Liability

The safety framework in the EU aims at preventing any harm or damages from occurring, however they may still occur despite the best efforts. In such cases, the liability regime comes into play to provide remedies (e.g., compensation) to those who suffer a harm to their physical integrity or property. The role of the concept of liability is twofold: on the one hand, it ensures that a person who has suffered harm or damage is entitled to claim and receive compensation from the party proven to be liable for that harm or damage, and on the other hand, it provides the economic incentives for natural and legal persons to avoid causing harm or damage in the first place or price into their behaviour the risk of having to pay compensation.[95] Liability framework complements the safety framework by requiring redressing any person for damages caused.

This sub-chapter outlines the concepts of civil liability, its connection with tort law and contract law, as well as the so-called strict liability and product liability. It aims to provide the applicable framework to constitute a basis for an in-dept legal analysis of the possible implications for the CoRoSect. It should be noted that EU law provides only a few mandatory rules regarding liability. The issues that are not addressed by the EU legal framework are dealt with national laws of each country, which can be divergent in their scope and application. This sub-chapter gives therefore reference to some national laws for explanatory purposes. For the purposes of this deliverable, this chapter only focuses on civil liability and not criminal liability.

[93] ibid., Art. 51.

[94] ENISA, *Public Consultation on the draft Candidate EUCC* Scheme, https://www.enisa.europa.eu/publications/enisa-report-public_consultation-on-the-draft-candidate-eucc-scheme, accessed 04 June 2021.

[95] EP, *Civil liability regime for artificial intelligence European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence,* 20 October 2020 (2020/2014(INL)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html, accessed 04 June 2021.

3.2.1. Civil Liability

Civil liability is a legal obligation that requires a party to pay for damages or to follow other court-enforcements in a lawsuit. For example, in case of a car accident, injured party may ask for compensation from the driver for the harm suffered. The aim of the civil liability is twofold: on the one hand, it ensures that victims of a damage caused by others get compensation and, on the other hand, it provides economic incentives for the liable party to avoid causing such damage. Civil liability rules aim at striking a balance between protecting public from harm while enabling businesses to innovate.[96]

A civil liability generally arises from either a contractual relationship or tort. The liable party is required to provide remedies to the victim, which may be in the form of compensation for monetary (e.g., hospital costs) or non-monetary damages (e.g., emotional distress). The injured party often bears the burden of proof to demonstrate that the liability of the injuring party is established. The burden of proof may shift to the liable person depending on the circumstances.

3.2.1.1. Contractual Liability

Contractual liability is a form of civil liability arising from a contract. A contract is a mutual agreement between two or more parties to establish or govern an economic relationship between them. Contractual parties generally enjoy a degree of freedom when agreeing the provisions of a contract. Mandatory rules of law may however stipulate minimum conditions or restrictions for the conclusion of contracts. A typical example of this is an employment contract, in which employee's interests are often balanced against the employer by the legal framework. Another example is a law that prohibits any provision in a consumer contract that excludes the liability of a producer. A contract is binding among the contracting parties, which means that the party breaching the terms of a contract may be forced by a legal action to execute the contract or provide remedies for non-compliance.

3.2.1.2. Tort Liability

Tort is a type of civil wrong that enable individuals the right to claim personal injuries inflicted by a wrongdoer. The tort law is based upon an ethical consideration of responsibility[97], which each individual has towards other individuals to protect the basic rights and interests of others. Liability arising from tort law differs from contract law in that the latter requires compliance with a specific duty arising from a predetermined obligation, whereas the first follows from a general duty to not to do harm to others. Tort liability obliges the person who intentionally or unintentionally commit a tortious act to provide monetary damages to the individual injured from such act. Although it found its place in both civil and common law jurisdictions, there is no common tort law framework in Europe. This means that the requirements to establish a tort liability may vary from country to country. The fundamental concepts of tort law are examined below.

3.2.1.2.1. Fault-based Liability

At the European level, there are no harmonized standards on tort law. The rules on the establishment of liability, basic concepts and standards of proof are determined under national laws of each country where the tortious act occurs. In civil law jurisdictions like France and Belgium, tort law is mainly based

---

[96] EC, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, 19 February 2020, COM(2020) 64 final, https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf, accessed 04 June 2021, p. 12.

[97] J. STEELE, *Tort Law: Text, Cases, and Materials*, Oxford University Press, 2014.

on fault. In order to establish a fault-based liability, the injured party need to prove the **damage** suffered by him or her, the **fault** of the wrongdoer and a **causal link between the fault and damage**[98].

Fault may arise either from commission of an act or omission to perform an act. Fault does not necessarily refer to an "intentional" act. The standard of "reasonable" or "prudent" person apply to determine whether a conduct corresponds to the conduct of, in the usage of traditional literature, "pater familias" under the same circumstances. In common law, on the other hand, the doctrine of "**duty of care**" is a fundamental concept to establish tort liability for any acts or negligence, which requires from the claimant to demonstrate that:

i. tortfeaser, i.e., the person who commits a tort, owed her a duty of care of some kind
ii. there is a breach of duty of care, and
iii. the claimant suffered a damage (e.g. physical or emotional injury, damage to property)

For instance, a customer can bring a claim against a shop owner who did not promptly take care of a spill that caused a customer to slip and injure herself. There are different tests apply by courts to determine whether a person has a duty to exercise care to another person. The Caparo test that is used by the courts until today applies the following criteria: "in addition to . . . **foreseeability of damage**, necessary ingredients in any situation giving rise to a duty of care are that there should exist between the party owing the duty and the party to whom it is owed a relationship characterised by the law as one of **'proximity' or 'neighbourhood'** and that the situation should be one in which the court considers it **fair, just and reasonable** that the duty of care."[99]

3.2.1.2.2. Strict liability

While the fault-based liability or duty of care is the principal basis for liability in many European countries, liability may be also justified without any fault on part of the "wrongdoer" in certain circumstances. Strict liability dates back to the early twentieth century when it has been increasingly recognized that the fault-based liability has proved inadequate to deal with some of the social and legal demands of the twentieth century. The major catalysis for this change was the rapid industrialisation which occurred in the nineteenth century, and the related hazards of an age of coal, steel, electricity and manufacturing of chemicals. This led to increased occurrence of accidental damage in which the prime factor was mechanical and anonymous. The victims of industrial accidents faced risk of not being compensated for grave injuries as they cannot demonstrate fault on the part of manufacturers. Against this backdrop, strict liability doctrine has increasingly found its place in national laws and courts cases, which does not require the proof of fault. The injured party is only required to demonstrate that she is injured by someone (e.g. child) or something (e.g. animal) that is under the custody of the liable person. Product liability is a typical example of strict liability, which is often separately regulated under European and national level.

---

[98] French Civil Code Art. 1382; Belgian Civil Code Art. 1382.
[99] N. MCBRIDE and R. BAGSHAW, *Tort Law*, Malaysia, Pearson Education, 2018, p. 84 and 87 quoting Lord Bridge of Harwich in Caparo Industries plc v Dickman [1990] 2 AC 605, 617-618.

3.2.1.2.3. Product Liability

The product liability framework introduces a system of strict liability of producers for damage caused by defects in their products, which constitutes an additional layer on top of the traditional fault-based liability.[100] Product liability ensures that **producer is liable if the product is defective, even if the defectiveness in the product does not result from any negligence of the producer.** Within the European Union, Product Liability Directive 85/374/EC[101] (Product Liability Directive) establishes the framework of the product liability regime. Product Liability Directive is implemented in all EU member states, and other EEA states (Iceland, Liechtenstein and Norway) and the United Kingdom through their own national legislation transposing binding requirements of the Product Liability Directive. It is applied in parallel to the fault-based liability (negligence) regime under the relevant national tort law because the latter allows the injured party to seek damages beyond the limitations and liability caps foreseen by the Product Liability Directive.

The European Product Liability regime sets out three core requirements for establishing liability on the part of the producer:

- a product defect,
- damage
- and a causal link between these two.

Product

Product Liability Directive defines the term product as "all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable. Primary agricultural products mean the products of the soil, of stock-farming and of fisheries, excluding products which have undergone initial processing. Product includes electricity.

A discussion relevant to the CoRoSect project concerns the question of whether software can be considered as a product under the Product Liability Directive. Software is essential to the functioning of a large number of products and may affect their safety. Software enables that the product to which it is integrated can be used for an intended purpose.[102] Therefore, a software that malfunctions can make a tangible product defective, leading to physical damage. A preliminary analysis arising from this interpretation leads to the conclusion that the Product Liability Directive is applicable to the CoRoSect.

[100] J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems", in J. DE BRUYNE and C. VANLEENHOVE, Artificial Intelligence and the Law, Mortsel, Intersentia, 2021, 376.
[101] Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, *OJ L* 210, 7 August 1985.
[102] EC, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, 19 February 2020, COM(2020) 64 final, https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf, accessed 04 June 2021.

Defect

The Product Liability Directive applies to any damage caused by a defect in the product. A product is deemed to be defective if it does not provide the safety that consumers generally are entitled to expect. EU law provides three specific circumstances to be taken into account when determining whether an end-user has a legitimate safety expectation: the presentation of the product, the use to which it could reasonably be expected that the product would be put and the time when the product was put into circulation.[103] The notion "legitimate" does not refer to any kind of personal expectation an individual might have. It refers to the expectations the public is entitled to have, which is a much more objective standard.

Damage

Producer shall be liable under the Product Liability Directive if a defect in her product caused a damage. Damage may be death or personal injury, as well as damage to property within the monetary determined limits. Directive's protection is limited to certain property, which[104]:

- is ordinarily intended for private use or consumption, and
- was used by the injured person mainly for his own private use or consumption.

Producer

If the injured party can demonstrate that the relevant damage is caused by the defective product, component part or raw material, she can seek compensation from their producer. "Producer" principally includes manufacturers of the product, component part or raw material. However, Art. 3 of the Product Liability Directive extends the definition of the producer to include:

- any person who, by putting his/her name, trademark or other distinguishing feature on the product, **presents himself/herself as the producer**,
- any **importer** which has imported the defective product, component or raw material into the European Union market; and
- any **supplier** (e.g. the retailer, distributor or a wholesaler) if the producer cannot be identified.

This means that, if the producer of the defective product or a defective component part or raw material is located outside the European Economic Area (EEA), an injured party can still bring action against the company based in EEA responsible for the harm inflicted.

[103] Product Liability Directive, Art. 6.
[104] Product Liability Directive, Art. 9.

- As a preliminary analysis, Product Liability Directive seems to be applicable to the CoRoSect's stakeholders because technologies concerning the CoRoSect project may be qualified as a product which can trigger the liability of their producer under the Product Liability Directive. However, it should be noted that the application of the EU product liability regime to new technologies is not always straightforward and requires further legal analysis. As the European Commission notes,"AI, the IoT and robotics are transforming the characteristics of many products and services." This is the consequence of some inherent characteristics of AI, such as self-learning abilities, opaqueness, autonomy, connectivity, data dependency which make it complicated, sometimes even impossible (so called "black-box"), to trace back problematic decisions made by AI system.[105] Another challenge is the allocation of liability between all actors involved. AI systems usually involve several parties such as software developers, producer of hardware, owner of the AI product, data suppliers, as well as the users of the product. The European Commission acknowledges the legal uncertainty in the application of Product Liability Directive by stating that "its scope could be further clarified to better reflect the complexity of emerging technologies and ensure that compensation is always available for damage caused by products that are defective because of software or other digital features. This would better enable economic actors, such as software developers, to assess whether they could be considered producers according to the Product Liability Directive".[106]

[105] J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems", in J. DE BRUYNE and C. VANLEENHOVE, *Artificial Intelligence and the Law,* Mortsel, Intersentia, 2021, 360.

[106] EC, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, 19 February 2020, COM(2020) 64 final, https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf, accessed 04 June 2021, p. 14.

4 Data Protection and privacy

The right to respect for private life (or the right to privacy) and the right to personal data protection are two closely related but distinct rights. The right to privacy emerged in the Universal Declaration of Human Rights (UDHR), which was adopted in 1948. Soon after, the European Convention on Human Rights (ECHR), adopted in 1950, provided that everyone has the right to respect for his or her private and family life, home and correspondence. Any public authority's interference to this right is prohibited, unless the interference is in accordance with the law, is necessary in a democratic society and pursues important and legitimate interests (such as, national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others).[107]

The UDHR as well as the ECHR were adopted before the rise of information society with which many risks to the right to privacy have arrived in individuals' lives. As a result of the efforts to mitigate these risks, regulations addressing personal data protection have developed. Data protection instruments were established at the European level since the 1970s during which some states in Europe started to adopt their own, related legislations. Over the years, data protection has developed into a distinct value which is not subsumed by the right to respect for privacy. The EU legal order recognises the data protection as a fundamental right, separate to the fundamental right to privacy.[108]

The right to privacy concerns the cases in which a private interest or the "private life" (or family life) of an individual has been compromised and this must be demonstrated by the right-owner. On the other hand, the right to personal data concerns situations in which personal data is processed, regardless of the relationship and impact on privacy. Therefore, the right to data protection is broader than the right to privacy. Processing of personal data may infringe privacy, but it is not necessary to demonstrate such an infringement for the rules on data protection to be triggered.[109]

Considering the above and the fact that data protection is an important ethical and legal issue in H2020 grant agreements, data protection, rather than privacy, will be at the core of legal and ethical requirements of the CoRoSect project, and so at the core of this deliverable.

4.1. Protection of personal data of human participants in research

Any research activity, which consists of the processing of personal data, must comply with the relevant ethical principles and with the applicable international, EU and Member State law.[110]

Art. 4 (1) of the General Data Protection Regulation (GDPR) of the EU defines "*personal data*" as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable*

[107]EU Agency for Fundamental Rights, *Handbook on European Data Protection Law*, Luxembourg, Publications Office of the European Union, 2018, p. 18.
[108] ibid., p. 18-19.
[109] ibid., p. 20.
[110] EC, *Horizon 2020 Programme Guidance – How to complete your ethics self-assessment*, 4 February 2019,https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf, accessed 04 June 2021, p. 19.

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".

Art. 9(1) GDPR prohibits the processing of special categories of data, which are the data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". The processing of these data can only take place where one of the exceptions listed under Art. 9(2) GDPR applies.

Personal data include location data, IP address, cookie ID, data held by a doctor/hospital, employee data and facial images, amongst other.[111]

As defined by Art. 4 (2) GDPR, "processing of personal data" means any operation or set of operations which is performed on personal data or on sets of personal data, either by automated means or manually, including:

- collection,
- recording,
- organisation, structuring, storage,
- adaptation or alteration,
- retrieval,
- consultation,
- use,
- disclosure by transmission, dissemination or otherwise making available,
- alignment or combination,
- restriction, erasure or destruction.

European Commission highlights in its H2020 Programme guidelines on ethics assessment that any action using personal data for research purposes normally qualifies as "processing", even when interviewees, human volunteers, patients are not actively involved in that research.[112]

In cases where AI robots are used -such as in the case of CoRoSect-, these AI robots, with the aim of performing and improving their functions, process vast amounts of data, often by covert means (e.g. sensors and cameras), threatening individuals' rights to respect for private life and to the protection of personal data (Art. 7 and 8 Charter of Fundamental Rights of the EU). Therefore, adherence to the GDPR's data protection and its requirements for data protection by design and by default are crucial. Considering that the accumulation of personal data makes such systems vulnerable to attacks and breaches, security concerns and their mitigation through technical and organisational measures are likewise relevant.

[111] ibid, p. 16.
[112] ibid., p. 16.

4.2. Processing of personal data in CoRoSect research

In order to achieve the research purpose, some consortium partners may be required to process personal data, particularly in the context of the pilot studies.

According to the proposal, personal data will be collected and processed within the project, and tracking or observation of participants and secondary use (use for any purpose other than the initial collection purpose) of the data collected will be the case. Processing of sensory data such as vision and speech is envisaged as well. This is also confirmed by the answers of some of the partners to the questionnaire prepared by the KU Leuven.[113]

However, it is unclear which data will be processed by which technologies and what kind of processing activities will be carried out. At this point, there are, amongst others, certain important questions:

- Will (vast amounts of) personal data be processed by covert means (e.g. sensors and cameras)?
- What level of human-robot collaboration is envisaged/planned to be achieved? Will the robots work in isolated environments on their own, or will those robots come in direct contact and interaction with human workers?
- If robots do directly interact with humans, will they be able process data such as these individuals' behaviours, voice, face or else?
- Will there be fully automated processing, or will human oversight be possible in the cycle of the system? (See below for further details on automated decision making)

Each time personal data is processed within the project, particularly during the pilots, the principles governing the processing of personal data under EU law -discussed in the following sections- must be assessed and implemented before and during the envisaged processing activities.

CoRoSect Consortium needs to observe the legal provisions, ethical principles and fundamental rights embedded in the regulatory framework at the EU level, including:

- The Charter of Fundamental Rights of the European Union (CFREU);
- The European Convention on Human Rights (ECHR);
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR);
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);
- Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014- 2020) and repealing Decision No 1982/2006/EC, especially its Rec. 29 and the Ethical Principles of Art. 19;
- Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 - the

[113] See Chapter I (Introduction).

Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006;

- The Opinions of the European Group on Ethics in Science and New Technologies (EGE), indicatively those included in the Opinion °24 - 17/12/2008 - Ethics of modern developments in agricultural technologies and the Report of the European Group on Ethics in Science and New Technologies on the Charter on Fundamental Rights related to technological innovation as requested by President Prodi on February 3, 2000;
- The Guidelines issued by the European Data Protection Board (EDPB) and its predecessor, Article 29 Working Party (WP29), including but not limited to Guidelines on Consent under Regulation 2016/679, Guidelines on Transparency under Regulation 2016/679, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679;
- The European Commission's "Ethics and Data Protection" in research settings (2018);
- Other recommendations related to ICT concerning data protection.

At the level of the Council of Europe, the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+) will also be taken into account. In addition, considering that the projected research activities of the Consortium involve the development and deployment of AI, the consortium will consider the Ethics Guidelines for Trustworthy AI, issued by the High-Level Expert Group on AI, and the European Commission's White Paper "On Artificial Intelligence - A European approach to excellence and trust", *also form a data protection point of view*. The Consortium will pay close attention to new developments in this area in order to provide the maximum level of privacy and data protection guarantees, introduce stakeholder training, raise relevant awareness and create a culture of trust and assurance around data.

As explained, it is currently unclear what personal data will be processed within the project. However, each time personal data is processed, all the procedures described in this deliverable need to be followed.

4.3. The General Data Protection Regulation (GDPR)

A particular attention must be paid to the EU General Data Protection Regulation ("GDPR"). This is the primary legal instrument of the European Union on data protection, adopted on in May 2016 with an aim of "making Europe fit for the digital age".[114]

As highlighted by the European Commission, "[t]he regulation is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. A single law will also do away with the current fragmentation in different national systems and unnecessary administrative burdens."[115]

The GDPR became fully applicable on 25 May 2018, when the EU Data Protection Directive was repealed. The directive was not directly applicable. Instead, it set out a goal that all EU Member States had to achieve by adopting their own laws. On the other hand, a regulation is binding legal act that

[114] EC, *Data Protection in the EU*, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en, accessed 04 June 2021.
[115] ibid.

"must be applied in its entirety across the EU".[116] Thus, since 25 May 2018, the data protection rules have been harmonized across the EU.

As stipulated in its Art. 1(1), the GDPR contains rules concerning the protection of natural persons. The second paragraph of the same article provides that the regulation seeks to protect fundamental rights and freedoms of natural persons and, more specifically, their right to the protection of personal data. Therefore, the GDPR does not deal with the rights and freedoms of legal persons (for example, companies).

4.3.1. Material Scope

Art. 2 of the GDPR regulates its "material scope", in other words, to which types of processing activities it applies. According to the first paragraph, the regulation is applicable in case of the processing completely or partly by automated means – for instance, a processing carried out with the use of computers containing digital databases. Furthermore, the GDPR also regulates the processing of personal data by any other means when these data are included in a filing system or are intended to be used in such a filing system. This means, the regulation also applies, for instance, in the case when personal data are manually processed and are contained or are to be contained in a filing system.

On the other hand, Art. 2(2) stipulates situations which are not covered by the GDPR. First of all, the GDPR does not regulate the processing that is carried out in the course of activities which are not subject to the EU law. Secondly, it will be the same in case of the processing of personal data by EU Member States when it concerns the activities performed within the framework of the common foreign and security policy. Thirdly, the GDPR is not applicable to the processing of personal data that natural persons carry out in the course of purely personal or household activities, for instance, correspondence and social networking. Lastly, the GDPR does not apply to the processing by competent authorities in the context of criminal justice.

- As noted, it is not completely clear at this stage what types of personal data will be processed within the CoRoSect framework. In any case, as it is confirmed by certain partners that sensors and cameras will be used to collect and process personal data, these activities will fall under the material scope of the GDPR.

4.3.2. Territorial Scope

With regards to the "territorial scope", which is regulated under the Art. 3 of the GDPR, the first paragraph stipulates that the regulation applies to the processing of personal data by the data controller or process who has an establishment in the EU. It does not matter whether the processing itself takes place in the EU or not.

Art. 3(2) regulates that, even in the cases where neither the data controller nor the processor has an establishment in the EU, the GDPR is applicable to the processing of personal data of individuals who are in the EU. Such processing activities must be related to the offering of goods or services (for a payment or for free) to these individuals, or to the monitoring of the behaviour of these persons as long as their behaviour takes place in the EU.

---

[116] EU, *Regulations, Directives and other acts*, https://europa.eu/european-union/law/legal-acts_en, accessed 04 June 2021.

Finally, according to the Art. 3(3), the GDPR applies to the processing of personal data by a controller not established in the Union, but in a place where an EU Member State law applies by virtue of public international law. This can be the case in consular posts or diplomatic missions of a Member State, as stated in the Recital 25 of the GDPR.

- There will be 5 pilots (executed in relevant environments provided by Nasekomo, Entomotech, Entocycle, Italian Cricket Farm, Invertapro) in 5 different countries (Bulgaria, Italy, Spain, the UK, Norway), amongst which there are EU member states. The behaviours of individuals, which will take place in these countries, will be monitored by sensors and cameras. Furthermore, most of the partners are established in the EU and they are supposed to be involved in processing activities (according to the responses to the questionnaire.) Thus, the processing activities will also fall under the scope of its territorial scope.

4.4. Principles applicable to the processing of personal data

The CoRoSect Consortium aims at conducting its research and testing in full compliance with the obligations posed by the EU data protection law – thus, by the GDPR. This section summarizes the key principles applicable to the processing of personal data under the GDPR.

The GDPR principles underlying the processing of personal data must be applied from the beginning to the end of the project, to ensure that all the ethical issues arisen by the processing activity taking place within the project are tackled properly.

Art. 5 GDPR stipulates that the processing of personal data must be compliant with the following principles:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- data accuracy;
- storage limitation;
- integrity and confidentiality.

Data Protection Principles

Principle of processing	***Importance for the CoRoSect***
Lawfulness (Art. 5(1)(a) GDPR)	The principle of lawfulness requires personal data to be processed only if and to the extent that the processing activity can be grounded on one of the legal bases listed under Art. 6 GDPR (or under Art. 9 GDPR in the case of special categories of data). As mentioned earlier, the processing of the special categories of data identified under Art. 9(1) GDPR is in principle prohibited, except where the lawful basis for processing is to be found in Art. 6 in combination with one of the exceptions

	listed under Art. 9(2) GDPR. However, processing of special categories of data is not envisaged within the CoRoSect project. Thus, any processing of personal data needs to be preceded by a careful and thorough assessment of the legal basis on which such processing can be grounded. The possible legal grounds which can be invoked within CoRoSect to process personal data are further discussed in deliverable 1.2.
Fairness (Art. 5(1)(a) GDPR)	As required by the principle of fairness, controllers must inform the data subjects that the processing will be performed in accordance with the principles of lawfulness and transparency. Furthermore, processing operations must not be performed in secret and the data subject must be informed about the possible risks that may be caused by the processing.[117]
Transparency (Art. 5(1)(a) GDPR)	According to the principle of transparency, the data subjects must be informed about how their data are processed and about their rights as data subjects. Such information must be given to the data subjects prior to the processing and must remain available and accessible to them in the course of the processing (including on the occasion of an access request).[118] This means, within CoRoSect, the participants/data subjects should be made aware of all the relevant information regarding the processing of their personal data in the context of the research. Information sheets and informed consent forms must ensure that data subjects are properly informed and that the research does not take place "in secret". In addition to the pilots, this principle should also be implemented and respected in the course of any activities related to the CoRoSect website.
Purpose limitation (Art. 5(1)(b) GDPR)	For each processing activity, there must be a specified, explicit and legitimate purpose, which must be determined prior to the processing. Any processing for undefined purposes, as well as any further processing that is incompatible with the original one, is unlawful. Art. 5(1)(b) GDPR introduces a presumption of compatibility, which is subject to the requirements under Art. 89 GDPR, for further processing for archiving purposes in the public

[117] EU Agency for Fundamental Rights, *Handbook on European Data Protection Law*, Luxembourg, Publications Office of the European Union, 2018, Section 3.1.2.
[118] ibid, p. 120.

	interest, scientific or historical research purposes or statistical purposes. The purpose of processing of personal data within the CoRoSect has been identified from the outset as a research purpose. The consortium partners are required to avoid the further processing for purposes that are not compatible with the purpose of conducting this scientific research.
Data minimisation (Art. 5(1) (c) GDPR)	The data minimisation principle requires to limit the processing of personal data, as long as these are adequate and relevant, to what is necessary in relation to the purposes for which they are processed. The CoRoSect Consortium should take the necessary measures to ensure only the strictly necessary data is collected and processed.
Data accuracy (Art. 5(1) (d) GDPR)	The data accuracy principle requires to ensure accuracy of the data collected and processed and, where necessary, keep it up to date. For this reason, every reasonable step must be taken to ensure that personal data that are inaccurate, for the purposes for which they are processed, are erased or rectified without delay. Thus, data need to be checked regularly and kept up to date in order to secure accuracy by the CoRoSect partners, while inaccurate data need to be erased or rectified without delay.
Storage limitation (Art. 5(1)(e) GDPR)	Where personal data is processed, it must be kept only as long as it is necessary for the project purposes to be achieved.
Data security (Art. 5(1)(f) GDPR)	A combination of technical and organizational measures, which must be appropriate to prevent the risk of unauthorized or unlawful processing and accidental loss, destruction or damage must be taken to achieve integrity and confidentiality of the data. The Consortium is required to ensure that state-of-the-art technical and organizational measures are implemented from the outset until the end of the project. According to art. 25 GDPR, the principles of data protection by design and by default also need to be implemented throughout the project. In line with these principles, measures on, among others, access-control shall be taken to prevent unauthorised persons from gaining access to data per se or data processing systems. In other words, it shall be ensured that persons authorised to access personal data and use data processing systems have access only to those data that they are authorised to access, and that personal data cannot be read, copied, altered or removed without authorisation during

	processing. Personal data will be pseudonymised and, where feasible, anonymised. The partners should also consider the possibility of processing the data on-premises, i.e. on servers accessible only locally to prevent any connection from outside. Overall, partners must ensure that personal data are kept securely (Art. 32 GDPR) and that publication does not breach confidentiality or anonymity
Accountability (Art. 5(2) GDPR)	According to the principle of accountability, controllers and processors are required to implement the technical and organizational measures to comply - and to be able to demonstrate compliance - with data processing obligations. This deliverable maps the legal and ethical framework contributes to help the Consortium fulfil the obligations deriving from the accountability principle. Thus, this (as well as next deliverable) can be regarded as an important step to demonstrate compliance with the legal and technical requirements set by the legislation. The Consortium must also consider promoting compliance with the accountability by adopting certain measures including: • records of processing activities • data protection by design and by default • a data protection impact assessment (DPIA) specifically for types of processing that are likely to result in a high risk to the rights and freedoms of the data subjects in accordance with the GDPR – for instance, in the case of automated decision-making.

When the research involves processing of personal data, H2020 ethics guidelines[119] requires providing certain information as follows,

a) Details of the technical and organisational measures to safeguard the rights of the research participants. – For instance: For organisations that must appoint a Data Protection Officer (DPO) under the GDPR: Involvement of the DPO and disclosure of the contact details to the research participants. For all other organisations: Details of the data protection policy for the project (i.e. project-specific, not general).
b) Details of the informed consent procedures.
c) Details of the security measures to prevent unauthorised access to personal data.

[119] EC, *Horizon 2020 Programme Guidance – How to complete your ethics self-assessment*, 4 February 2019, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf, accessed 04 June 2021, p. 17.

d) How all of the processed data is relevant and limited to the purposes of the project ('data minimisation' principle)
e) Details of the anonymisation /pseudonymisation techniques.
f) Justification of why research data will not be anonymised/ pseudonymised (if relevant).
g) Details of the data transfers (type of data transferred and country to which it is transferred – for both EU and non-EU countries)

Furthermore, H2020 ethics guidelines also requires, if relevant, informed consent forms and information sheets used to be provided/kept in the file.

Besides all the above, It is also important to consider that national laws can also play an important role in connection with the 5 pilots that will be carried out in 5 different countries. National legislations must be carefully assessed, in particular to identify the requirements under Art. 89(1) GDPR, which are applicable to the further processing of data for research purposes.

Data Protection Impact Assessment

The Consortium must perform a preliminary assessment of whether any of the activity envisaged under the project might require a Data Protection Impact Assessment (DPIA) as provided for under Art. 35 GDPR. The GDPR mandates that where a processing activity is likely to pose high risks to the rights and freedoms of natural persons, "the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data" (Art. 35(1) GDPR).

Under Art. 35 (3) GDPR, a DPIA is made necessary, in particular, where the processing entails

a) a systematic and extensive evaluation of personal aspects based on automated decision making, including profiling,
b) processing on a large scale of special categories of data or
c) a systematic monitoring of a publicly accessible area on a large scale.

As it will be explained further below, automated decision making may be the case within CoRoSect and in such a case, an impact assessment will be required to be carried out.

Where deemed necessary, and based on the input received by partners regarding the different types of data they aim to process and the related processing activities, a DPIA will be provided in line with Art. 35 GDPR. Where such need is confirmed, the performance of a DPIA will be subsumed under the responsibility of the Project Coordinator and the respective data controller, with possible additional guidance from KUL. In addition, where required, the members of the Consortium will appoint Data Protection Officers (DPOs) and make the contact details of the latter available to data subjects involved in the research. As the research activities of CoRoSect are currently envisaged, they do not fulfil the requirements for the assignment of a DPO. However, an assessment will be carried out prior to any processing activity in order to estimate whether this condition may be considered applicable in the future.

H2020 ethics guidelines[120] stipulates that when data processing "involve profiling, systematic monitoring of individuals or processing of large scale of special categories of data, intrusive methods of data processing (such as, tracking, surveillance, audio and video recording, geolocation tracking

[120] ibid., p. 18.

etc.) or any other data processing operation that may result in high risk to the rights and freedoms of the research participants", certain information shall be provided:

a) Details of the methods used for tracking, surveillance or observation of participants
b) Details of the methods used for profiling
c) Risk assessment for the data processing activities
d) How harm will be prevented, and the rights of the research participants safeguarded
e) Details on the procedures for informing the research participants about profiling, and its possible consequences and the protection measures

Furthermore, if relevant, an opinion of the data controller on the need for a data protection impact assessment (Art. 35 GDPR) shall also be provided/kept in the file.

4.5. Legal basis for the processing of personal data in CoRoSect

As required by the principle of lawfulness, an appropriate legal basis, under Art. 6 GDPR (and under Art. 9(2) GDPR in the case of special categories of data) must be identified prior to any personal data processing activity.

Before each processing activity, a **case-by-case assessment** of the most appropriate legal basis must be performed. The appropriate legal basis needs to be analysed for both the primary processing of personal data (when the partners collect data from participants and undertake any initial processing activity) and the secondary processing (processing of data for a purpose other than the one for which the data was initially collected).

Under Art. 6 (1) GDPR, the possible legal bases are

a) data subject's consent
b) performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
c) compliance with a legal obligation to which the controller is subject
d) vital interests of the data subject or of another natural person
e) performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
f) legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

As noted above, a case-by-case assessment should be done by the data controller prior to each processing activity.

4.5.1. Informed Consent

If data subjects' consent is the applicable legal basis for the CoRoSect project, that must be informed. In other words, consent can only be a legal ground if data subjects are properly informed about the processing activity and the risks that may involve.

This informed consent form, which will be provided by the relevant partners to the human participants, must take into consideration the following requirements:

- written in clear and plain language (in terms completely understandable to the participants)

- describing the aims, methods and implications of the research and the data processing activities envisaged within the research, and any benefits, risks or discomforts that might be involved
- explicitly stating that participation and being a subject to data processing is voluntary, and that everyone has the right to refuse to participate and to withdraw at any time without giving a reason and without any disadvantage.
- detailing the purpose of data processing and duration of retention
- detailing the legal rights of the participants to access, correct, block or delete their data
- specifying the personal data that will be collected, and to what degree (and how) confidentiality of such data will be ensured
- providing information to the participants concerning who will be in charge of storing the collected data and who will have access to those data.

It is important to note that, this informed consent is different from the one related to research ethics. This is explained in detail in relevant part under Part IV (Research Ethics).

4.6. Lawfulness of further processing for scientific research purposes

Under Art. 5(1)(b) GDPR which regulates the principle of purpose limitation, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. However, "presumption of compatibility", as aforementioned, is introduced by the same article for the further processing of personal data for scientific research purposes when such further processing is in compliance with Art. 89(1) GDPR.

The presumption of compatibility requires the adoption of appropriate technical and organizational measures aimed at ensuring data minimization (Art. 89(1) GDPR). It can be achieved, particularly, through measures such as pseudonymization, access limitation or even anonymization, in cases where the same purposes can be achieved with anonymised data.

On the condition that these technical and organizational measures are implemented, the processing of personal data for scientific research purposes can take place in derogation of certain data subject rights (access, rectification, restriction of processing, object), where the EU or Member State law allows for such derogations (Art. 89(2) GDPR). Hence, it is always imperative to also investigate the applicable national laws in the context of research.

However, the European Data Protection Supervisor (EDPS) has warned that the presumption of compatibility cannot be interpreted as a general authorisation for further processing of personal data for scientific purposes: "Each case must be considered on its own merits and circumstances. But in principle personal data collected in the commercial or healthcare context, for example, may be further

used for scientific research purposes, by the original or a new controller, if appropriate safeguards are in place".[121]

Regarding the principle of lawfulness (and the need to identify a specific legal basis prior to any processing activity), Recital 50 GDPR, which is non-binding yet advisory, states that in case of personal data being processed for secondary compatible purposes, "no legal basis separate from that which allowed the collection of the personal data is required. […] Further processing for […] scientific research purposes shall be considered to be compatible lawful processing operations". The recital seems to address both personal and special categories of data since it is not accompanied by prescriptive legal provisions in the GDPR.

Although the principles of purpose limitation and lawfulness seem to overlap, the EDPS argues that "in order to ensure respect for the rights of the data subject, the compatibility test under Art. 6(4) should still be considered prior to the re-use of data for the purposes of scientific research, particularly where the data was originally collected for very different purposes or outside the area of scientific research".[122]

Art. 6(4) provides that "Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law", the compatibility of the further processing must be assessed on the basis of:

a) the link between the initial purpose of collection and the secondary purpose;

b) the context of collection of the data, with a particular attention to the relationship between the data subject and the controller;

c) the nature of the personal data, in particular whether special categories of data or data related to criminal conviction or offences are processed;

d) the possible consequences of the further processing for data subjects;

e) the existence of appropriate safeguards such as pseudonymization or encryption.

Furthermore, where research partners would further process previously collected personal data, e.g., pre-existing data sets or sources, partners will follow the H2020 ethics guidelines[123]. In parallel with the above-mentioned GDPR provision, the partners shall be able to provide adequate information concerning

a) Details of the database used or of the source of the data
b) Details of the data processing operations
c) How the rights of the research participants will be safeguarded
d) How all of the processed data is relevant and limited to the purposes of the project ('data minimisation' principle)

---

[121] EDPS, *Preliminary Opinion on Data Protection and Scientific Research*, 6 January 2020, https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en, accessed 04 June 2021, Section 6.7.
[122] ibid.
[123] EC, *Horizon 2020 Programme Guidance – How to complete your ethics self-assessment*, 4 February 2019, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf, accessed 04 June 2021, p. 18.

e) Where relevant, why the research data will not be anonymised/pseudonymised

In addition, the following documents will be provided/kept on file:

a) a declaration wherein the lawful basis for the data processing is explicitly confirmed
b) if applicable, the permission by the owner/manager of the data sets
c) informed consent forms and information sheets where applicable

- Likewise, where the research would involve publicly available data, partners who make use of the data shall confirm that the data used in the project is publicly available and the information can be freely used for the CoRoSect. If applicable, permission by the owner or manager of the data sets shall be sought.

In light of all the above, national laws governing research activities will have to be analysed and applied, together with the provision referred above, to the specific case, particularly within the pilots.

4.7. Data Subjects Rights

The data subject, the natural person whose personal data is being collected and processed, is granted certain rights under the Chapter III of GDPR. These rights are important as they will result in certain obligations for data controllers and data processors. Data subjects have certain rights as listed below:

1) right to be informed about any processing of their personal data
2) right to access their own personal data and obtain information about the processing
3) right to the rectification of their personal data, so that these are accurate and up to date
4) right to the erasure of their personal data (right to be forgotten), under certain conditions
5) right to temporarily restrict the processing of their data
6) right to data portability, meaning to transfer their data from one controller to another, under certain conditions
7) right to object to the processing of their data, under certain conditions
8) right not to be subject to solely automated decision-making, under certain conditions along with other rights relevant to automated decision-making

The project must take the necessary measures to ensure data subjects to be able to practice their rights. Exemptions may apply in certain cases, as will be explained in the D1.2 Ethical and Legal Requirements Specification Report.

4.7.1. Automated Decision-Making

At this point, it is not completely clear whether the AI developed during the CoRoSect project and deployed within the pilots, with the cameras and sensors, will be capable of automated decision making or not. This depends on what technologies and algorithms will be used, and what level of human-robot collaboration is intended to be achieved by the partners and will be clarified in the course of the project. Thus, it is important to explain what legal framework will be applicable in case of automated decision making.

With regards to profiling and automated decision-making, the GDPR has introduced specific rules in its Art. 22, of which the first paragraph stipulates that data subject “shall have the right not to be subject to a decision based solely on automated processing, which produces legal effects concerning him or her”.

The Article 29 Working Party highlights that, this article states a general prohibition on fully automated decision-making.[124] However, the Art. 22(2) of the GDPR notes that, data controllers may be exempted from such prohibition only in three specific cases: when the decision is:

a) necessary for the performance of a contract between the data subject and the controller,
b) permitted by an EU or national law, or
c) based on explicit consent.

- Should automated decision-making be the case within CoRoSect, collecting explicit consent of human participants, whose personal data will be collected and processed by automated decision-making, will be needed.

Furthermore, as stipulated by Art. 22(3) of GDPR, it will be required to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

Although special categories of personal data are not envisaged within CoRoSect project according to its proposal, it is useful to note that according to Art. 22(4) of GDPR, automated decision-making cannot be used to process special categories of personal data referred to in Art. 9(1), unless point (a) or (g) of Art. 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

As explained before, automated decision making requires a data protection impact assessment to be carried out in line with Art. 35 GDPR and certain requirements listed in H2020 ethics guidelines, as referred before, apply.

4.7.2. Data Transfers

According to the Chapter V of the GDPR, when data transfers need to occur from the EU to the third countries, these shall be predicated on one of the following grounds:

- the explicit consent of the data subject (which requires them to be informed in advance of any such transfers);
- an "adequacy determination" by the European Commission (EC) in respect of the country in question;
- a data-transfer agreement containing EC standard contractual clauses giving effect to EU data protection law; or
- binding corporate rules covering both sender and recipient and approved by a national supervisory authority.

[124] Article 29 Working Party, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, 3 October 2017, p. 9.

- The CoRoSect consortium includes partners that are based in non-EU countries, namely Norway (Invertapro), Serbia (FSH) and the United Kingdom (Entocycle). Hence, any potential data processing activities involving these partners might include the transfer of personal data to these countries. In such a scenario, the following will apply:
  - Regarding Norway: Since the EU data protection rules apply to the European Economic Area (EEA) -which includes all EU countries and non-EU countries Iceland, Liechtenstein and Norway-, all data protection provisions apply directly to Norway, without any further measures required.
  - Regarding Serbia: As there has been no adequacy decision for Serbia, the Consortium needs to explore the use of the Standard Contractual Clauses issued by the European Commission to offer sufficient safeguards on data protection (i.e. Decision 2001/497/EC, Decision 2004/915/EC and Decision 2010/87/EU).
  - Regarding the United Kingdom (UK): The Brexit transition period, during which EU law continued to be applied in the UK, ended on 31 December 2020. Under the new trade deal, the EU has agreed to delay transfer restrictions for at least four months (ended at the end of April 2021), which is extended to six months (known as the bridge). The European Commission (EC) on 19 February 2021 published its draft decisions on the UK's adequacy under the EU's GDPR and Law Enforcement Directive (LED). In both cases, the UK is found to be adequate by the EC. The European Data Protection Board (EDPB) and a committee of the 27 EU Member States are now considering these draft decisions. If they are approved by the committee, then the EC can formally adopt them as legal adequacy decisions. If adequacy decisions are not adopted at the end of the bridge, transfers from the European Economic Area (EEA) to the UK will need to comply with Chapter V of the EU GDPR. Thus, in case of personal data transfer from the EEA to the UK, it is recommended to put alternative safeguards in place. To note, the bridge does not override the provisions of the Withdrawal Agreement, which applied as of 01 January 2021.[125]

When it is planned to export data from the EU to non-EU countries, H2020 ethics guidelines requires to provide information on:

a) details of the types of personal data to be exported,
b) how the rights of the research participants will be safeguarded

In addition, declaration that confirms compliance with Chapter V of the GDPR needs to be provided/kept in the file.[126] On the other hand, in case of a transfer from any of these countries to the EU, the applicable law in that country will apply. According to H2020 ethics guidelines, information on

[125] UK Information Commissioner's Office (ICO), *Data protection now the transition period has ended*, https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/, accessed 04 June 2021.
[126] EC, *Horizon 2020 Programme Guidance – How to complete your ethics self-assessment*, 4 February 2019,https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf, accessed 04 June 2021, p.19.

details of the types of personal data to be imported shall be provided, and declaration confirming compliance with the laws of the country in which the data was collected shall be provided/kept in the file.[127] In both cases (import and export), it is essential to specify the types of personal data and countries involved.

[127] ibid.

5 Research Ethics

As highlighted by the European Commission (EC), ethics is an integral part of all the research activities funded by the European Union, from the outset to the end, and ethical compliance is key to "achieve real research excellence". A thorough ethical evaluation from the conceptual stage of the research proposal is clearly needed, not only to fulfil the legal requirements but also to "enhance the quality of the research." To conduct ethically responsible research, relevant fundamental ethical principles and legislation concerning scientific research need to be applied. [128]

As a result of this high importance of research ethics, the ethical dimension of activities funded under Horizon 2020 is assessed and addressed by going through a process called the Ethics Appraisal Procedure. This procedure concerns all activities funded in Horizon 2020 and includes the Ethics Review Procedure, which is conducted before the start of the project, and the Ethics Checks and Audits.[129] The Ethics Review Procedure has been completed for the CoRoSect project prior to the start of the project but the Ethics Checks and Audits, which normally takes place during the ongoing project, is not required by the EC for this project.

As a part of the Ethics Review Procedure, an Ethics Self-assessment starting with the completion of an Ethics Issues Table has been done. "Horizon 2020 Programme – Guidance: How to complete your ethics self-assessment" by the EC provides practicalities needed to fulfil the necessary ethical compliance of the research. This very section of this deliverable is based on this guidance document as well as on the Ethics Issues Table in Part A and the Ethics Self-Assessment in Part B of the proposal of the CoRoSect project.

The issues listed in the Ethics Issues Table are as follows:

- Humans
    - The research involves human participants.
- Personal data
    - It involves personal data collection and/or processing.
        - It involves tracking or observation of participants.
        - It involves further processing of previously collected personal data (secondary use).
- Animals
    - It involves animals.
- Third countries
    - The research related activities undertaken in the non-EU countries that are involved raises potential ethics issues.
    - It is planned to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, etc.).
- Environment, health and safety

[128] EC, *Ethics* (*H2020 Online Manual)*, https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm, accessed 04 June 2021.
[129] ibid.

- It involves the use of elements that may cause harm to the environment, to animals or plants.
- It involves the use of elements that may cause harm to humans, including research staff.

As data protection and AI-related ethical issues are already covered in separate sections before, they are not assessed in this section again but instead, only the other, research-related ethical issues are dealt with here.

5.1. Involvement of Human Participants

Dealing with human participants in a Horizon 2020 research implies that the consortium must ensure respect for people and for human dignity and fair distribution of the benefits and burden of research, and that it must protect the values, rights and interests of the research participants. Moreover, it must obtain: the necessary ethics approvals (if required) and free and fully informed consent of the research participants.

As explained in the Ethics Self-Assessment in Part B of the proposal, the CoRoSect project will involve human participants in its research activities. Specifically, humans will participate in the testing of technologies developed and integrated through CoRoSect as mere users, meaning that no experiments will be conducted on them. This involvement is relevant and necessary to the data collection and the evaluation of the proposed pilots, given that the project seeks to create a robust human-robot collaborative environment. Therefore, it is imperative to test the technologies developed in real-life, operational settings. In doing so, CoRoSect will comply with the highest ethical standards to ensure that a good balance between the objectives of the research and means which the project partners employ to achieve these.

All human participants involved will be adults (over 18 years old), fully capable of understanding the project and their role in it. No children/minors, patients, vulnerable individuals or groups unable to give consent will be involved. Vulnerable individuals or groups are to be understood as those who are at a higher risk of harm or exploitation that others in a similar situation, or those who are less capable of protecting themselves from harms and exercising their rights to the fullest extent. The involved partners will appoint the specific users and pilot participants in connection with the purpose of the project.

The involvement of human participants will not amount to any invasive procedures or otherwise physical intervention processes. Human participants will only be observed in an overt manner, with due consideration to requirements of confidentiality and anonymity. In addition, partners will ensure that appropriate Health and Safety procedures will be followed in accordance with relevant local/national guidelines and legislation. Where robotic systems are engaged, human oversight and supervision will be ensured at all times, following a Human-In-The-Loop (HITL) approach.

According to H2020 research ethics guidelines[130], when a research involves human participants, ethical principles as well as applicable international, EU and national law must be complied with. This implies that it is required to ensure respect for people and for human **dignity** and fair distribution of the **benefits and burdens of research**, and to protect the **values**, **rights** and **interests** of the research participants. Moreover, the necessary ethics approvals (if required) and free and fully **informed consent** of the research participants must be obtained.

- The Ethical Self-Assessment noted, the CoRoSect project will adhere to ethical principles, and applicable international, EU and national law, satisfying all relevant compliance requirements for each specific activity. It will ensure respect for individuals and human dignity, fair distribution of burden and research benefits, while at the same time protecting the values, rights and interests of all research stakeholders.

5.1.1. Informed Consent

When human participants are involved in CoRoSect, their participation must be entirely voluntary, and their informed consent must be clearly documented in advance.[131]

According to the above mentioned H2020 research ethics guidance document[132], participants must be given an informed consent form and detailed information sheets:

- written in a language and in terms they can fully understand
- describing the aims, methods and implications of the research, the nature of the participation and any benefits, risks or discomfort that might ensue
- explicitly stating that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time — without any consequences
- stating how biological samples and data will be collected, protected during the project and either destroyed or reused subsequently
- stating what procedures will be implemented in the event of unexpected or incidental findings (in particular, whether the participants have the right to know, or not to know, about any such findings).

It must be ensured that potential participants have fully understood the information and do not feel pressured or coerced into giving consent.

---

[130] EC, *Horizon 2020 Programme Guidance – How to complete your ethics self-assessment*, 4 February 2019,https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf, accessed 04 June 2021, p.7-8.

[131] Consent is not required if national laws provide for an exception (e.g. in the public interest).

[132] EC, *Horizon 2020 Programme Guidance – How to complete your ethics self-assessment*, 4 February 2019,https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf, accessed 04 June 2021, p. 8.

As a principle, participants must give their consent in writing (by signing the informed consent form and information sheets) but if consent cannot be given in writing (such as in case of illiteracy) non-written consent must be formally documented and independently witnessed.

Informed consent is one of the pivotal principles in research ethics to ensure voluntary participation in research, and it also represents the most important procedure to address data protection and privacy issues in research.

It is important to clarify that there are **two different types of informed consent** relevant to this project:

i. informed consent as ethical standard in research
ii. informed consent as a principle of data protection

The existence of these two coexisting forms of consent, and their intertwined relationship, is often not completely clear nor straightforward. It is, however, important that both forms of consent are obtained in separate procedures. As also acknowledged by the recent EDPS Preliminary Opinion on data protection and scientific research[133], "there is some (understandable) confusion regarding consent, which is a principle of both data protection and research involving human participants".

- In certain types of research, for instance clinical trials for the testing of a pharmaceutical product, these two "layers" of consent are (more clearly) distinct. On the other hand, in a research where the involvement of human participants equates to the processing of personal data, consent as a principle of research ethics and consent as a principle of data protection tend to somehow overlap. Such an overlap is not envisaged in CoRoSect. However, this is not a final assessment and the technologies which will be developed and/or deployed throughout the project will be determinant.

As noted by the EC with regards to the involvement of human participants in a H2020 research[134], it must also be ensured that the research methodologies used do not result in discriminatory practices or unfair treatment.

The general principle is to **maximise benefits** and **minimise risks and/or harms**. In addition, when conducting surveys, interviews or focus groups where personal information is gathered and stored, it must also be paid attention to:

- Privacy
- Data protection
- Data management
- The health and safety of participants

[133] European Data Protection Supervisor (EDPS), *Preliminary Opinion on Data Protection and Scientific Research*, 6 January 2020, https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en, accessed 04 June 2021.
[134] ibid., p. 8- 9.

5.2. Involvement of Animals

According to H2020 research ethics guidelines[135], when the research involves animals, the following information must be provided,

1) Details of the species and rationale for their use, numbers of animals to be used, nature of the experiments, procedures and techniques to be used
2) Justification of animal use (including the kind of animals to be used) and why alternatives cannot be used

To fulfil these requirements, the Ethics Self-Assessment in Part B of the proposal notes that the use of animals, and specifically insects, is deemed necessary since the project aims at the automation of insect rearing. Specifically, within this project, insects will be detected, monitored and sorted based on certain traits (e.g. colour, diameter, movement) throughout their life stages (egg, larva, pupa, imago). Insects will be picked up, sorted and fed with a robotic arm, and they will be monitored through biosensors.

However, the animals involved fall under none of the following categories: vertebrates, non-human primates, genetically modified animals, cloned farm animals, endangered species. Specifically, the project will use black soldier flies (Hermetia illucens), mealworms (Tenebrio molitor) and crickets (Acheta Domesticus).

The EC guidance document[136] requires complying with ethical principles as well as applicable international, EU and national law (in particular, EU Directive 2010/63/EU, which is designed to limiting the use of animal testing for scientific purposes. It sets out EU-wide animal welfare standards –including authorisations, restrictions on the use of certain kinds of animals, standards for procedures, minimum requirements for personnel, recording and traceability, care and accommodation–. However, some EU members may have stricter national rules.

It also requires choosing alternatives to animal use where possible and implement the '**three Rs**' as guiding principles, i.e. the principles of **Replacement** (replacing animal use by an alternative method or testing strategy -without use of live animals-) – **Reduction** (reducing the number of animals used) – **Refinement** (improving the breeding, accommodation and care of animals and the methods used to minimise pain, suffering, distress or lasting harm to animals).

Furthermore, the necessary authorisations for the supply of animals and the animal experiments (and other specific authorisations, if applicable) must be obtained before the use of animals.

5.3. Involvement of third countries

In cases where:

- research activities are conducted, partially or wholly, in a non-EU country,
- participants or resources come from a non-EU country, or
- material is imported from or exported to a non-EU country,

[135] ibid., p. 22.
[136] ibid., p. 23.

the research, by not being a subject to the European rules and standards, may raise specific ethical issues (particularly in developing countries), such as:

- exploitation of research participants
- exploitation of local resources
- risks to researchers and staff
- research that is prohibited in the EU.[137]

In case non-EU countries are involved, if the research related activities undertaken in these countries raise potential ethics issues, the EC[138] requires providing information regarding,

- Risk-benefit analysis
- What activities are carried out in non-EU countries?

It also requires the following documents to be provided/kept in the file:

- Copies of ethics approvals and other authorisations or notifications (if required),
- Confirmation that the activity could have been legally carried out in an EU country (for instance, an opinion from an appropriate ethics structure in an EU country)

In cases where it is planned to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, etc.), the same guidance document also requires providing the details on what types of local resources will be used and how. As in this project, human resources will not be used but animals, plants, micro-organisms or associated traditional knowledge will be used, documentation demonstrating compliance with the UN Convention on Biological Diversity (e.g. access permit and benefit sharing agreement) is the document that must be provided/kept in the file[139].

The Ethics-Self Assessment notes, the Consortium involves members established in non-EU countries. These members have been selected for their established expertise in relation to insect farming and/or food matters. However, they will participate solely as end-users (Entocycle, Invertapro) or dissemination partners (FSH), which means that they will not carry out any research activities.

5.4. Use of elements that may cause harm to the environment, health and safety

Due to the experimental design of the research or any undesirable side-effect of the technologies used, the research may adversely affect environment, or health and/or safety of human participants of the research.[140]

[137] EC, *Horizon 2020 Programme Guidance – How to complete your ethics self-assessment*, 4 February 2019,https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf, accessed 04 June 2021, p. 25.
[138] ibid.
[139] ibid., p. 25-26.
[140] ibid., p. 29.

5.4.1. Environment

According to the EC guidance[141], when the research involves the use of elements that may cause harm to the environment, animals or plants, the below information must be provided:

- Risk-benefit analysis
- How the precautionary principle will be applied (if relevant)
- Details on what safety measures will be taken

The following documents also need to be provided/kept in the file:

- Safety classification of laboratory
- Copy of GMO and other authorisations (if required)

Furthermore, it is required to comply with ethical principles and applicable international, EU and national law. In particular,

- the precautionary principle (which requires that where there is plausible scientific evidence for serious risks, you must prove that a new technology will not harm the environment), and
- legislation on nature conservation and pollution control (including the EU Habitats Directive 92/43/EEC, the EU Wild Birds Directive 79/409/EEC, EU Regulation (EC) No 338/97 on protection of wild fauna, the EU GMO Directive 2009/41/EC and the Cartagena Protocol on Biosafety)

Therefore, the consortium is required to assess potential risks to the environment and avoid or minimise such risks. Moreover, it must obtain necessary environmental authorisations (if applicable).

5.4.2. Health and Safety

If the research involves elements that may cause harm to humans, including research staff, information on details of the health and safety procedures must be provided and a document regarding the safety classification of laboratory must be provided/kept in the file.[142]

- The Ethics Self-Assessment notes that the CoRoSect envisages the use of Automated Guided Vehicles (AGVs) to transfer crates/boxes from one place of the factory to another. As such, the Consortium acknowledges that the health and safety of humans on the premises shall be safeguarded. The Project Coordinator will take all measures to assure that appropriate environmental safety provisions are fulfilled in the course of the project; obtain the necessary health and safety authorisations, where applicable; and take all measures to assure for all partners, research subjects and unconcerned third parties that strict safety procedures are in place in compliance with national and EU regulations. One such measure will be to provide adequate guidance to employees. Overall, issues related to workplace safety will also be examined through the project's core research activities (for example under T6.4), considering that one of the project's objectives is directly linked to the creation of a safe and efficient human- robot collaborative environment.

[141] ibid., p. 29-30.
[142] ibid., p. 31.

5.5. Other ethics issues

As rightfully noted in the proposal, the introduction of robots into the workplace might significantly affect the labour market in the long run, by replacing and not just complementing human workers. The application domain of such AI-enabled automation is no less important: automating an industry whose goal is to 'feed the world's population while respecting future generations' needs and expectations in terms of food security, safety and sustainability' warrants particular ethical scrutiny.[143]

Having highlighted previously, the respect of ethical principles and legislation in scientific research is key to achieve research excellence. Thus, research carried out within CoRoSect, must satisfy the highest standards of **integrity** and avoiding research misconduct such as falsification and plagiarism. To this end, "The European Code of Conduct for Research Integrity"[144], which identifies and explains good research practices as well as conducts amounting to violations of research integrity, could be a helpful point of reference, among others, for the CoRoSect Consortium.

There is one last important point raised in the Ethical Self-Assessment in Part B of the proposal. As a project with an aim of creating an automated insect rearing farm, among CoRosect's underlying motivation is the promotion of insects as food and feed. Therefore, and although its research is not directly food-related, the Consortium should take into consideration the Guidance Note - Ethics and Food-Related Research[145]. It should particularly pay attention to the following issues examined therein: food security; sustainable food production and distribution; and legitimacy of publicly funded research/societal benefits.

[143] European Group on Ethics in Science and New Technologies to the European Commission, *Ethics of Modern Developments in Agricultural Technologies*, 17 December 2018, http://op.europa.eu/en/publication-detail/-/publication/9369a035-5a5e-45da-8e37-09717ed806d5/language-en/format-PDF, accessed 04 June 2021, p. 60.

[144] All European Academies (ALLEA), *The European Code of Conduct for Research Integrity*, 2017, https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf, accessed 04 June 2021.

[145] EC, *Guidance Note - Ethics and Food-Related Research*, https://ec.europa.eu/research/participants/data/ref/fp7/89847/research-food_en.pdf, accessed 04 June 2021.

6 Conclusion

This deliverable has provided an overview of the applicable legal and ethical legal framework in the context of CoRoSect technologies. It further mapped the policies, guidelines and recommendations stemming from the European Strategy on AI and identified those that are relevant for the project. It identified that, in the current state of AI governance, rules concerning AI mainly arise from soft law instruments, meaning that there is no binding legal text, like a law or a treaty. Nevertheless, these soft law recommendations are of great importance and have a significant impact in practice. A considerable part of the existing framework comprises of ethical principles and guidelines. Ethical principles, including human oversight, transparency and accountability should be fully respected in the design and development of AI-based technologies. However, this does not mean that there are not any binding legal rules applicable to the project. For instance, the existing legal framework on product safety and liability applies to the CoRoSect project, although the application of the relevant rules to specific technologies are not always clear due to the uncertainties and specificities involved in the AI-based technologies. In addition, European Commission's proposal regarding AI regulation, Artificial Intelligence Act, is a piece of potential legislation that provides guidance for the CoRoSect. Even though it is not finalized as a binding law yet, it provides an important source for the project as it shows the direction of law. In fact, it is crucial to take the legal developments into account in the design and development technologies so that they can comply with the relevant laws at the time of marketing.

Furthermore, EU data protection law provides a legal framework that fully applies to the CoRoSect. AI robots, with the aim of performing and improving their functions, process vast amounts of data, often by covert means (e.g. sensors and cameras), creating risks for the individuals' rights to respect for private life and to the protection of personal data (Art. 7 and 8 Charter of Fundamental Rights of the EU). Therefore, adherence to the GDPR's data protection and its requirements for data protection by design and by default are crucial. Considering that the accumulation of personal data makes such systems vulnerable to attacks and breaches, security concerns and their mitigation through technical and organisational measures are likewise relevant. Although it is not completely clear at this stage what types of personal data will be processed within the CoRoSect framework, a preliminary analysis has shown that personal data will be collected and processed through cameras and sensors. These activities will fall under the material scope of the GDPR. Any personal data should be processed in line with the principles outlined in this deliverable.

Last but not least, CoRoSect project should adhere to ethical principles, including human dignity, protection of health and environment and research integrity, satisfying all relevant compliance requirements for each specific activity. This is an integral part of all the research activities funded by the Eu, from the outset to the end, and a key to "achieve real research excellence".

References

Legislation

Belgian Civil Code

Declaration of cooperation on Artificial Intelligence of 10 April 2018, https://ec.europa.eu/jrc/communities/sites/default/files/2018aideclarationatdigitaldaydocxpdf.pdf

Directive 70/156/EEC of 6 February 1970 on the approximation of the laws of the Member States relating to the type-approval of motor vehicles and their trailers *OJ L* 42, 23 February 1970

Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, *OJ L* 210, 7 August 1985

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance), *OJ L 11,* 15 January 2002.

Directive 2002/24/EC of the European Parliament and of the Council of 18 March 2002 relating to the type-approval of two or three-wheel motor vehicles and repealing Council Directive 92/61/EEC

Directive 2003/37/EC of the European Parliament and of the Council of 26 May 2003 on type-approval of agricultural or forestry tractors, their trailers and interchangeable towed machinery, together with their systems, components and separate technical units and repealing Directive 74/150/EEC, *OJ L* 171, 9 June 2003

Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) *OJ L* 157/24, 9 June 2006

French Civil Code

Law 25 February 1991 'betreffende de aansprakelijkheid voor produkten met gebreken', B.S. 22 March 1991

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), *OJ L* 119, 4 May 2016

Regulation (EU) 2017/745 of the European Parliament and the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L* 303, 28 November 2018

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certificationand repealing Regulation (EU) No 526/2013, PE/86/2018/REV/1, *OJ L* 151, 7 June 2019

Policy Documents

All European Academies (ALLEA), *The European Code of Conduct for Research Integrity*, 2017, https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf

Article 29 Working Party, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, 3 October 2017

EC, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

EC, *Coordinated Plan on Artificial Intelligence of 7 December 2018* (Annex to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions), COM (2018), 795 final

EC, *Coordinated Plan on Artificial Intelligence 2021 Review of 21 April 2021* (Annexes to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence), COM (2021) 205 final

EC, *Ethics* (*H2020 Online Manual)*, https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm

EC, *Excellence and Trust in AI – Brochure*, 23 February 2021, https://ec.europa.eu/digital-single-market/en/news/excellence-and-trust-ai-brochure

EC, *Factsheet: Artificial Intelligence for Europe*, 25 April 2018, https://digital-strategy.ec.europa.eu/en/library/factsheet-artificial-intelligence-europe

EC, *Guidance Note - Ethics and Food-Related Research*, https://ec.europa.eu/research/participants/data/ref/fp7/89847/research-food_en.pdf

EC, *Horizon 2020 Programme Guidance – How to complete your ethics self-assessment*, 4 February 2019,https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

EC, *Pilot the Assessment List of the Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/futurium/en/ethics-guidelines-trustworthy-ai/register-piloting-process-0

EC, *Proposal of 21st April 2021 for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts*, COM (2021) 206 final, https://ec.europa.eu/newsroom/dae/redirection/document/75788

EC, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, 19 February 2020, COM (2020) 64 final, https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf

EC, *White Paper on Artificial Intelligence*, 19 February 2020, COM (2020) 65 final, commission-white-paper-artificial-intelligence-feb2020_en.pdf

EC, *White Paper on Artificial Intelligence: Public consultation towards a European approach for excellence and trust, Consultation Results*, 17 July 2020, https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence

European Group on Ethics in Science and New Technologies to the European Commission, Ethics of Modern Developments in Agricultural Technologies, 17 December 2018, http://op.europa.eu/en/publication-detail/-/publication/9369a035-5a5e-45da-8e37-09717ed806d5/language-en/format-PDF

EP, *Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)),* 16 February 2017, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html

EP, *Civil liability regime for artificial intelligence European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence,* (2020/2014(INL)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html

Expert Group on Liability and New Technologies (New Technologies Foundation), *Report on Liability for Artificial Intelligence and other emerging digital technologies*, 2019, https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608

HLEG AI, *Ethics Guidelines for Trustworthy AI,* 8 April 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

HLEG AI, *Policy and Investment Recommendations for Trustworthy Artificial Intelligence*, 26 June 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60343

HLEG AI, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, 17 July 2020, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342

HLEG AI, *Sectoral Considerations on Policy and Investment Recommendations for Trustworthy AI*, 23 July 2020, https://futurium.ec.europa.eu/sites/default/files/2020-07/Sectoral%20Considerations%20On%20The%20Policy%20And%20Investment%20Recommendations%20For%20Trustworthy%20Artificial%20Intelligence_0.pdf

UK Information Commissioner's Office, *Data protection now the transition period has ended*, https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/

Doctrine

DE BRUYNE, J. and VANLEENHOVE, C., *Artificial Intelligence and the Law*, Mortsel, Intersentia, 2021

MCBRIDE, N. and BAGSHAW, R., *Tort Law*, Malaysia, Pearson Education, 2018

NIXON, M., and AGUADO, A., *Feature Extraction and Image Processing for Computer Vision*, 2019, London (UK), Elsevier Science & Technology, 626

STEELE, J., *Tort Law: Text, Cases, and Materials*, Oxford University Press, 2014

TIELEMANS, J., A look at what's in the EU's newly proposed regulation on AI , Iapp, 2021, https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/

Other

BERTOLINI A., *Artificial Intelligence and Civil Liability,* European Parliament, July 2020, https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)621926

Deloitte Germany (Risk Advisory), *Artificial Intelligence Act*, May 2021, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Deloitte%20TAI%20DE%20-%20Artificial%20Intelligence%20Act.pdf

DHEU O., EU report on AI, new technologies and liability: key take-aways and limitations, 9 January 2020, https://www.law.kuleuven.be/citip/blog/eu-report-on-ai-new-technologies-and-liability-key-take-aways-and-limitations/

EC, *Call for a High-Level Expert Group on Artificial Intelligence*, 9 March 2018, https://digital-strategy.ec.europa.eu/en/news/call-high-level-expert-group-artificial-intelligence

EC, *Data Protection in the EU*, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

EC, *Machinery,* https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

EC, *Press Release Coordinated Plan on Artificial Intelligence 2021 Review*, 21 April 2021, https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

EC, *Strategy for Artificial Intelligence (updated),* https://digital-strategy.ec.europa.eu/en/policies/strategy-artificial-intelligence

EDPS*, Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary - Press Release*, 23 April 2021, https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en

EDPS, *Preliminary Opinion on Data Protection and Scientific Research*, 6 January 2020, https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en

ENISA, *Public Consultation on the draft Candidate EUCC* Scheme, https://www.enisa.europa.eu/publications/enisa-report-public_consultation-on-the-draft-candidate-eucc-scheme

EU Agency for Fundamental Rights, *Handbook on European Data Protection Law*, Luxembourg, Publications Office of the European Union, 2018

EU, *Regulations, Directives and other acts*, https://europa.eu/european-union/law/legal-acts_en

EVAS T., *A common EU approach to liability rules and insurance for connected and autonomous vehicles: European Added Value Assessment*, 2018, https://op.europa.eu/en/publication-detail/-/publication/df658667-20f1-11e8-ac73-01aa75ed71a1/language-en

IBM Cloud Education, *Artificial Intelligence (AI*), 3 June 2020, https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

NEVEJANS N., *European Civil Law Rules in Robotics*, October 2016, https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf

Register of Commission Expert Groups and Other Similar Entities, *Expert Group on liability and new technologies (E03592)*, https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3592

UN Sustainable Development Goals, https://sustainabledevelopment.un.org/?menu=1300

VAN DEN SPIEGEL, P. and BOGAERT, B., "EU strategic plan on Data and AI, The data strategy and the White Paper on AI unveiled", KPMG Insights, https://home.kpmg/be/en/home/insights/2020/02/ta-eu-strategic-plan-on-data-and-ai.html

CoRoSect

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101016953