D1.2. Ethical and Legal Requirements Specification 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
Work Package	Work Package 1
Delivery Date (DoA)	31 December 2021
Actual Delivery Date	23 December 2021
Abstract:	This deliverable specifies the ethical and legal risks posed in the context of CoRoSect's automated rearing platforms. It suggests mitigation measures to these risks, including by-design strategies. Such strategies mainly relate to data protection, safety and security by design guidelines, given that robots process and generate personal and non-personal data, which might be vulnerable to breaches.

Document Revision History			
Date	**Version**	**Author/Contributor/ Reviewer**	**Summary of main changes**
20/08/2021	0.1	Ana Maria Corrêa Harcus	Table of content
27/08/2021	0.2	Ana Maria Corrêa Harcus	Initial Input
21/10/2021	0.3	Ana Maria Corrêa Harcus	Chapter 2
15/11/2021	0.4	Ana Maria Corrêa Harcus	Input Chapter 3
19/11/2021	0.5	Burcu Yasar	Input Chapter 4 and 5
29/11/2021	0.6	Ana Maria Corrêa Harcus	Review
30/11/2021	0.7	Burcu Yasar	Amendments
06/12/2021	0.8	Anton Vedder	Review
07/12/2021	0.9	Burcu Yasar	Amendments
09/12/2021	1.0	Ana Maria Corrêa Harcus	Review & Amendments
15/12/2021	1.1	Rebeca Ramos Bueno	Quality Review
16/12/2021	1.2	Rico Möckel	Review
20/12/2021	1.3	Ana Maria Corrêa Harcus	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

LEGAL NOTICE

Table of Contents

List of tables

List of figures

List of Abbreviations and Acronyms	
AI	Artificial Intelligence
ALTAI	Assessment List on Trustworthy Artificial Intelligence
Art.	Article
Art29WP	Article 29 Working Party
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
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EP	European Parliament
EU	European Union
GDPR	General Data Protection Regulation
HIC	Human-in-Command
HITL	Human-in-the-Loop
HLEG AI	High-Level Expert Group on Artificial Intelligence
HOTL	Human-on-the-Loop
ICO	UK Information Commissioner's Office
WP	Work Package

Executive Summary

Cognitive Robotic System for Digitalized and Networked (Automated) Insect Farms (CoRoSect) promotes research, innovation and robotization of the mass rearing in insect farms in order to optimize and scale insects as a relevant edible resource. The consortium aims to create cognitive robotic ecosystems that will replace humans cognitively and physically during the insects' lifecycle. Considering CoRoSect's system involves human-robot collaboration schemes, and sophisticated AI-based cognitive perception capabilities, several legal and ethical issues are at stake. This report analyses the ethical and legal requirements concerning the CoRoSect automated rearing platform and suggests mitigation measures to comply with these requirements in the areas of AI, security, food and feed safety, animal welfare and data protection.

1 Introduction

CoRoSect aims to address food safety by developing sustainable solutions related to insect farming. Given that edible insects are valuable resources for farming animals, scaling their production and decreasing costs are necessary means to promote sustainable food supply in the following decades in the EU. In this sense, CoRoSect fosters research, innovation and robotization of mass rearing in insect farms in order to optimize and scale insects as a relevant edible resource. The consortium is currently gathering technical efforts to create cognitive robotic ecosystems that will replace human cognitively, physically and repetitive tasks during the insects' lifecycle, including the transferring and handling of crates, monitoring of environmental conditions, larvae separation and detection, and insect feeding. Such a robotic ecosystem will be experimentally implemented in five insect farms in five European countries. The general goal of the consortium is to develop a collaborative environment between humans and robots in different manipulation tasks.

Given CoRoSect's system is consisted of human-robot collaboration schemes and sophisticated AI-based cognitive perception capabilities, which process large amounts of data, several legal, ethical, privacy and security issues are at stake during all the stages of the project. In this context, KUL is expected to provide expertise on ethical, privacy and data protection matters involving the development and implementation of CoRoSect's cognitive robotic ecosystems. In the **D1.1 Ethical and Legal Framework: Initial Assessment Report**, KU Leuven Centre for IT and IP Law (CiTiP) covered a wide spectrum of legal domains that may apply to the project. The first deliverable broadly presented issues related to liability, artificial intelligence (AI), safety, privacy, data protection, and ethics concerning human participants and research on insects. In general, the **D1.1 Ethical and Legal Framework: Initial Assessment Report** shed light on the AI governance, the legal framework on safety and liability, and data protection and privacy rules in the EU.

In this second report (**D1.2 Ethical and Legal Requirements Specification Report**), the authors further analyse the ethical and legal requirements concerning the CoRoSect automated rearing platform, in addition to addressing mitigation measures regarding AI, security, food and feed safety and data protection risks. Realising trustworthy AI involves the respect and promotion of moral principles such as human autonomy, prevention of harm, fairness and explicability. In this sense, realising trustworthy AI depends on the application of rules and principles and implementation of technical and non-technical methods to the entire life cycle of AI systems, which include developers, deployers, end-users and broader society. As the CoRoSect technologies will be deployed in insect farms, the creation of ethically and legally compliant AI will also help to ensure that the food and feed can be produced in safe and hygienic conditions. The existing rules on food and feed safety and animal welfare rules will therefore be explored to guide the development of emerging technologies.

The second chapter of this deliverable focuses on the challenges involved in the development and use of AI systems in the workplace environment in insect farms and suggests mitigation measures to address these challenges. The third chapter further specifies the safety and security challenges and recommends AI developers measures to safeguard the security of the system. The fourth chapter provides the applicable safety and hygiene requirements for food and feed, and animal welfare standards recommended by the industry for the insect farm operations. It suggests organisational measures to ensure compliance with good hygiene practices. The fifth chapter specifies the EU data protection principles and rules, providing guidance to implement data protection by-design measures in the development and use of CoRoSect technologies.

2 CoRoSect's AI-Enabled Solutions: Ethical Issues

Robots and AI already have significant impacts on the development of the social, economic and legal fabrics. If there is a novel movement from policy-makers to create a binding framework to promote trustworthy AI in the EU, reflections around the ethics and safety issues posed by automated systems, robots, and AI have occupied the minds of scholars and philosophers for a much longer period of time[1]. Ethical and safety issues regarding AI are vast. Robots poorly trained or lacking robust technical elements may put the privacy and personal data protection of individuals at stake, in addition to being manipulative and biased. Human-robot collaboration may include safety risks to individuals' physical and mental integrity. Not to mention the economic dimension with social implications of replacing workers with automated, self-learning, autonomous machines.

AI brings great opportunities to economic and sustainable developments. An ethical governance is necessary, however, to ensure the entire society benefits from it. Such governance is relevant to establish a framework with ethical principles that will bind the whole AI production chain. The EU has opted to address digital technologies with the compromise to promote ethical principles, fundamental rights as well as to support the functioning of the common market. Considering data does not stop at member states borders, a single governance framework tends to better harmonise the digital single market. Having this in mind, this chapter highlights the EU governance approach to AI, the ethical and safety risks posed by the technologies developed by the consortium and mitigation measures to such risks.

2.1 EU Approach to AI

The EU approach to AI aims to ensure that AI-based technologies are in compliance with ethical principles, fundamental rights, rules that guarantee the functioning of the common market and individuals' safety. In the EU, AI shall be lawful, robust and **ethical**[2]. Lawfulness refers to the requirement of complying with applicable laws and regulations. In the EU, the regulation of AI includes an emerging regulatory framework oriented by the deliverables of the HLEG AI and existent rules on data protection and safety requirements[3]. Robustness relates to the technical reliability of the AI system, which might provide optimal performance and avoid at all costs vulnerabilities that might result in malfunction in specific conditions[4]. In opposition to optimal performance, an AI system poorly performs when it cannot operate well in a context that is considered normal by humans. Ethics regards the need to adhere to ethical values and principles, including the respect for human autonomy, prevention of harm, fairness and explicability. Tensions between these principles may exist in the context of trustworthy AI.

EU policies aspire to provide a governance framework favourable to the development of **human-centric AI**. By and large, human-centric AI empowers rather than replaces humans. This means that AI systems must be able to offer an understandable explanation to the way it decides, must be open to

[1] Patrick Lin, Keith Abney, George A. Bekey, *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press, 2014); Michael Anderson, *Machine Ethics* (CUP, 2011).

[2] HLEG AI, Ethics Guidelines for Trustworthy AI, 8 April 2019, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419> accessed 19 November 2021.

[3] To cite a few: 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; 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 and the Artificial Intelligence Act (proposal).

[4] Ronan Hamon, Henrik Junklewitz and Jose Ignacio Sanchez Martin, *Robustness and Explainability of Artificial Intelligence*, (Publications Office of the European Union, 2020).

taking advice from humans and must have compatibility with ethical and moral values that are expected from other social agents. Essentially, human-centric AI differs from data-centric AI in one main aspect: the latter makes decisions based on big data models that are not understandable by non-experts but also by the developers of the system[5]. Pure data-centric AI is no longer a conceivable model for EU policymakers. Given the EU ambitions to create an ethical-aligned environment to AI, the European Commission has created a comprehensive strategy that encompasses policy option for AI regulations[6]. Further details on how the EU AI strategy has been developed since 2018 are available on **D1.1 Ethical and Legal Framework: Initial Assessment Report**.

In the European Union, the Ethics Guidelines for Trustworthy AI provide an ethical framework to be complied with by developers, deployers and end-users of AI systems[7]. The document was published with the contribution of the independent expert group, appointed by the European Commission (HLEG AI), and with the input of more than 500 interested stakeholders in the private and public sector. The Guidelines acknowledge that AI systems must adhere to the ethical principles of respect for human autonomy, prevention of harm, fairness and explicability. Particular attention should be given to contexts involving venerable groups, including children, persons with disabilities and others that have been disadvantaged or at risk of exclusion. Several mitigation measures to attenuate risks to human autonomy, harm and opacity are provided by the Guidelines and further explored in this deliverable in the section 2.4.

More recently, aligned with the compromise to create a legal framework for AI that is grounded on ethical principles, fundamental rights and safety, the European Commission released, in April 2021, a proposal for an Artificial Intelligence Act[8]. The proposal includes a robust and flexible harmonised set of rules for the EU that may be directly applicable to all Member States. In precise terms, the proposal pursues to address the "opacity, complexity, bias, a certain degree of unpredictability and partially autonomous behaviour of certain AI systems, to ensure their compatibility with fundamental rights and facilitate the enforcement of legal rules"[9].

Furthermore, in the EU, the GDPR contains several provisions that are relevant to regulate the development of AI systems. The rules related to the protection of personal data are relevant to the extent to which AI systems are trained upon personal and non-personal data. Chapter 5 will provide more details on how the consortium shall comply with the regulation. The Directives on Machinery and General Product Safety are also relevant to AI developments, given some AI systems offer safety risks to individuals they interact with[10]. If enacted, the machinery regulation proposal is also likely to

[5] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Building Trust in Human-Centric Artificial Intelligence Brussels, 8.4.2019 COM(2019) 168 final.

[6] 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: Artificial Intelligence for Europe Brussels, 25.4.2018 COM (2018) 237 final.

[7] 'Ethics Guidelines for Trustworthy AI', see note 2.

[8] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act - Proposal) and Amending Certain Union Legislative Acts COM/2021/206 Final. Hereinafter, Artificial Intelligence Act.

[9] Reasons for and Objectives of the Proposal, Artificial Intelligence Act.

[10] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending directive 95/16/EC and Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4).

affect AI systems developed and deployed by CoRoSect. This proposal definition of AI is aligned with the one in the Artificial Intelligence Act proposal[11].

Despite the existence of disputes among scholars and experts around the concept of AI and its essential elements, AI can be initially defined as software systems that can create content, predictions, recommendations or even decisions that somehow impact the environment they interact with[12]. This software system may encompass: (1) machine learning with supervised, unsupervised and reinforcement learning using several methods of deep learning; (2) logic and knowledge-based techniques, such as knowledge representation, inductive programming, knowledge bases, inference and deductive engines, reasoning and expert systems; (3) statistical approaches, Bayesian estimation, search and optimization systems[13]. This definition is not legally binding, considering the Artificial Intelligent Act proposal has not been enacted yet. However, this proposal shed some light on the way the EU will likely regulate AI in the near future. In addition, the list of techniques used for AI developments will be susceptible to updates by the adoption of delegated acts with the goal to follow recent technological developments available to the market[14]. Ultimately, the scope of application will likely include providers, users, importers and distributers of AI systems inside the EU.

2.2 Ethical Considerations

The achievement of trustworthy AI depends on the alignment with ethical norms. Ethical norms are especially important when statutory law is not adapted to technological developments. This may happen when there is no political will or capacity to legislate at the same fast pace of technological developments. In this case, ethical principles should be mobilized.

The High-Level Expert Group on Artificial Intelligence, appointed by the European Commission, with the contribution of private and public stakeholders created an AI ethical framework to govern AI technologies in the European Union[15]. This ethical framework is present in the following four documents: Ethics Guidelines for Trustworthy AI; Policy and Investment Recommendations for Trustworthy AI; Final Assessment List for Trustworthy AI (ALTAI); Sectoral Considerations on the Policy and Investment Recommendations. In particular, the Ethics Guidelines for Trustworthy AI highlight that trustworthy AI is grounded on four ethical principles, namely the **respect of human autonomy**, **prevention of harm**, **fairness** and **explicability**. An extensive explanation on each of these principles is developed in **D1.1 Ethical and Legal Framework: Initial Assessment Report.** In the present D1.2, a summary of these principles is provided in the following sections. Moreover, mitigation measures are developed in 2.4.

2.2.1 Principle of Human Autonomy

The moral principle of human autonomy relates to the individual's capacity for self-determination or self-governance. This capacity to make deliberate choices instead of merely being subjected by the interests of others is a cornerstone of liberal societies. AI systems that directly or indirectly interact

[11] Proposal for a Regulation of the European Parliament and of the Council on Machinery Products COM/2021/202 final; and Recital 63, Artificial Intelligence Act (proposal).
[12] Jan de Bruyne and Cedric Valeenhove, *Artificial Intelligence and the Law* (Intersentia, 2021); Art. 71, Artificial Intelligence Act (proposal).
[13] Annex I. Brussels, 21.04.2021 COM(2021) 206 final Annexes 1 to 9 to the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.
[14] Recital 6, Artificial Intelligence Act (proposal).
[15] *See* European Commission, High-level Expert Group on Artificial Intelligence, <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai> accessed 1 September 2021.

with human beings should respect the principle of human autonomy by preserving individuals' self-determination. In this sense, the AI Ethics Guidelines highlight that AI systems should not 'subordinate, coerce, deceive, manipulate, condition or herd humans'[16]. AI systems are human-centric when they empower human capacities by enhancing individual possibilities of choice. AI systems should be designed to respect this freedom of choice and human autonomy.

2.2.2 Principle of Prevention of Harm

The principle of prevention of harm includes the dimensions of human dignity, mental and physical integrity[17]. AI systems should be designed in order to not cause any harm to these three aspects of the human existence. The European Union has historically established governance frameworks focused on the prevention of harm or damage. In this regard, for instance, the precautionary principle has been mobilized to ensure human health, among other things, in decision-taking involving risks[18]. Similar to the precautionary principle, the values related to the prevention of harm aim at preserving human dignity and integrity and should be invoked when a phenomenon, product or process may cause a harmful impact to human beings. The assessment of potential harm does not need to be determined with total certainty in order to motivate changes in the design of an AI system. Particular emphasis to the principle of prevention of harm should be given in contexts in which there is asymmetry of power or information. Such contexts include the relationship of employers and employees, companies and consumers, and government and citizens.

2.2.3 Principle of Fairness

Trustworthy AI systems must comply with the moral principle of fairness. The moral principle of fairness is complex and embraced by distinct philosophical theories. In this deliverable, the author's purpose is not to explore the principle of fairness in the light of distinct theories. Controversies related to this moral principle will not be explored. Instead, fairness is presented according to the understanding of the High-Level Expert Group on Artificial Intelligence.

In brief words, fairness encompasses substantial and procedural aspects. Procedural fairness relates to the decision-making process. Fair procedures have: (1) independent criteria to determine what constitutes a fair outcome of a certain decision-making process; (2) steps that ensure a fair outcome will result from the decision-making[19]. In AI systems, procedural fairness is ensured when there is a possibility to call into question an AI decision and, more importantly, to have effective remedies against it. In this sense, procedural fairness requires that AI decisions are identifiable and explicable.

Substantial fairness relates to the content of the AI decision-making. It does not relate to the process of the decision-making itself, but with its outcome. AI systems must promote to the extent of their possibilities substantial fairness. Promoting substantial fairness translates into safeguarding just distribution of costs and benefits, treatment free of discriminatory bias, equal opportunities, avoidance of stigmatisation of historical vulnerable groups.

2.2.4 Principle of Explicability

Trustworthy AI systems are able to provide explanations regarding their decision-making. In practical terms, the principle of explicability requires from AI systems the capability to explain why they have created a certain output or even the reasons why they have decided in a certain way. The principle of

[16] 'Ethics Guidelines for Trustworthy AI', see note 2, p. 12.
[17] I*bid.*
[18] Communication (COM(2000) 1final) on the precautionary principle <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0001&from=EN>.
[19] J Rawls, *A Theory of Justice: Revised Edition* (Harvard University Press, 1999).

explicability partially ensures procedural fairness, considering it provides transparency to the AI decision-making process. In cases explicability is not technically viable, AI developers should at least ensure that their automated decision-making has traceability and is auditable. These extra safeguards aim to provide more transparency to AI systems.

These four ethical principles (**respect of human autonomy**, **prevention of harm**, **fairness** and **explicability)** unfold into the core requirements to the practical implementation of trustworthy AI, which are summarized in table 1 below.

Human agency and oversight
Technical robustness and safety
Privacy and data governance
Transparency
Diversity, non-discrimination and fairness
Societal and environmental wellbeing
Accountability

Table 1 Requirements for the implementation of trustworthy AI

Each of these requirements has the same level hierarchy and must be fairly balanced depending the practical case they apply on. These requirements are extensively developed in **D1.1 Ethical and Legal Framework: Initial Assessment Report.** It is worth noting that these seven requirements shall be addressed during the AI system's life cycles via technical and non-technical methods which are further developed in section 2.4 below. Ultimately, an entire life cycle of AI systems encompasses developers, deployers, end-users and broader society[20].

2.3 CoRoSect's AI-Enabled Solutions: An Overview

CoRoSect develops several types of technologies that fit into the concept of AI provided by the European Commission proposal for an Artificial Intelligence Act and by several legal scholars[21]. CoRoSect will create technologies equipped with vision-based systems and arms that handle crates, material for insect rearing and insects. In particular, robots will be integrated with machine vision in order to identify relevant objects and insects. In addition, robots will be trained with sound recognition to identify cricket sound waves. Robots will autonomously move on the shop floor and stop when they encounter obstacles. Robots will be trained by data collected from human workers in order to operate autonomously in the farms.

CoRoSect's AI developments are dependent on data. In addition, they include robots that behave autonomously and complex decision-making processes that are, at first sight, opaque to a layperson. These sets of characteristics may potentially affect the safety of humans involved in CoRoSect's operations and their fundamental rights provided in the EU Charter of Fundamental Rights. Requirements for trustworthy AI aims at mitigating these negative impacts in the entire AI's system life cycle. In particular, the protection of human dignity, respect for private life and protection of personal data, non-discrimination, workers' rights to fair and just working conditions and a high-level

[20] 'Ethics Guidelines for Trustworthy AI', see note 2.
[21] Jan de Bruyne and Cedric Valeenhove, Artificial *Intelligence and the Law*, see note 12.

of consumer protection must be safeguarded[22]. In order to ensure that safety and fundamental rights are promoted and protected, the fundamental value concerning the freedom to conduct business, also enshrined in the Charter, is submitted to restrictions[23]. These restrictions translate into the obligation imposed on AI developers to guarantee that their system is built on high-quality data, besides the duties related to documentation and traceability, transparency, human oversight, accuracy and robustness. These requirements are expected to apply to high-risk AI systems.

This section provides, first, an overview of AI-enabled technologies to be developed by CoRoSect that are relevant to this deliverable. Second, the legal, safety and ethical risks involving such technologies. Third, mitigation measures to such risks.

2.3.1 Farm-level Modelling and Workflow Orchestration

CoRoSect aims at improving the workflows in the farms to an optimal level. The optimization of the workflows will take into consideration processes encompassing robotic components and human workers. Modelling robotic and human activities involve the integration of data generated by sensors and robots, such as the crate temperature and camera recording, and data provided by human workers. In WP4, T4.3, the consortium highlights that the integration of robotic and human data is necessary to the creation of an intelligent and optimal workflow in the farm environment. Ultimately, the modelling system to be created by CoRoSect will guarantee that robots, sensors and other AI tools are properly interconnected and cooperating.

The creation of an intelligent farm orchestration involves legal, safety and ethical risks related to (1) the training of robotic activities by the integration of human data, (2) vulnerabilities of the system to external attacks, (3) collection of data from workers and (4) camera recording.

In this context, the quality of data matters to the mitigation of risks involving the AI system at stake. Errors in the data used to train the robots or unstructured data might undermine the reliability of the farm workflow and the safety of workers. Considering machine learning cannot fully grasp the context of the chores it performs, the system might count on high quality data during its training to safely operate in the farm. In addition, given robots rely on human-provided training data to operate, human bias may be involuntarily embedded into the system. Diversity and inclusion must be taken into account in the initial training data. Moreover, poor data training and sources may also represent security vulnerabilities to the entire system. In this regard, outdated data sources included in the AI model may give room to manipulation in order to change its behaviour to serve a harmful end goal[24]. Cyberattacks involving AI systems, in general, and CoRoSect's robots, in specific, may compromise the safety of farmers and any individual related to the activity at stake. Current instances of cyberattacks include sensitive infrastructure but also the private industry. Cyberattacks have resulted in permanent damage to manufacturers' plant and equipment[25]. CoRoSect's cybersecurity will be addressed in chapter 3 of this deliverable. Finally, the collection of data from workers and camera recording involve legal risks related to personal data protection and privacy. It is worth noting that the right to respect

[22] Articles 1, 7, 8, 21, 31, and 28, Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 Hereinafter EU Charter of Fundamental Rights.
[23] Art. 16, EU Charter of Fundamental Rights.
[24] Marcus Comiter, 'Attacking Artificial Intelligence: AI's Security Vulnerability and What Policy Makers Can Do About It', (2019) *Harvard Kennedy School Working Paper*, < https://www.belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf> accessed 15 October 2021.
[25] Anro Johannes Hermanus Redelinghuys, Anton Herman Basson and Karel Kruger, 'Cybersecurity Considerations for Industry 4.0' (International Conference on Competitive Manufacturing, February 2019).

for privacy and the right to personal data protection are two closely related but distinct rights. Similarities and differences of these two rights are extensively developed in **D1.1 Ethical and Legal Framework: Initial Assessment Report** at page 48. These privacy and data protection risks will be addressed in detail in chapter 5.

The interaction of robots and humans in the farming context is aspired by CoRoSect. The orchestrations of workflows involve data training. The risks relate to safety of workers, the systems' vulnerabilities, and privacy.

2.3.2 Creation of AI-Enabled Robots with Perception Systems

CoRoSect will intensively work on developing AI technology enabled to perceive the surrounding environment. The purpose is to increase farm level of autonomy and efficiency by equipping them with advanced AI perception methods. The development of AI perception methods will be built on human motion analysis and prediction. The analysis will include whole-body action, hand gestures and finger movements, such as sitting, standing, pointing, waving, lunging, among others. This human motion analysis and prediction undertaking will contribute to the development of robots equipped to handle material for insect rearing, feed and insects.

At this stage, robotic perception includes machine learning algorithms that will enable the machines to learn from sensory data. Legal and ethical risks concern the processing of large amounts of data by covert means, including sensors and cameras. Individuals' rights to respect for private life and to the protection of personal data, enshrined in the EU Charter of Fundamental Rights and the GDPR, must be safeguarded through the compliance with the GDPR requirements for data protection by design and by default[26].

CoRoSect implements sensors and cameras. These technologies may pose privacy and data protections risks.

2.3.3 Robotic Actions Planning and Human-Robot Collaboration

CoRoSect will develop robots equipped with vision-based technology to handle boxes filled with soil and insects and for handling crates. The robots will consist of robot arms and autonomous guided vehicles, with a high-resolution vision system and a tool for picking the crates. Different techniques will be tested to enable robots to autonomously discover and learn optimal actions for completing tasks set by both human operators and CoRoSect decision support system. The robots will be trained to stop in front of obstacles and when humans cross into their way. CoRoSect plans to make humans and robots coexist safely in the farms they operate by optimizing available information on human and robots' location, crate sensors and task status.

Human-Robot integrations throughout the project are aimed to achieve the following purposes: CoRoSect will develop machine learning techniques to train robots to learn from human input. Communications between robots and humans will be based upon methods that are responsive to individuals' needs. In addition, the consortium will implement autonomous robotic systems to act without compromising human workers' safety. Ultimately, CoRoSect will likely allow human workers and robots to work in the same environment in the farm in an optimal way.

[26] Articles 7 and 8, EU Charter of Fundamental Rights; Recital 78, GDPR.

In WP8, CoRoSect specifically works to create an autonomous and human-aware robot trajectory planning. The goal is to equip robots with sufficient intelligence to independently operate and to avoid crashing into humans while moving boxes without human workers' control. To achieve this goal, ATOS will develop situation awareness algorithms. In addition, the consortium plans to design ubiquitous technologies that optimize human-robot communication on the insect care shop-floor. Wearable glass will be developed to provide workers with (1) indications of next robot steps; (2) information about the status of an ongoing task; (3) robot failure that requires human intervention.

Besides risk concerns related to sensors as highlighted in the section above, the vision based technology scanner must take into consideration the privacy rights of workers. In addition, robotic action planning and human-robot collaboration may present risks related to the safety of human workers. Hazards related to workplace robotics include injuries and fatalities when human workers directly interact with robots. Injury and fatality risks also exist when there is no direct collaboration between robots and human workers. The Consortium has anticipated these risks and provided strict safety requirements to address them by following well-established and tested safety concepts for AGV. The **D6.7 Safety Concept for Robotic Systems (Planning)** presents requirements such as the 'movement of the machines should avoid any collision, no matter the object creating the issue (people or any unexpected element in the aisle). This gives us another requirement: **avoid collision with any obstacle** at all times'. The consortium takes into consideration that there will be people in the factory where the machines will operate. In **D6.7 Safety Concept for Robotic Systems (Planning),** it is also highlighted that even when people are not supposed to interact with robots, to maintain the highest safety measures regarding people, the requirements are that 'people will access all areas (even if dangerous or forbidden) and **people have to be safe at all times avoiding all collisions and near-miss**'. CoRoSect aims at using cameras and AI algorithms to detect objects and obstacles with high reliability. This system may be able to detect a person with high reliability, according to the deliverable D6.7. Other safety requirements are expected to be addressed by technical partners.

Training robots with vision-based technology may pose at risk the privacy of individuals interacting with the robots. Autonomous robots may also present risks to individuals' physical safety and integrity.

2.4 Mitigation Measures to Ethical Risks

Following the overview of AI-enabled technologies to be developed by CoRoSect and the ethical risks involving such technologies, this section addresses mitigation measures that aim to ensure trustworthy AI. Such measures encompass technical methods and non-technical methods. Some measures such as high-quality data, documentation, traceability and transparency are, so far, explicitly expected from high-risk AI systems as strictly necessary to mitigate risks to fundamental rights and safety[27]. Risk mitigation measures must ensure responsible development of technologies and innovation.

The European Union has worked on a risk-based approach to impose necessary measures to mitigate negative impacts posed by AI. In this regard, AI must fit into four categories: unacceptable risks, high-risk, limited and minimal risks. Each level of risk imposes different sets of horizontal obligations. Even though regulatory burdens are expected to be imposed in cases AI systems are likely to pose high risks to fundamental rights and safety, in the EU, providers of non-high-risk AI systems are **encouraged** to

[27] Artificial Intelligence Act (proposal).

voluntarily apply the mandatory requirements for high-risk AI systems[28]. In this sense, developers and providers of non-risky AI systems are advised, on a voluntary basis, to create and put in place codes of conduct that reflect the mandatory mitigation measures imposed on high-risk AI systems[29].

CoRoSect's AI system may represent limited fundamental rights and extended safety risks in the light of the definitions provided by the Annex III of the Artificial Intelligence Act proposal. Annex III is still not binding and susceptible to changes and updates. So far, listed high-risk AI systems include: (1) biometric identification and categorisation of natural persons; (2) management and operation of critical infrastructure; (3) educational and vocational training; (4) employment, workers' management and access to self-employment; (5) access to and enjoyment of essential private and public services and benefits; (6) law enforcement; (7) migration, asylum and border control management. AI systems representing a limited or minimal risk to safety and fundamental rights are bound to minimum transparency obligations when interacting with humans, even though the recommendation to follow risk-mitigation requirements for trustworthy AI on a voluntary basis applies to AI systems that offer limited or minimum risks[30].

2.4.1 EU Ethical Framework for AI

The EU approach and strategy to AI have centred on the concepts of trust and excellence. In this sense, policies and regulation related to AI have the mission to safeguard an environment prone to innovation and competition but also with fairness. In order to achieve these ambitious goals, the EU has put in place a strategic plan that involved the appointment of an expert group responsible for reflecting and elaborating guidelines and recommendations related to AI policies.

The High-Level Expert Group on Artificial Intelligence (HLEG AI) work paved the way to the developments of the AI legal and ethical framework[31]. Even though the HLEG AI mandate came to an end in July 2020, the published deliverables in addition to the Artificial Intelligence Act proposal reflect the ongoing legal and ethical framework on AI in the EU. The *rationale* of the ethical framework provided by the HLEG AI reflects on the legislative proposal for an Artificial Intelligence Act. This ethical framework can be found on four main documents released by the HLEG AI: (1) Ethics Guidelines for Trustworthy AI; (2) Policy and Investment Recommendations for Trustworthy AI; (3) Final Assessment List for Trustworthy AI (ALTAI); (4) Sectoral Considerations on the Policy and Investment Recommendations.

Given the **D1.1** addressed in a detailed manner each of the four policy documents, this present deliverable will, first, briefly bring into light some important concepts to the implementation of trustworthy AI. Second, develop aspects that were not taken into account in D1.1 including technical and non-technical methods to the implementation of trustworthy AI. Third, correlate ethical and legal principles concerning the implementation of trustworthy AI to the specific technologies developed by CoRoSect.

2.4.2 Practical Steps for Trustworthy AI

The implementation of trustworthy AI requirements is a continuous process. It must start in the development phase and continue through the usage period. At this point, a rigorous analysis of the

[28] Recital 81, Artificial Intelligence Act (proposal).
[29] Title IX, Artificial Intelligence Act (proposal).
[30] Transparency obligation includes informing individuals that they are interacting with an AI system when it is not obvious.
[31] *See* European Commission, High-level Expert Group on Artificial Intelligence, <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai> accessed 1 September 2021.

requirements must be conducted, and re-designing possibilities must be considered if it is necessary. Trustworthy AI heavily relies on the ability of the technical team to evaluate whether the technical and non-technical methods are met and to justify such evaluation. These mitigation measures will be assessed in the D1.3. In this deliverable D1.2, technical and non-technical methods and requirements necessary to achieve trustworthy AI are presented. The Figure 1 below briefly presents the actors involved in the AI system's life cycle.

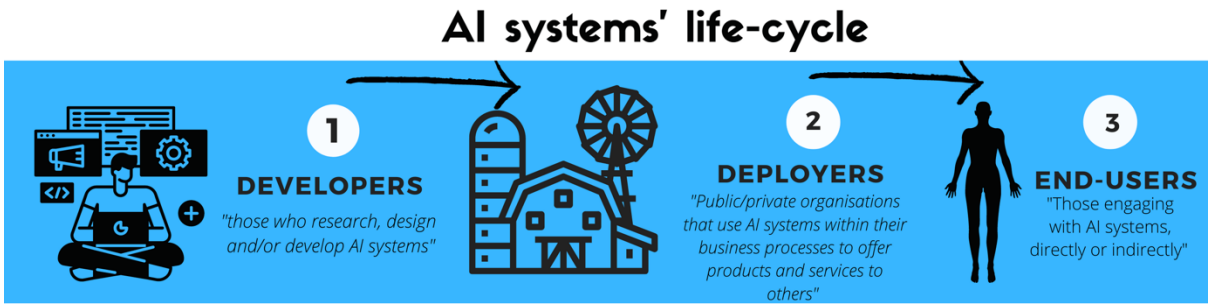

Figure 1[32] AI systems' life-cycle

2.4.3 Technical Methods

Technical methods aim to ensure that trust can be reflected in the design, developments and usage stages of AI technologies. Trustworthy AI depends on several design decisions. The subsections below provide an overview of the technical requirements for trustworthy AI[33].

2.4.3.1 Architectures for Trustworthy AI

The architecture of AI technologies must include the requirements for trustworthy AI. To achieve this purpose, AI developers must set a list of ethically desirable behaviours and rules that the system shall always comply with (white list), and a set of rules and behaviours that the system shall never breach (black list)[34]. In addition, a monitoring system to safeguard compliance with these trustworthy guiding rules during the operation of the AI system must be implemented separately.

To ensure that trust is built-in AI technologies that are constantly learning from new data, developers must attempt that the requirements for trustworthy AI are present in the entire life-cycle of the system. In this sense, the integration of the desirable and undesirable behaviours should follow the sense, plan and act stages of the AI system.

In broad terms, when the CoRoSect consortium develops its robots to select the insects based on data learned and provided by human workers, it must bear in mind that:

1. The technology must be developed in a way that recognizes all environmental elements required to ensure that the ethically desirable behaviours will be accomplished (Sense-Step);
2. The technology must only take into account action strategies that adhere to the ethically desirable behaviours (Plan-Step);
3. The technology must be limited to actions that realise the ethically desirable list created by developers (Act-Step).

[32] Designed by A.M. Corrêa.
[33] 'Ethics Guidelines for Trustworthy AI', see note 16; and HLEG AI, Final Assessment List for Trustworthy AI (ALTAI), July 2020.
[34] 'Ethics Guidelines for Trustworthy AI', see note 16.

2.4.3.2 Ethics and Rule of Law by Design

AI developers shall safeguard that ethical requirements and safety rules are implemented by-design in their AI systems. By-design methods provide the paths companies should pursue in order to implement abstract principles into their systems. Trustworthy AI must comply with the ethical principles of respect for human autonomy, prevention of harm and fairness.

The fairness principle encompasses a substantive and procedural dimension. On the one hand, substantive fairness relates to the concepts of equity and non-discrimination. On the other, procedural fairness concerns the ability of individuals to seek relief in case their rights are breached. The safeguard of procedural fairness also includes the ability of individuals to get an unbiased assessment of their demand.

Human autonomy is a moral and political value that govern individuals lives in most western societies. Autonomy is the capacity to govern oneself by independent considerations and desires. Individuals should be able to live their lives with self-determination. Therefore, AI systems should not manipulate, coerce or deceive individuals with whom it interacts. A human-centric approach to AI requires that AI systems serve human autonomy as a moral and political value.

The principle of prevention of harm requires that the freedom to act is limited to the extent to which it has harmful consequences to others. In this regard, AI systems should operate in a way they do not harm individuals' mental and physical integrity. The principle of prevention of harm deserves special consideration in contexts in which AI systems interact with vulnerable persons or in situations permeated by asymmetries of power, such as the employment and governmental ones. The prevention of harm shall be attempted through the implementation of safety by-design, privacy-by-design and security-by-design. High data quality is fundamental especially when techniques including the training of models are implemented. In this case, data quality will determine whether the AI system will operate safely and without breaching fundamental rights. The aspects concerning security and privacy-by-design will be addressed in chapters 3 and 5, respectively.

The table below contains the requirements AI developers and deployers should implement to protect and promote human autonomy by design:

1. Ensuring the AI system does not manipulate individuals with whom it interacts;
2. Ensuring individuals are aware that decisions they are eventually submitted to are the result of an algorithmic decision;
3. Implementing procedures to avoid end-users over-rely on the AI system;
4. Implementing procedures to avoid that the AI system accidentally affects human autonomy;
5. Implementing procedures to avoid manipulative behaviours.

The prevention of harm should also be attempted with designing solutions. Safety by-design possibilities might be acquired with human oversight in some contexts. Human oversight encompasses three different possibilities: (1) human-in-the-loop (HITL); (2) human-on-the-loop (HOTL); (3) human-in-command (HIC).

Human Oversight	Definition

Human-in-the-loop (HITL)	Possibility for human intervention in every decision cycle of the system
Human-on-the-loop (HOTL)	Possibility for human intervention during the design cycle of the system and monitoring the system's operation
Human-in-command (HIC)	Possibility to oversee that overall activity of the AI system and its impact on economic, societal, legal and ethical values. This capability should allow the decision to not use an AI system in a particular situation and the ability to overrule a decision by the AI system.

Table 2 Three Human Oversight Possibilities

The CoRoSect consortium may determine whether the AI system they develop is a self-learning or autonomous system; is overseen by a human-in-the-loop; is overseen by a human-on-the-loop; is overseen by a human-in-command. The requirements to prevent harm should consist of:

1. In cases the consortium counts with HITL, HOTL, HIC, it must make sure that the humans involved have been given specific training to exercise the oversight;
2. The consortium must make sure to detect any responses mechanisms for undesirable adverse effects of the AI system for the end-users;
3. The consortium must make sure that the robots have a 'stop button' or any safety procedure to abort an operation when it is necessary. This requirement is particularly relevant to the workers' safety;
4. Concerning the self-learning and autonomous nature of CoRoSect's AI systems, the consortium must make sure that specific oversight measures are taken.

Concerning general safety, the requirements include:

1. The definition of the risks, risks metrics and risk levels of each AI developed system. The risks must be measured and assessed on a continuous basis. End-users must be eventually informed of existent or potential risks;
2. Technical faults in the AI system must be investigated and identified. Levels of safety threat related to human integrity should be given special attention by the technical partners;
3. Reliability and robustness tests must be implemented.

2.4.3.3 Explanation Methods

Explainable AI improves accountability, trust, compliance and performance. Creating explainable AI allows human experts and non-experts to understand the causes of a decision and, in some instances, to consistently predict AI model results. The purpose is to make possible to provide an explanation about what happens in the AI model from input to output. Explainable methods increase the ability to question a certain decision and, therefore, increase trust. Explainability has two main possible approaches: global and local. The global approach expresses an overall explanation of the AI model behaviour. It presents a broad view of the model and how the data processing affects the results. The local approach explains each instance of data processing individually and how it individually affects the results.

The requirements of explainable methods consist of:

1. Explaining the decisions of the AI systems to end-users;
2. Continuously assess whether users are aware of the decisions taken by the AI systems.

2.4.3.4 Testing and Validating Methods

The implementation of testing and validating methods intend to ensure the stability and robustness of AI systems. Considering AI technologies have a non-deterministic and context-specific nature, they must be monitored during training and deployment periods. In this regard, testing and validation of AI systems must:

1. Be implemented in early stages;
2. Ensure that it behaves as originally planned during its entire life cycle;
3. Include the whole elements used to create it, such as data, pre-trained models, environments and behaviour;
4. Be designed by a diverse group of people;
5. Include varied metrics with the purpose to test the model from different perspectives;
6. Have deliberately attempted to break the system in order to find its vulnerabilities and weaknesses.

More specific details on CoRoSect's cybersecurity requirements will be addressed in chapter 3.

2.4.3.4 Quality of Service Indicators

Indicators include measures to evaluate the testing and training of algorithms and other traditional metrics to assess software metrics of functionality, performance, usability, reliability, security and maintainability. The appropriate quality of these indicators is a condition to ensure that security and safety are met in AI systems.

2.4.4 Non-Technical Methods

Non-technical methods also serve the purpose of creating trustworthy AI. Similarly to technical methods, non-technical methods should continuously be evaluated. In the subsections below, there is a summary of non-technical methods relevant to CoRoSect.

2.4.4.1 Codes of Conduct

Codes of conducts are helpful to the development of trustworthy AI systems to the extent to which they summarize relevant ethical, legal and safety values. They must serve as internal guidelines for developers with clear and accessible language. A code of conduct with practical guidelines for the accomplishment of trustworthy AI may also contain a charter of fundamental rights to be protected and promotes, as well as ethical principles such as prevention of harm, human autonomy and fairness. Several private companies have their ethics codes of conduct to serve as guidelines[35].

2.4.4.2 Standardisation and Certification

Standards and certification are co-regulatory tools often used to orient customers in their decision-making. In general, the adherence to standards and certification offers to the partners, end-users, and partners of AI developers the ability to recognise that safety and ethical values and rules were met. Currently, ISO standards are internationally agreed upon by experts and include a vast range of purposes. ISO standards cover quality management to attest products' resilience to failures, safety standards to reduce accidents in workplaces, IT security standards to ensure sensitive information is secure. Some of these ISO standards might be useful to CoRoSect developments. The HLEG AI encouraged standardisation organisations to develop trustworthy AI technical standards. The label

[35] *See* IBM, Everyday Ethics for Artificial Intelligence (IBM, 2019). <https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf>, accessed 10 October 2021; Microsoft, Putting Principles into Practice, <https://www.microsoft.com/en-us/ai/our-approach?activetab=pivot1%3aprimaryr5> accessed 10 October 2021.

trustworthy AI should be able to confirm that a certain system adheres to the rules of safety, robustness and transparency, for instance.

2.4.4.3 Accountability via Governance Framework

Companies and organizations developing AI should implement an ethical governance framework. In practice, this framework should consist of a person or an internal/external board in charge of the ethical issues regarding the technologies developed. This framework should be able to provide internal oversight and advice, in addition to sharing the best practices and negative effects with other relevant social actors. In some instances, certification and standardisation serve the purpose of external oversight.

Documentation on how AI systems were developed and expectations about their performance during their lifecycle is a condition to assess whether a certain system complied with trustworthy AI requirements. Documentation and traceability are especially relevant to high-risk AI and should include general aspects, capabilities, limitations of the systems, in addition to the algorithms, data, training, testing and validation process implemented.

2.4.4.4 Diversity and Inclusive Design Teams

The diversity of teams engaged in AI development contributes to the provision of different perspectives and objectives. Diversity should include individuals with different gender, cultural background and age; ideally, diversity should not only be limited to demographic aspects but also to skills and professional paths. Diversity should be present in the teams that design AI systems, test, and deploy.

3 Security Analysis on Human-Robots Interaction

CoRoSect's robots will interact with human workers. Given this reality, CoRoSect's system must have technical robustness in order to ensure low risks to the ones who are interacting with it. Unintentional harm must be prevented as much as possible. General safety and resilience against attacks should be ensured. More precisely, robots' deployment in critical infrastructures, such as the industrial ones, raise concerns related to security, safety, accuracy and trust[36]. Security concerns the resilience robots have against cyber-attacks. Safety includes the risks of accidents in environments of human and robots' collaboration. Accuracy relates to the possibility of performing tasks without faults. Trust concerns the level of satisfaction of these robots to flawlessly replace certain human performances. Safety, security, accuracy and trust should be considered by robot developers in their initial design.

3.1 Security Risks

The main security risks are summarized in Table 3 below:

Lack of Secure Networking	It occurs when the communication between robots and humans are not secure and susceptible to attacks.
Lack of Proper Authentication	Standard usernames and passwords ease unauthorized access to the system and increase the possibility of external attacks.
Lack of Confidentiality	Weak encryption algorithms may lead to the exposure of data and robotic design plans.
Lack of Integrity	Weak authentication protocols can be compromised and lead to the alteration of robotic data.
Lack of Verification	It includes the absence of biometric features to avoid abuses of usage privilege and unauthorized access.
Lack of Authorization	It relates to the possibility of physical access inside robotic labs and control.
Misconfiguration and Bad Programming	It makes robotic systems incapable of performing a planned task with proper accuracy. It may threaten human operators.
Lack of Tamper-Resistant Hardware	Weak hardware turns robots susceptible to damage. This may represent the loss of the robot's operational capacity.
Lack of Self-Healing Processing	The inability to recover in time to attacks exposes robots to cascading attacks.
Lack of Safety Designs	It may entail lethal and threatening accidents towards humans. It may also represent financial losses
Lack of Security By-Design Features	It facilitates breaking into the systems' architecture and the exploitation of security gaps.
Lack of Update	Outdated systems may expose robotic systems to cyber-attacks.

[36] Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman and Ali Chebab, 'Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations' (2021) *International Journal of Information Security*, Mar 19: 1-44.

Table 3 Main Security Risks

The HLEG AI has provided guidelines to address safety and security risks encountered in AI systems. The guidelines contain assessment measures in order to define how susceptible a certain operational system is to external attacks, in addition to assessment measures to define whether the system poses risks to the safety of third parties.

3.2 Assessment Measures to Security Risks

Concerning the aspect of resilience to attack and security, developers should bear in mind whether the AI system:

1. Represents adversarial, critical, or damaging effects to humans or the society, in general, in the case of technical faults or malicious use;
2. Complies with specific security standards;
3. Is vulnerable to certain forms of potential attacks, including data poisoning; model evasion; model inversion.

Developers of AI systems should implement measures to safeguard the integrity, robustness and security against attacks over its lifecycle. End-users should always be informed of the security coverage and updates of a certain system.

Concerning general safety, AI developers should:

1. Define risks, risk metrics and risks levels of the system;
2. Implement continuous assessment measures;
3. Inform end users of existing risks;
4. Identify possible threats, including design faults, technical faults, environmental threats and their consequences;
5. Define safety criticality levels related to human integrity that might result from the faults and misuse of the AI system;
6. Align reliability testing requirements to appropriate levels of stability;
7. Develop mechanisms to assess when the AI system has changed and needs a review of its technical robustness and safety.

4 Insects as Food and Feed: A roadmap to sustainable insect farms

4.1 Ethical Considerations

The way the farms are organized and equipped have tremendous impacts on the lives, health and welfare of animals, humans and society. The treatment of farmed animals in the production, transportation and other farming practices have been a matter of concern for the wellbeing of animals, consumers, and the development of the economy.[37] Humane treatment and care in handling animals are essential for the protection of animals from high mortality, poor welfare and distress, ensuring consumer safety and the protection of the environment.

The welfare concerns for animals have led to a set of strict rules in Europe for the handling of farmed animals.[38] In addition, scientific research on animals has been limited at the national level and in the EU, which ultimately aims to abolish the use of animals for research purposes.[39] Animal research is underpinned by the 'three R' principles: the principles of **Replacement** (replacing warm-blooded animals with plants, eggs or animals that have simple characteristics or ideally with nonanimal models), **Reduction** (reducing the number of animals used in testing), **Refinement** (improving the breeding, accommodation and care of animals and the methods used to minimise pain, suffering, distress or lasting harm to animals).[40] However, these principles and rules generally concern vertebrate animals such as cattle and sheep. Animal welfare legislation and the three R principles do not apply to invertebrates, a category to which insects belong.[41] The ethical use of insects in scientific research has also gained little attention.[42]

Little ethical consideration for insects compared to other animals can be explained by various factors. Different from the vertebrates, there is a lack of consensus in the scientific community regarding the insects' consciousness, the ability to have subjective experiences and feelings such as pain.[43] The damage caused by certain insect species to agriculture, livelihoods, and biodiversity have also been the main focus of research regarding this category of animals.[44] Fischer and Larson note that even when insects are considered valuable for biodiversity and human health, there is a tendency to see

[37] David B Wilkins, *Animal Welfare in Europe: European Legislation and Concerns* (Kluwer Law International, 1997).
[38] Council Directive 98/58/EC of 20 July 1998 concerning the protection of animals kept for farming purposes *OJ L 221, 8.8.1998,* p. 23–27.
[39] European Commission, Animals used for scientific purposes <https://ec.europa.eu/environment/chemicals/lab_animals/index_en.htm> accessed 19 November 2021.
[40] European Commission, 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 19 November 2021.
[41] Council Directive 98/58/EC of 20 July 1998 concerning the protection of animals kept for farming purposes *OJ L 221, 8.8.1998,* p. 23–27.
[42] It must be noted that research over endangered species are generally prohibited. CoRoSect does not involve research on any endangered species. European Commission, 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 19 November 2021.
[43] Jessica Devitt, Insects and Ethics, <https://aucklandecology.com/2017/04/29/insects-and-ethics/> accessed 19 November 2021
[44] Ibid.

them as a whole species rather than individuals.[45] While the authors acknowledge that there is a lack of evidence that insects have conscience, they argue that there is a possibility for insect consciousness because there are recent studies showing that some species demonstrate complex behaviour such as maternal care and tend to avoid painful stimuli. The authors suggest giving some weight to this possibility in moral considerations and applying the three R principles in a moderate manner in the collection of insects for conservation as a mitigation measure.[46]

To sum up, the animal welfare rules and the rules regulating scientific research on animals do not apply to insects. Nevertheless, as noted below in 4.2.2, insect farming industry suggests implementing good welfare practices in insect farms to the extent possible in the special circumstances of insects[47]. In fact, the treatment of insects with care is also closely related to the protection of human and animal health, and the protection of environment. Therefore, insect production is regulated by the highest level of food and feed legislation, which is further addressed below.

4.2 Legal Framework

In addition to the consideration for the wellbeing of animals that are subject to farm practices and research, animal safety and wellbeing are also inextricably linked with the health of humans and other domestic or farmed animals who consume them. As a consequence of the consumers' interest in accessing safe and wholesome food and ensuring the high-level protection of human and animal life, insects produced for human and animal consumption should adhere to the highest safety standards. Below is an overview of standards to which insect farms are responsible to adhere.

4.2.1 European Union

EU legislation on food and feed safety is underpinned by an integrated approach to food safety from 'Farm to Fork'. The so-called 'Farm to Fork' strategy is primarily founded in the White Paper on Food Safety of the European Commission[48], covering the whole food supply chain from production to distribution (See Figure 2). The strategy aims to achieve a sustainable food system which[49]:

- ensure food security and public health;
- ensure access to affordable food while preserving fair economic returns;
- mitigate environmental impacts and address climate changes risks;
- foster conversation of biodiversity.

[45] Bob Fischer and Brendon M. H. Larson, 'Collecting insects to conserve them: a call for ethical caution, Insect Conservation and Diversity' (2019) 12 *Insect Conservation and Diversity* 173.
[46] *Ibid*.
[47] See below 4.2.2.
[48] European Commission, White Paper on food safety, <https://op.europa.eu/en/publication-detail/-/publication/6d4b523b-dad8-4449-b2b4-9fa9b0d6e2be/language-en> accessed 19 November 2021.
[49] European Commission, Farm to Fork Strategy, <https://ec.europa.eu/food/horizontal-topics/farm-fork-strategy_en> accessed 19 November 2021.

Figure 2 European Commission's Farm to Fork Strategy[50]

Based on this strategy, the EU provides a robust framework for food and feed safety that also concerns insect farms. In the EU, insect farm activities are governed by the general legislation on food and feed safety standards applicable to all food and feed products. A set of EU legislation, commonly referred as the General Food Law[51] and the Hygiene Package,[52] lays down principles and rules to ensure that the animals can be safely consumed by humans and other animals produced as pets or human food. These principles and rules are further integrated by the national laws at the country level.

The EU legislation provides general principles governing food and feed safety, hygiene requirements and good practices, as well as organisational arrangements and procedures that may have an impact on food and feed safety. Food that is injurious to health and unfit for human consumption should not be placed on the market.[53] All food or feed producers, distributors and business operators, including insect farms that supply their products to the EU market, are responsible for complying with the relevant principles, good practices and procedures.

Under this framework, insect farms should demonstrate compliance with the applicable standards and rules by putting in place organisational measures and safeguards. For instance, they have an obligation to register or receive approval for their activities before national competent authorities,

[50] *Ibid*.

[51] Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety, *OJ L 31, 1.2.2002,* p. 1–24.

[52] Commission Regulation (EU) 2021/382 of 3 March 2021 amending the Annexes to Regulation (EC) No 852/2004 of the European Parliament and of the Council on the hygiene of foodstuffs as regards food allergen management, redistribution of food and food safety culture (Text with EEA relevance). C/2021/1312, *OJ L 74, 4.3.2021*, p. 3–6.

[53] Art. 14(2), Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety, *OJ L 31, 1.2.2002,* p. 1–24.

comply with hygiene standards throughout insect's life cycle, and ensure that their insects are in good health by feeding them only with acceptable materials and preventing the spread of diseases.[54]

In accordance with a preventive approach to address the food and feed safety before any harm occurs, insect farms are encouraged to adhere to good hygiene practices such as[55]:

- controlling the contamination of hazardous materials;
- measures to use water, organic waste, fertilisers, plant protection products, veterinary medicinal products and feed additives in an appropriate manner;
- taking measures to prevent transmissible diseases and notify the competent authority, where required;
- applying good hygiene practices to ensure feed safety in the production, preparation, storage and transport of feed;
- Keeping records;
- Disposing of dead animals, waste and litter properly;
- ensuring traceability of feed.

In addition, the following regulations apply to the activities of insect farms:

- Regulation (EC) No 1069/2009 on animal by-products. Insects are categorized as 'farmed animals', and therefore must be fed with the feed materials applicable to this category of animals. The processing of animal by-products is subject to hazard analysis and critical control points (HACCP) principles.56 Necessary approvals should be obtained for the killing and further processing of insects in accordance with Art. 24(1)(a));
- Regulation (EU) 2016/429 of the European Parliament and of the Council of 9 March 2016 on transmissible animal diseases and amending and repealing certain acts in the area of animal health (Animal Health Law).57 As insects are considered farmed animals, they should be handled in accordance with the animal health standards applicable to farmed animals. Insect producers should put in place measures to ensure that insects and their derived products intended for food and feed are not pathogenic or have negative impacts on plants, animals or human health. Diseases that are transmissible to animals or humans should be prevented and controlled;
- Regulation (EU) No 1143/2014 on the prevention and management of the introduction and spread of invasive alien species. To preserve biodiversity and mitigate environmental impacts, certain insect species are excluded from farming activities. Insects listed as an 'invasive alien species' cannot be subject to farming operations.58 The list of invasive alien species is

[54] Technical specifications of the insect species involved in the CoRoSect project are addressed under WP2.
[55] PART B Recommendations for guides to good practice, Regulation (EC) No 183/2005 of the European Parliament and of the Council of 12 January 2005 laying down requirements for feed hygiene (Text with EEA relevance), *OJ L 35, 8.2.2005*, p. 1–22.
[56] Art. 29(1)(a), Regulation (EC) No 1069/2009 of the European Parliament and of the Council of 21 October 2009 laying down health rules as regards animal by-products and derived products not intended for human consumption and repealing Regulation (EC) No 1774/2002 (Animal by-products Regulation) *OJ L 300, 14.11.2009*, p. 1–33.
[57] Consolidated text: Regulation (EU) 2016/429 of the European Parliament and of the Council of 9 March 2016 on transmissible animal diseases and amending and repealing certain acts in the area of animal health (Animal Health Law).
[58] Commission Implementing Regulation (EU) 2016/1141 of 13 July 2016 adopting a list of invasive alien species of Union concern pursuant to Regulation (EU) No 1143/2014 of the European Parliament and of the Council C/2016/4295, OJ L 189, 14.7.2016, p. 4–8.

regularly updated. The research conducted by end-user partners in the CoRoSect project does not concern the listed species.

In addition, EU animal welfare legislation lays rules for the protection of animals bred or kept for farming purposes. However, animal welfare rules do not apply to insects because invertebrate animals are exempted from these rules.[59] As a result, insect farms are not bound by the EU animal welfare legislation.

Insect-farms are responsible for the safety and hygiene of food and feed in their management structures. Technologies developed in CoRoSect should allow end-users to comply with their obligations regarding food and feed safety and hygiene. CoRoSect platform should allow the provision of the necessary environmental needs of insects such as optimal temperature, humidity, gas levels, air speed and light.

4.2.2 Animal Welfare for Insects

In spite of the fact that EU legislation does not provide welfare rules for insects, the ethical production of insects has been encouraged by the insect farming industry. In the absence of legal rules, the industry's efforts to create harmonized standards can play a crucial role in guiding the farm practices of industry actors.

Based on Brambell's 5 degrees of freedom, Figure 3 provides a list of freedoms suggested by the industry to establish good welfare practices to the extent that they can be implemented in the context of specificities of insect production processes.[60]

[59] Art. (1)(d), Council Directive 98/58/EC of 20 July 1998 concerning the protection of animals kept for farming purposes, *OJ L 221, 8.8.1998,* p. 23–27.

[60] International Platform of Insects for Food and Feed (IPIFF), Ensuring High Standards of Animal Welfare in Insect Production,<https://ipiff.org/wp-content/uploads/2019/02/Animal-Welfare-in-Insect-Production.pdf> accessed 19 November 2021. Invertapro and Nasekomo are ordinary members, ICF and Entocycle are associated members and KU Leuven is an academic member to the IPIFF: See IPIFF Members <https://ipiff.org/ipiff-members/> accessed 19 November 2021.

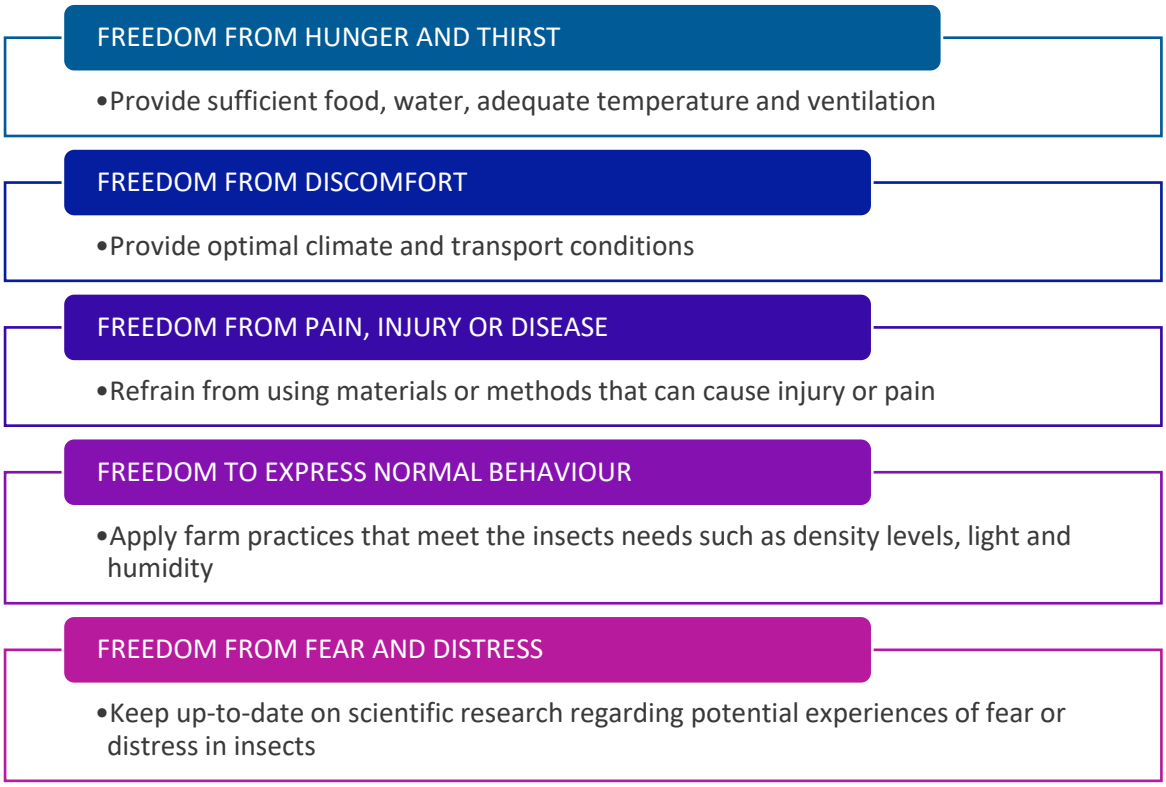

Figure 3 Five Degrees of Freedom

The differences between vertebrates and invertebrates require the implementation of these freedoms in the specific context of insects. The technical specificities of insects and challenges arising from their natural instincts, such as cannibalism, are some of the factors to take into account when enabling a normal behaviour environment and limiting injuries and deaths.[61]

Animal welfare rules should be implemented to the extent that they apply to the specific technical and other needs of insects. CoRoSect platform should allow and foster the handling of insects in a manner that does not cause hunger or thirst, discomfort, pain or distress to them. The conditions created by the use of the CoRoSect platform should enable creating the proper environmental conditions and providing an appropriate level of feed and water to insects. AI-based object recognition methods used for quality control should be designed in a technically robust way to ensure that insects are selected and treated under acceptable welfare conditions in addition to the safety and hygiene standards.

4.3 Organisational Measures for Good Hygiene Practices

The adequate level of production facilities, equipment and staff are prerequisites for the implementation of the highest safety and hygiene standards for food and feed. The design and use of production infrastructure and any relevant tools and equipment are essential factors in keeping production areas free from contamination and hazardous materials, avoiding damages and ensuring

61 *Ibid*.

that insects are not accidentally released.[62] Therefore, their design and instalment are subject to certain rules and requirements, which should be implemented with technical and organisational measures. Insect producers are responsible for providing and designing production facilities in a way that good practices for hygiene and safety can be applied.

Hygienic conditions of the pieces of production equipment, containers, crates, vehicles, vessels and other tools are important factors to guarantee the cleanness and safety of the production processes. The design and construction of such tools should enable that the surrounding areas should be kept clean and easily disinfected. In feed production, the applicable framework imposes that facilities and equipment should be designed and constructed in a way that they enable:

1. adequate cleaning and disinfection;
2. minimisation of the risk of error;
3. avoiding contamination and other general effects that can jeopardize the feed safety and quality.

Similarly, the equipment, crates, vehicles and other tools are required to be kept clean and disinfected in food production.[63] All pieces of equipment and fittings that come into contact with the food should be adequately cleaned and disinfected in sufficient frequency.[64] Therefore, they should be constructed and kept in a way that they can be easily cleaned. Their material content and technical condition should allow the elimination of the risk of exposing the foodstuff to harmful elements.[65] The use and instalment such equipment should not create an obstacle to performing hygienic practices in the surrounding area.[66] If necessary, a control device should be launched to ensure that the equipment function in the required manner.[67]

Importantly, to the extent that the equipment and tools perform various tasks such as cleaning, controlling environmental conditions, feeding and monitoring growth of insects in an automated manner, it becomes even more crucial that their design and use adheres to the high standards applicable to the hygienic requirements for the handling of animals and other sources. New technologies should enable and support insect farms to implement their general duties such as keeping animals clean, using clean water, handling waste, monitoring animal health for contagious diseases, correct use of additives and medicinal products.[68] The skills and training of the farm staff can also contribute to the appropriate use of technologies and enable human intervention where necessary. In this context, insect-farms should consider taking organisational measures. Below, it is provided a list of non-exhaustive measures.

---

[62] International Platform of Insects for Food and Feed (IPIFF), Guide on Good Hygiene Practices, <https://ipiff.org/wp-content/uploads/2019/12/IPIFF-Guide-on-Good-Hygiene-Practices.pdf> accessed 19 November 2021, p. 35.

[63] Annex 1 Part A(II)(4), Commission Regulation (EU) 2021/382 of 3 March 2021 amending the Annexes to Regulation (EC) No 852/2004 of the European Parliament and of the Council on the hygiene of foodstuffs as regards food allergen management, redistribution of food and food safety culture (Text with EEA relevance) C/2021/1312, *OJ L 74, 4.3.2021*, p. 3–6.

[64] Annex II Chapter V(1), Commission Regulation (EU) 2021/382 of 3 March 2021 amending the Annexes to Regulation (EC) No 852/2004 of the European Parliament and of the Council on the hygiene of foodstuffs as regards food allergen management, redistribution of food and food safety culture (Text with EEA relevance) C/2021/1312, *OJ L 74, 4.3.2021*, p. 3–6.

[65] *Ibid*.

[66] *Ibid*.

[67] *Ibid*.

[68] *Ibid*. Annex I Part A(II)(4).

Organisational measures that can be implemented by insect farms for good hygienic practices include:

- Designating qualified staff for the technical maintenance and service;
- Ensuring that the staff is sufficiently equipped and trained to use, check and clean advance technological equipment;
- Establishing cleaning programmes for clean and hygienic equipment;
- Standardising and validating manually or automatically performed cleaning practices;
- Keeping records of the cleaning measures as part of an internal quality management system;
- Regularly checking and carrying out audits in accordance with the instructions and warnings of the equipment's manufacturer;
- Testing devices for accuracy;
- Deploying control device for the use of equipment, if applicable[69].

Technologies developed by the CoRoSect project will integrate the insect farm premises in the production and handling of insects. These cutting-edge tools will be important to carry out the management procedures and decision-making in the production practices, feeding, watering and measuring the environmental conditions such as temperature, humidity and light. They should be designed in a manner that they are cleaned and disinfected in an easy manner. The development of legally and ethically compliant, robust AI and robotics is important to ensure that unforeseen risks to food and feed hygiene and occupational risks are prevented, and insect production practices are managed in an appropriate manner. Regular tests, checks and audits should be performed to ensure accurate functioning. It should be ensured that the staff who will be in charge of using and monitoring these technologies are well-trained and skilled to perform such tasks.

[69] Annex II Chapter V(1), Commission Regulation (EU) 2021/382 of 3 March 2021 amending the Annexes to Regulation (EC) No 852/2004 of the European Parliament and of the Council on the hygiene of foodstuffs as regards food allergen management, redistribution of food and food safety culture (Text with EEA relevance) C/2021/1312, *OJ L 74, 4.3.2021*, p. 3–6.

5 Personal Data Protection and Privacy on CoRoSect's Rearing Platform

D1.1 Ethical and Legal Framework: Initial Assessment Report preliminarily explained that data protection requirements apply to the processing activities of CoRoSect project where personal data are processed. The consortium member carrying out such processing activity would be the data controller. Data controller is the main responsible for the legal and ethical processing of personal data in accordance with the data protection rules. The rationale behind this responsibility is that the controller is the person who has the authority to make any decision regarding the processing activities in a given situation.[70] Data controller exercises control in relation to the determination of whether personal data will be collected, and why and how the processing will be carried out. [71] The question of ''why'' refers to the **purpose** of processing, which are the legal grounds listed under GDPR that legitimize the processing. The question of ''how'' refers to the **means** of processing, referring to both technical and organisational decisions. Technical decisions include the ways in which the data will be processed, for instance, the technology used. Organisational decisions include measures regarding the selection of data, sharing of data with others or storage periods.[72] As such, the use of CoRoSect can be considered as a determination of purposes and means of the processing of personal data within insect farms. Therefore, the legal entity owning and operating the farm, as data controller, will handle, manage and control the data processing, which should be in accordance with GDPR.

In the remaining of this chapter, the requirements that need to be complied under the data protection framework are analysed. Building on **D1.1 Ethical and Legal Framework: Initial Assessment Report**, the principles and data subjects rights are further specified and elaborated, which must be taken into account in the development of CoRoSect.

5.1 Data Protection by Design

Compliance of the end-users of CoRoSect with data protection requirements is closely linked with the data protection by design principle that requires the implementation of appropriate measures which are designed to comply with data protection rules. Legally established for the first time under the GDPR, this principle imposes on the controller the obligation to put in place technical and organisational measures in order to ensure that all data processing activities are carried out in accordance with the data protection principles and the rights and freedoms of data subjects are protected.[73] The so-called measures cover a wide variety of solutions whose suitability to a particular processing activity will depend on the context and risks associated with the processing in question.[74] The EDPB provides guidelines for controllers to assist in the implementation of these measures that may be in the form of the following examples[75]:

- use of advanced technical solutions;
- pseudonymization of personal data;
- storing personal data available in a structured, commonly machine-readable format;
- providing information to data subjects and/or enabling their intervention in the processing;

[70] Art29WP, 'Opinion 1/2010 on the concepts of "Controller" and "Processor"' (2010) 00264/10/EN, p. 8.
[71] *Ibid*, p. 14.
[72] *Ibid*.
[73] Art. 25(1), GDPR.
[74] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (2019), p. 6.
[75] *Ibid*, see also, Recital 78, GDPR.

- providing information about the storage of personal data;
- having malware detection systems;
- training employees about basic "cyber hygiene" or other issues;
- establishing privacy and information security management systems;
- carrying out Data Protection Impact Assessment (DPIA)[76].

The data protection by design principle directly concerns the end-user controller who will process personal data but also the developers and producers of technological tools and devices. Derived from the concept of ''privacy by design''[77] – proactively embedding privacy into the practice of engineering and system architecture – the data protection by design principle implies that developers and procedures of technological devices and tools should design and produce any technical solutions that will be used by the end-users in the processing of personal data by taking into account the principles, rules and safeguards of data protection law. Recital 78 of GDPR illustrates this understanding:

''When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.''

Therefore, the principles and rules provided in this chapter and the EDPB guidelines on the implementation of the data protection by design principle are also relevant for the technical partners of the CoRoSect project. In line with the by design approach, the developers of the CoRoSect technology should take into account these principles and rules in the design and development of the technological tools, devices and software. The implementation of the data protection by design principle will help the end-users of CoRoSect to fulfil their data protection-related obligations after the end of the project (for example, by deploying technical measures that will make it possible to meet personal data storage requirements). CoRoSect will provide the means by which data protection can become a reality.

Hence, the remaining of this chapter aims to guide the consortium members, on the one hand, to provide an understanding about any direct obligation that the framework may impose on them as controllers, and to facilitate the integration of the data protection requirements in the system architecture by technical partners, on the other hand.

5.2 Key Terms and Definitions Involving Data Protection

Processing is a broad term encompassing a wide range of activities from collecting, recording, disclosing, combining or deleting.[78] As processing one's information concerns the individual's right to individuals' rights to respect for private life[79] and to the protection of personal data[80], it should be carried out in accordance with law, data protection principles and rules. Data protection aims to find a balance between the interests of those who use data for their interests, including research or

[76] See D1.1 Ethical and Legal Framework: Initial Assessment Report.
[77] A. Cavoukian, *Privacy by Design*, Leading Edge, IEEE Technology and Society Magazine, 2012, 31/4.
[78] Art. 4(2), GDPR.
[79] Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) Art. 8; Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 ECHR, Art. 8.
[80] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 ECHR, Art. 7.

economic interests on the one hand, and the rights of individuals whose data are used for such interests on the other.

A core concept for the purposes of data protection is the notion of personal data. As data protection rules are principally applied when personal data is processed, it is important to differentiate the type of data used in the CoRoSect project.

5.2.1 Personal Data

The concept of personal data is defined by Article 4(1) of GDPR (See Figure 4):

> Personal data means any **information relating to an identified or identifiable natural person** (data subject); an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Figure 4 Definition of Personal Data

The GDPR provides a broad definition of personal data, which encompasses a wide range of information that do not necessarily concern the private or family life of an individual (the so-called **data subject**). The definition in the GDPR is construed in a technology-neutral way, without any reference to how this concept will be applied in the context of a specific technology or application. In practice, assessing whether a piece of information is personal data may not be straightforward and may require a well-rounded examination of a variety of factors in a particular case. Opinions and guidance of Article 29 Working Party – independent working party that dealt with issues relating to the protection of privacy and personal data in Europe until it was succeeded by the European Data Protection Supervisor in 2018- provide further help in this regard.

The main constituents of personal data are further explained below:

i. Information

Information is a broad concept that includes both objective elements (e.g. DNA) and subjective factors such as opinions or beliefs (e.g. an assessment of the work performance of an employee). For information to be qualified personal, it does not need to be true or correct.[81] As the protection offered by the right to personal data goes beyond what falls under private and family life, it covers data providing any information such as IP addresses, location data or an online identifier.

Information amounting to personal data may take any form such as alphabetical, numerical, graphical, photographical or acoustic information. Information concerning an individual kept in paper-based format or stored in a technological device by means of codes or recordings are capable of qualifying personal information.[82] Voice records and video images allowing to recognize an individual are examples of personal information.[83]

ii. Natural Person

Personal data represents information of a living natural person (individual), i.e. data subject, regardless of his or her nationality or residence status. Consequently, information about legal entities (such as companies and associations) or deceased persons are generally not protected by data protection law.[84] However, it is possible that information concerning a company can still be a personal data if it reveals information about a natural person. For instance, official title of a company revealing the name of the sole natural person shareholder can be considered as personal data protected by the data protection rules and principles.

iii. Link between the information and data subject

Personal data reveals information **relating** to a data subject, referring to the necessity to establish a link between information and the individual in question. Information that typically concerns objects can also relate to an individual under some circumstances. This is the example of a property price used to calculate the tax duty of an individual.[85] Similarly, information relating to a machine or a technical process in the context of human-machine interaction may relate to an individual depending on the context in which the data is used or is like to be used.[86] In the following alternative scenarios, information can be considered to relate to an individual[87]:

''Content'' scenario one: Information is ''about'' an individual. It reveals the identity and characteristics of an individual, such as name or date of birth.

''Purpose'' Scenario two: Information is used or is likely to be used with the purpose to evaluate, treat in a certain way or influence the behaviour of an individual. An example is the use of location or the number of kilometres made by a taxi to evaluate the performance of taxi drivers.

''Impact'' Scenario three: The use of information has an impact on the interests of the individual even if it is a minor impact, for instance, when individual is treated differently than others.

iv. identifiability

[81] Art29WP, 'Opinion 4/2007 on the concept of personal data' (2007) 01248/07/EN, p. 6.
[82] *Ibid*, p. 7-8.
[83] *Ibid*, p. 10.
[84] Recital 27, GDPR.
[85] Art29WP, 'Opinion 4/2007 on the concept of personal data' (2007) 01248/07/EN, p. 9.
[86] *Ibid*.
[87] *Ibid*, p. 10-11.

As the fourth element of personal data, the information relates to an individual who is ''identified or identifiable''. Identifiability refers to the phenomenon that a piece of information enables distinguishing an individual from other individuals and makes the individual recognizable. The so-called ''identifiers'' can allow to sing out an individual among others in a direct fashion, name or picture of a person being typical examples. Identifiers can also make it possible to identify a person in an indirect fashion when combined with other pieces of information. For example, a phone number, ID number profession of a person cannot all alone identify a person, however, if they are searched through a database of human resources, they can allow the identification combined with other information found in the database. Similarly, even colour of a t-shirt or whether a person is tall or short can be potential identifiers if there is a possibility to single-out the individual with additional information, for example, if it is known that there was only one person with that clothing or height in a certain time and place.[88]

Importantly for the CoRoSect project, it must be underlined that the European independent bodies and courts apply a very low threshold for determining whether a piece of information allows singling out a person, bringing a wide variety of information within the scope of personal data. Technological tools and devices that collect information on the behaviour of a machine can make it possible to identify or influence the behaviour of their user, or assign decisions for him or her without the necessity of identifying the identity of the individual in a strict sense.[89] Personal data are not necessarily obvious identifiers such as name or ID number, but can also be, for instance, web surveillance tools, cookies or computerized files registering unique identifiers for individuals. Simple traffic data in an information system linked to the computer of an employee can be also be considered personal data.

As noted above, information relating to an individual is not only characterized by its content but can be characterized by its purpose or impact. For example, a robot collects location data and detects body parts of a worker to avoid collusion. Even if it does not collect data on identifiable body parts of the workers (such as face), it may be argued that the collected data are personal data relating to an identifiable individual because the processing may have an impact on the individual, for instance, the impact of collusion in case of a defect.

The wide definition of personal data is also evident in the concept of ''identifiability'', i.e. the possibility of identification. Even when a person does not possess all the necessary information to identify an individual at a particular point in time, there may still exist certain means that makes identification possible. For example, a business X share their customer's financial information with company Y in order to calculate their business risks. To enable client confidentiality and reduce the shared information to a minimum, the business X assigns numbers for each customer without disclosing the identity of customers. Company Y is not able to know which number is assigned to which customer, thus cannot identify the identity of customers in a narrow sense, however shared information would still be considered personal data because business X possesses the means of identifying them.

On the other hand, mere hypothetical possibility is not sufficient for identifiability. Recital 26 of GDPR refers to "all the means likely reasonably to be used by the controller or any other person". The potential for identification should be dynamically assessed as long as data is kept, taking into account factors such as costs necessary for identification, legal risks of identification (e.g. breaches of

[88] *Ibid*, p. 12-13.
[89] *Ibid*, p. 14-15.

confidentiality duties) and the level of technological capabilities that can make identification possible.[90]

In *Breyer v Bundesrepublik Deutschland*[91], the CJEU considered that dynamic IP addresses registered by online media service providers when individuals visit their websites are personal data, although another person, internet service provider, has additional information that can enable identification of the owners of an IP address. The court noted that all information necessary for identification does not need to be at the hands of one person. The court analysed whether online media service providers have the means likely reasonably to be used to identify individuals visiting websites. Internet service providers are not legally allowed to transfer the additional data necessary for identification to media service providers, however, in certain circumstances such as cyber-attacks, the latter has the legal means to request from public authorities to receive the additional data from the internet service providers to hold attackers criminally liable. Therefore, it was considered that online media service providers have the means for identification, which meant that IP addresses registered by online media providers are considered to be personal data.

5.2.2 Special Categories of Data

The GDPR distinguishes certain types of data as special categories of data, or the so-called 'sensitive data', which are afforded a higher level of protection due to their link to the data subject's autonomy and dignity, and importance for the protection of data subject's rights. Such data includes personal 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.[92]

5.2.3 Anonymous and Pseudonymised Data

As a technical and organizational measure, personal data can be anonymised to prevent the identification of an individual. **Anonymisation** refers to the process in which all elements allowing the identification of an individual are removed from personal data so that the individual is no longer identifiable (See Figure 5).[93] Anonymisation breaks the link between identifiability and the rest of the constituents of personal data, rendering it non-personal. Thus, the GDPR does not apply to anonymous data.[94]

[90] *Ibid*, p. 15.
[91] CJEU C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, 12 May 2016.
[92] Art. 9(1), GDPR.
[93] Art29WP, 'Opinion 05/2014 on Anonymisation Techniques' (2014) 0829/14/EN, p. 5.
[94] It must be clarified that anonymization is a kind of processing personal data, therefore GDPR applies to the anonymization itself. This means that anonymization of personal data can be carried out only if it is lawful under GDPR.

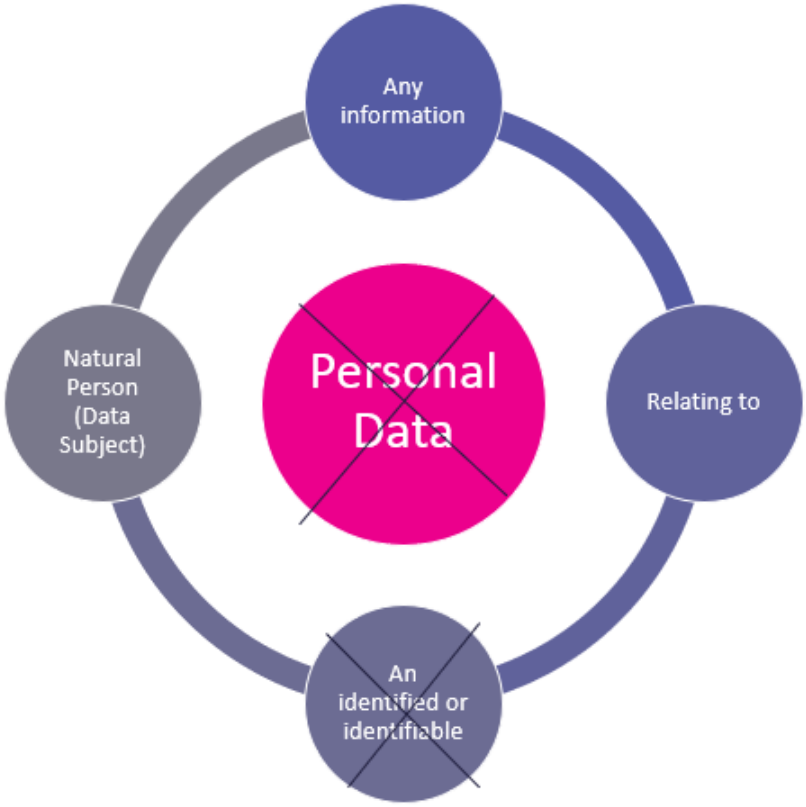

Figure 5 Anonymized Data

Pseudonymisation, on the other hand, does not change the personal character of data. It refers to a way of processing ''personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information''.[95] Identifying elements such as name, date of birth or address are replaced by a pseudonym or an identifier, and kept separately from the rest of the information relating to the individual. Such identifiers are further protected on a technical and organisational level, for instance by allowing only a limited number of authorized persons to access to the pseudonymised data.[96] There are different pseudonymisation techniques, one of them being data encryption.[97] Pseudonymisation is one of the technical measures that help to protect personal data, minimize the risks to the rights of the data subject, and comply with the GDPR obligations.[98]

5.2.4 Non-Personal Data

Non-personal data are all kinds of information that fall outside the scope of personal data such as environmental or industrial data. It may be manually processed or machine- generated data that is characterized by the fact that it does not relate to an identified or identifiable individual. Data protection law does not apply to non-personal data. Nevertheless, non-personal data may be subject to EU law and national laws establishing legal and technical limitations to the free movement of non-

[95] Art. 4(5), GDPR.
[96] Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, para. 18.
[97] Art29WP, 'Opinion 05/2014 on Anonymisation Techniques' (2014) 0829/14/EN, p. 20-21.
[98] Recital 28 and Art. 25(1), GDPR.

personal data. Such limitation includes data localisation requirement for data used for public security purposes.[99]

At the EU level, Regulation (EU) 2018/1807 (Regulation on the Free Flow of Non-Personal Data) applies to non-personal electronic data with the aim of facilitating free storage and processing of non-personal data throughout the EU.[100] Regulation on the Free Flow of Non-Personal Data encourages services providers such as cloud service providers to develop codes of conduct regarding the conditions under which users can move data between cloud service providers and back into their own IT environments. It also clarifies that cybersecurity requirements applicable to businesses storing and processing data will continue to apply to storage or processing data across borders in the EU or in the cloud.[101]

5.2.5 Challenges to Personal & Non-Personal Data Distinctions

The GDPR and Regulation on the Free Flow of Non-Personal Data are two distinct yet complementary instruments, which together govern the free flow of data in the EU. Two separate instruments applicable to personal or non-personal data may suggest that if the personal data criteria are followed, the applicable framework can be identified depending on the type of data. However, the differentiation between personal and non-personal data is not an easy task in practice, making it difficult to determine which rules are applicable. This sub-section points out two challenges to such distinction.

The first challenge relates to the mixed datasets, being the most-used data set in the data economy.[102] Especially, mixed datasets are common in the context of new technologies involving AI and big data analytics.[103] The European Commission provides guidance regarding the applicable framework to mixed datasets, providing the following examples of them[104]:

- a company database including information on individual IT incident reports;
- data collected through an IoT device to make predictions relating to individuals;
- a research project's database containing both raw data and anonymised statistical data;
- analysis of operational log data of manufacturing equipment.

In case personal and non-personal data can be distinguished within a dataset, each legal framework will apply to the relevant type of data.[105] However, the personal and non-personal data parts of the datasets are ''inextricably'' linked, meaning that it would not be practically possible, economically efficient or technically feasible to separate them, GDPR applies to the whole dataset.[106] A decrease in dataset's value or necessity to invest in additional products and services may substantiate the

[99] Regulation (EU) 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, 28.11.2018.
[100] European Commission, Free flow of non-personal data, Available at: https://digital-strategy.ec.europa.eu/en/policies/non-personal-data accessed 21 October 2021.
[101] Regulation (EU) 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, 28.11.2018, Recital 33-34.
[102] European Commission, Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European, 29.05.2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0250&from=EN, accessed 21 October 2021, p. 8.
[103] *Ibid*.
[104] *Ibid*.
[105] *Ibid*, p. 8-9.
[106] Art. 2(2), Regulation (EU) 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, 28.11.2018.

motivation not to separate the datasets. In fact, data controller does not have an obligation to do so.[107] Where dataset stays as mixed, data controller will handle the dataset as a whole in accordance with the GDPR standards, regardless of the proportion of personal data within the dataset.[108] As a result, the difference between the two data types will be meaningless in practice as they will both be treated the same way.

The second challenge stems from the fluid nature of data. Technical capabilities resulting from increasingly available data points and sophisticated algorithms, coupled with the legal uncertainty as to what means are ''reasonably likely'' to single out an individual make it possible that certain personal data may be wrongly considered as non-personal.[109] Article 29 Working Party acknowledges that none of the anonymisation techniques is free from shortcomings, and their effectiveness in making identification impossible have been challenged in the literature.[110] In addition, even anonymized data can become personal again, depending upon the purpose of the further processing and future data linkages.[111] Therefore, some authors advocates for a dynamic understanding of data, arguing that the responsibility of recipients of anonymous data does not come to an end because GDPR principle is no longer applicable. For those who consider anonymizing data, Article 29 Working Party recommends taking into account the inherent limitations of anonymisation techniques in light of the purpose of anonymisation and increasing robustness by combining different types of techniques.[112]

5.2.6 Data Protection Principles

As provided in **D1.1 Ethical and Legal Framework: Initial Assessment Report**, GDPR incorporates a set of principles that must be applied to the processing activities carried out by CoRoSect project from the beginning to the end. Data protection principles provide a general framework, which is then applied in more detailed provisions of GDPR. They provided the basis for the application of the data subject's rights and obligations provided in data protection legislation. All data protection rules at the national level should comply with these principles. Deviations and exemptions from these principles are possible when these are provided for by law, pursue a legitimate aim and be necessary and proportionate measures in a democratic society.[113] For completeness and clarity, six data protection principle are summarized below (See Figure 6).

[107] European Commission, Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European, 29.05.2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0250&from=EN, accessed 21 October 2021, p. 10.
[108] *Ibid*. p. 9.
[109] M. Fink and F. Pallas, 'They Who Must Not Be Identified—Distinguishing Personal from NonPersonal Data under the GDPR' (2020) 10 International Data Privacy Law, p. 11-12.
[110] P. Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 UCLA Law Review 1701.
[111] S. Stalla-Bourdillon and A. Knight, 'Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2016) 34 Wisconsin International Law Journal 284.
[112] Art29WP, 'Opinion 05/2014 on Anonymisation Techniques' (2014) 0829/14/EN, p. 23-24.
[113] Art. 23(1), GDPR.

Figure 6 Data Protection Principles

Lawfulness, fairness and transparency: Personal data should be processed lawfully, fairly, and in a transparent manner in relation to the data subject.[114]

- To be considered *lawful*, processing activities should be based on a legal ground established by law. GDPR provides an exhaustive list of six legal grounds on which processing activities can rely on, which are further discussed in the context of CoRoSect below in 5.3.
- The requirement of *fairness* prohibits the collection of processing of personal data in an unfair, deceptive or secret manner. Fairness of processing ensures a fair relationship between the data controller and the data subject. The controller should inform the data subjects about the potential risks and demonstrate compliance with the data protection rules.[115]
- For processing activities to be *transparent*, data subject should be informed in a clear and plan language about the processing activities, including information on what data is being or will be processed, who will process it for which purpose and data subject's rights.[116] Transparency guarantees that all necessary information is provided to the individuals ideally before the processing starts and is available during the processing and upon request of the individual whose data is processed.

Purpose limitation: Personal data shall be obtained for explicit and well-defined purposes determined before personal data is collected.[117] For further processing for a new purpose to be legitimate, the new purpose must be compatible with the initial purpose of collection of personal data, or the new processing must have its own legal ground. Further processing for archiving purposes in the public

[114] Art. 5(1)(a) and Art. 9(1), GDPR.
[115] EU Agency for Fundamental Rights, Handbook on European Data Protection Law, Luxembourg, Publications Office of the European Union, 2018, p. 118.
[116] Recital 39, GDPR.
[117] Art. 5(1)(b), GDPR.

interest, scientific or historical research purposes or statistical purposes enjoy an exception to this rule if protective measures (such as e pseudonymisation) are in place.[118]

Data minimisation: Only relevant data that is necessary for achieving the purpose of the processing shall be collected.[119] Personal data should not be collected if the purpose of processing can be reasonably fulfilled by other means.[120]

Data accuracy: Collected data should be kept accurate and up-to-date. This also means that inaccurate data should be erased or corrected without delay.[121]

Storage limitation: Where personal data is processed, it must be kept only as long as it is necessary for the project purposes to be achieved.[122]

Data Security (integrity and confidentiality): Technical or organisational measures should be taken to ensure appropriate security of the processed personal data, protecting them against unauthorised or unlawful processing and against accidental loss, destruction or damage.[123] Such measures include[124]:

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

State of the art of technology, the scope of processing, costs and risks associated with it can be taken into account when determining and implementing the appropriate measures.[125]

Accountability: The principle of accountability refers to the data controller's obligation and responsibility to ensure compliance with the five principles described above. Data controllers should consider whether the processing activities comply with them and take the relevant technical and organisational measures. For instance, the data controller can demonstrate compliance by keeping records of processing activities and carrying out Data Protection Impact Assessment.

5.3 An Overview of Personal Data in CoRoSect

5.3.1 Processing Employee Data

As CoRoSect will be tested and used in the working environments, employees of the end-users are expected to be in the closest proximity to the developed tools and technologies. Therefore, any potential data protection impacts of the CoRoSect closely relates to the employees of the end-users. It has been long established in European law and jurisprudence that employees enjoy the protection

[118] Art. 89(1), GDPR.
[119] Art. 5(1)(c), GDPR.
[120] Recital 39, GDPR.
[121] Art. 5(1)(d), GDPR.
[122] Art. 5(1)(d), GDPR.
[123] Art. 5(1)(f), GDPR.
[124] Art. 32, GDPR.
[125] Art. 25(1), GDPR.

afforded by data protection law.[126] In the private sector, processing activities carried by employers in relation with their employees' personal data are governed by the general provisions of GDPR, except where GDPR or a national law in the country in which the relevant consortium partner operates provide a special provision.[127] Therefore, collective labour contracts that include data protection clauses or other form of documents (e.g. consent forms) allowing the processing of personal data of employees should comply with the rules on European level, on the one hand, and with the national laws on the other.[128]With a view of the employment context and key issues and examples surrounding the working environment, WP29 Working Party provides guidance concerning the processing of personal data at the workplace in a legal and proportionate manner, which are applicable to all kinds of employment relationship, regardless of its nature (be it based on employment contract, freelance or another form)[129]. Rapid technological developments enable news forms of data processing activities, including systematic and intrusive forms of data processing, creating new types of risks and challenges to the data protection framework in the employment context.[130]

New technological devices and tools make it possible to collect and process data in less overt ways in comparison with traditional tools that can be more visible to its surroundings.[131] Data collected by a visibly seen camera in the entrance of a workplace, for instance, can be better anticipated compared to location data constantly collected through a smart device. Unawareness, among employees, regarding the nature and purpose of such tools and devices would put the **fairness** of the data processing at risk. This is why, it is of utmost importance to comply with the **transparency** principle, which requires, among others, informing data subject whether processing takes place and how and why it is carried out.[132] Personal data should be processed in a fair manner, finding a balance between the interests pursued by the employer- which may include economic interest- and the rights of the data subject, in this case, the employee. In addition, technological devices provided to the employees should follow data protection by design and by default principle.[133] The impacts of the tools and devices that will process the employees' personal data should be assessed by carrying out a Data Protection Impact Assessment.[134]

In addition to the above-mentioned challenge posed by new technologies, the very nature of employment relationship may create a challenge for the application of data protection rules and principles. In traditional labour law perspective, the relation between employer and employee is the one between a subordinate and superordinate, resulting from the economic imbalance between two

[126] *Niemietz v. Germany*, No. 13710/88, 16 December 1992 (ECtHR); *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007; 6 CJEU, C-342/12, Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), 30 May 2013, p. 19.

[127] Art. 88, GDPR; Art. 9(2)(b) of GDPR provides such provision which allows employers to process sensitive data of their employees (such as health data or biometric data used to uniquely identify an individual) in order to fulfil their legal duties as an employer (e.g. social security).

[128] Osborne Clarke, GDPR and "consent" in employment contracts: employers must take a new approach' https://www.osborneclarke.com/insights/gdpr-and-consent-in-employment-contracts-employers-must-take-a-new-approach, accessed 7 December 2021.

[129] Art29WP 'Opinion 2/2017 on data processing at work at Work' (2017) 17/EN WP 249, p. 4.

[130] Hendrickx F, 'Privacy 4.0 at Work: Regulating Employment, Technology and Automation' (Regulating for Globalization, 23 September 2019) http://regulatingforglobalization.com/2019/09/23/privacy-4-0-at-work-regulating-employment-technology-and-automation/ accessed 19 November 2021.

[131] Art29WP 'Opinion 2/2017 on data processing at work at Work' (2017) 17/EN WP 249.

[132] Council of Europe, Committee of Ministers (2015), Recommendation Rec(2015)5 to member states on the processing of personal data in the context of employment, April 2015, para. 10; WP29 'Opinion 2/2017 on data processing at work at Work' (2017) 17/EN WP 249, p. 8.

[133] Art29WP 'Opinion 2/2017 on data processing at work at Work' (2017) 17/EN WP 249, p. 8.; Art. 35, GDPR.

[134] Art29WP 'Opinion 2/2017 on data processing at work at Work' (2017) 17/EN WP 249, p. 8.

sides, as well as the legal authority exercised by the employer over the employee.[135] Therefore, the application and interpretation of certain rules and principles of GDPR in the employment context may require special attention. This is, for instance, the case when an employee agrees to the processing of personal data through a consent form or a contract. As explained further below, GDPR requires that data processing is lawful, i.e. it has a legal basis. Consent is one of such legal basis. However, it is questionable whether employees can give their consent freely for the processing activities at the workplace. Due to the implicit dependency of the employee to the employer, employee may feel obliged to give consent or agree to the employment contract that bundles data protection clauses and other unrelated clauses, which opens the question of whether employee's consent is ''free'', and therefore valid.[136] The answer to this question and other employment-relevant issues are addressed in the relevant sub-sections below.[137]

5.3.2 Image and Video Recordings

CoRoSect is expected to collect video recordings demonstrating individuals performing a task in order to train AI-models that will perform the same task, as well as collecting data through sensors and robots in order to detect and recognize objects and human actions in order to handle insect farm operations.[138] Where video recordings, including images and sound, relate to an identified or identifiable individual, they fall under the definition of personal data, meaning that they should be collected and processed in accordance with the data minimisation principle and other data protection principles described in this deliverable.

Due to the potentially intrusive nature of video images and the risks involved with them, Article 29 Working Party and its successor, EDPS, separately addressed in their opinions and guidelines key issues regarding the application of data protection law to video recordings.[139] Even when video recordings are lawfully collected for a legitimate purpose, their availability makes them prone to the risk of misuse and further use for initially unexpected purposes, which calls for careful consideration of their use in a GDPR-compatible manner.[140]

The use of image and video recording techniques and its compatibility with GDPR is especially pertinent in the employment environment. The issue has been addressed in the context of continuously monitoring the behaviour of employees and video surveillance in the workplace through devices such as CCTV cameras. Video surveillance systems aimed directly at controlling the performance at work is, as a matter of principle, prohibited.[141] Monitoring the facial expressions of employees are likewise considered unlawful.[142] Labour laws in each country may have additional rules or safeguards.

[135] EU Agency for Fundamental Rights, Handbook on European Data Protection Law, Luxembourg, Publications Office of the European Union, 2018.
[136] See Osborne Clarke, GDPR and "consent" in employment contracts: employers must take a new approach' https://www.osborneclarke.com/insights/gdpr-and-consent-in-employment-contracts-employers-must-take-a-new-approach, accessed 7 December 2021.
[137] See below 5.4.
[138] See particularly WP5 and WP8.
[139] Article 29 Data Protection Working Party, 'Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance' (2004); EDPB, Guidelines 3/2019 on processing of personal data through video devices' (2019).
[140] EDPB, Guidelines 3/2019 on processing of personal data through video devices' (2019), p.4
[141] Art29WP Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance p.25.
[142] Art29WP 'Opinion 2/2017 on data processing at work at Work' (2017) 17/EN WP 249, p.19.

5.3.2.1 Nature of Data

Regarding the nature of data, it should be noted that even if a video image is not viewed or used to identify a natural person or it was viewed by not recorded, it can still be considered personal data. The identifiability element of personal data implies the possibility of identification rather than an actual identification. For instance, further information held by other persons can still make the identification a possibility.[143] However, this possibility is limited to the ''means reasonably likely to be used'' in all circumstances.[144] When cameras attitude or angle does not allow identifying natural persons or the costs and technical capacity necessary for identification are beyond what are reasonable to use, data collected can be considered as non-personal.

If the personal data collected through visual image also constitute a special category of data, the processing can be carried out only under exceptional circumstances described under Article 9(2) of GDPR (including explicit consent or employer's legal obligations). Special categories include biometric data processed ''for the purpose of uniquely identifying'' a person such as fingerprints, voice or face recognition. As the wording suggests, visual image or voice data can be considered as sensitive data, depending on the context in which they are used. One of the recitals of GDPR clarifies that photographs are considered as biometric data only when they are subject to a special technique in order to find out the identity of the person in the photograph.[145] As a consequence, visual images or voice are not automatically considered as sensitive.[146]

5.3.2.2 Necessity

Once it is deemed that personal data may be collected through video devices, cameras or other similar devices, it should be assessed, in light of the data minimisation principle, whether the use of video recordings are **necessary** to achieve the targeted purpose, and the recordings should be processed for that particular purpose.[147] This involves the examination of whether there are other means that can be used to achieve the same goal, which would be less intrusive to the data subject's rights and interests.[148] Video images relating to individuals should be an option if the purpose of the processing cannot be reasonably fulfilled by other means. For instance, if a car's video camera that assists in parking can be designed in a way that it does not collect information about other individuals (such as the licence plate of another car), the preference should be given to design it in that way. Similarly, the possibility to use an anonymised version of images and recordings can be explored.

Where personal data needs to be collected, and anonymisation is not possible, techniques used to record and process videos and images of individuals are subject to other guarantees, such as securing data with pseudonymisation or encryption, applying storage limitation and fulfilling data subject's access rights.

5.3.3 Connected Devices for Human-Machine Interaction

In order to enable a human-robot collaborative working environment, CoRoSect is expected to explore the use of augmented reality or virtual reality-based connected devices such as wearable glasses and gloves. Such devices will provide information to provide human input to AI-based systems or enable human-robot interaction. In case information collected and processed through such devices such as visual and haptic information relating to an identifiable person, it will be qualified as personal data,

[143] Article 29 Data Protection Working Party, 'Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance' (2004), p. 15.
[144] See above 4.2.1.
[145] Recital 51, GDPR.
[146] EDPB 'Guidelines 02/2021 on virtual voice assistants' (2021), p. 23, see footnote 31.
[147] For legally accepted purposes, please see below 4.3.
[148] EDPB, Guidelines 3/2019 on processing of personal data through video devices' (2019), p.8.

triggering the application of GDPR. This may be the case when collected data include audio and video material, location, data received from the computer of an identified individual, as well as when such information are stored and transferred to other persons (such as service providers or device manufacturers).

On the one hand, connected devices used in a business context can provide benefits in terms of employee safety, productivity and production efficiency.[149] On the other hand, connected devices interacting with other devices and systems enable collecting, processing, storing and transferring an extensive amount of data, making them ''pervasive'' and ''ubiquitous''.[150] Because of the ability of connected devices to collect and share data in a manner that may not be obvious to the data subject, European independent bodies pointed out the challenge they pose for data subject's control over his or her data[151]. Lack of transparency in the collection and processing of personal data may result in a situation where ''the user can lose all control on the dissemination of his/her data''.[152]

Further, the availability of mass amount of data collected through connected devices makes it possible to process them for further purposes, which were not initially expected or foreseen by the data subject.[153] This may be the case, for instance, when data collected for ensuring network security is further used to evaluate the performance of employees or shared with third parties. In accordance with the purpose limitation principle, data can be processed for a secondary purpose if this purpose is compatible with the initial purpose. Otherwise, processing of the same data for secondary purposes would be treated as a new processing activity, which should have its own legal basis.[154] If the secondary processing does not have a legal basis, the processing would be unlawful even if the initial collecting and processing were lawful. Connected devices are also subject to other principles, such as applying technical and organisational measures for data security.

5.4 Finding a legal basis for Collecting, Processing and Using Personal Data in CoRoSect

In line with the principle of lawfulness, personal data should be based on one of the six legal grounds enshrined under Art. 6(1) of GDPR. If the processing involves the so-called sensitive data, the processing is possible under a number of exceptional conditions prescribed under Art 9(2) of GDPR. Processing activities in CoRoSect project is expected to fall under one or more legal grounds in Art. 6(1), which are further explained below.

5.4.1 Consent

Consent is one of the potential legal basis that may be relied on for lawful processing of personal data in CoRoSect. Consent shows agreement of the data subject to the processing of her personal data, and can manifest itself by a statement or a clear affirmative action of the data subject. Rationale behind obtaining consent is to give individuals the opportunity to exercise control over their personal data,

[149] EDPS 'Technology report No 1 Smart glasses and data protection' (2019), p. 9.
[150] Art29WP, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (2014) 14/EN WP 223, p. 4.
[151] EDPS 'Technology report No 1 Smart glasses and data protection' (2019); EDPB 'Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications' (2021) and WP29, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (2014) 14/EN WP 223, p. 6.
[152] Art29WP, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (2014) 14/EN WP 223, p. 6.
[153] *Ibid*, p. 7.
[154] See below 4.3.

determining whether or not data relating to them can be used by others.[155] To make the control over data a reality, the formality of obtaining consent should reflect the real intent of the data subject and not just an ''illusory'' one.[156] The control over one's data cannot be exercised in a meaningful way if data subject is not given a real choice to reject the processing or is under direct or indirect pressure. A valid consent meets the following qualities:

- freely given;
- specific;
- informed;
- unambiguous.

5.4.1.1 Challenges to Consent

5.4.1.1.1 Free consent

For consent to be considered freely given, data subject should have a genuine or real choice, and should be able to refuse or withdraw consent without facing any repercussions.[157] In the AI context, one may wonder whether data subject can generally consent to the processing of her personal data through AI-based applications or through the use of data analytics. Free consent implies the granularity of consent, in other words, the ability to provide separate consents to a different type of processing activity.[158] Data subject should be able to separately consent (or not consent) ''essentially different kinds of AI-based processing''.[159] This may be the example of processing the same data to provide different type of advertisements to the data subject.

Similarly, data subject's freedom to make a choice might be impaired if consent is a **pre-condition** to have access to a service or a contract, although it is not necessary for the provision of such a service or performance of the contract. In such a case, consent should be obtained separately rather than as an integral part of a contract.[160]

Free choice of a data subject may also be affected in case of **power imbalance** between the data subject and the controller. In the employment context, such power imbalance can be considered to exist between the employer and the employee because the latter may feel unable to refuse giving consent, fearing any potential negative consequences. For this reason, EDPB finds it unlikely that employees can consent freely to the processing of their personal data by their employers in most cases.[161] Nevertheless, it acknowledges that employees' consent can be exceptionally considered valid, where consenting or not consenting ''will have no adverse consequences at all[.]''[162] Therefore, in case the employees of some of the consortium members will, for instance, participate in the pilots, consortium members should make sure that no adversary consequence is attached for not consenting or not participating. If consent is not seen as a viable legal basis for a particular processing activity, consortium members should not rely on consent and find another legal basis to rely on, such as a legal obligation or legitimate interests.

[155] Art29WP, 'Guidelines on consent under Regulation 2016/679' (2017) 17/EN WP259, p. 3.
[156] *Ibid*.
[157] Recital 42, GDPR.
[158] Recital 43, GDPR.
[159] European Parliamentary Research Service 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020), p. 43.
[160] Recital 43, Art. 7(4).
[161] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (2020), p. 9.
[162] *Ibid*., Art29WP 'Opinion 2/2017 on data processing at work at Work' (2017) 17/EN WP 249, p. 23.

The assessment of the validity of the employee's consent is a highly context- specific one. EDPB provides the below example of a situation in which employees can freely consent[163]:

Example: ''A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming.''

Consortium members should assess whether they can process their employees' data based on consent in the context of the circumstances surrounding the particular processing activities. Video recordings for a limited time with appropriate safeguards would be expected to be assessed differently than a technological tool that systematically monitors the behaviour of the employees for a longer period of time. If consent is not a viable option, another legal ground should be relied on.

5.4.1.1.2 Specific Consent

Consent should be given for a specific purpose described to the data subject clearly and unambiguously. If personal data will be processed for more than one purpose, every single processing activity should be explicitly indicated to the consenting data subject.[164] The requirement of specificity may limit the possibility of further processing of data through AI-based applications or connected devices, for example data analytics, unless it was explicitly consented.[165] If processing activities change in a way that would be unexpected to the data subject, a new consent for the changed purpose should be obtained.

5.4.1.1.3. Unambiguous Consent

Unambiguous consent manifests itself in a way that it casts no doubt on the data subject's intention to consent. Use of default consent options (consent-based on silence) does not qualify as unambiguous.[166]

5.4.2. Contract

Contract can provide a legal basis where the processing of personal data is necessary to perform the contractual obligations or enter into a contract. As an example, a product purchase agreement can be relied on to process the purchaser's name, address and contact details to deliver the product. Similarly, an employment contract between employee and employer can provide a basis for data processing of the employee. In these examples, a relevant question would be whether entering into a contract to have access to a product or service can authorize the processing of personal data through AI-based applications relevant to access that product or service. While there is not a clear-cut answer to this question, the exact purpose of the contract plays an important and determinative role. European supervisory authorities interpret the performance of a contract strictly, excluding processing activities that are not ''genuinely''[167] necessary even if they are also included in the

[163] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (2020), p. 9.
[164] EU Agency for Fundamental Rights, Handbook on European Data Protection Law, Luxembourg, Publications Office of the European Union, 2018, p. 147.
[165] European Parliamentary Research Service 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020), p. 42.
[166] Art29WP, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (2014) 844/14/EN WP 217, p. 16.
[167] *Ibid*. See also EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (2020), p. 10.

contract. To give an example, setting up an automated database of employees' names and contact details could be considered as necessary for the performance of an employment contract, whereas video surveillance in the workplace may fail the necessity test depending on the factual circumstances.[168]

5.4.3. Compliance with a Legal Obligation

The controller, can lawfully process personal data to comply with a legal obligation stemming from national law or EU law.[169] This is the case, for example, when employers transfer their employees' personal data to public authorities to fulfil the requirements of tax or social security law. Especially in the context of cybersecurity law, EU or national laws may create legal obligations to implement security measures in certain sectors, which may be a basis for deploying technologies that process personal data to tackle cybersecurity risks. In case the users of the CoRoSect technologies can demonstrate that processing personal data is necessary to fulfil a legal obligation, they can rely on this basis.

5.4.4. Legitimate Interest

In the context of CoRoSect, the legitimate interests of the controller or of a third party may also provide a legal basis for the processing activities.[170] Controllers' interests can follow a public interest that benefits society or a private interest such as economic interest. The examples may include the interest of the employer to ensure monitoring health and safety in the workplace or to ensure physical security, IT and network security.[171] Because the processing activities also concern the fundamental rights and freedoms of the data subject, this legal ground requires balancing the interests of the controller against the interest of the data subject. Legitimate interests of the controller should be relied on only if they do not create excessive burden on the data subject.[172] The interests at stake are not comparable in a quantitative manner, which is why finding a balance is not an easy task.[173]

In assessing the interests of both sides, a variety of factors should be taken into account such as the nature of the controller's interest, impact on the data subject and the existence of appropriate safeguards (such as information provided to the data subject regarding processing activities).[174] Whether the processing for the controller's purposes is expectable for the data subject also plays a role in such an assessment.

5.4.5. Vital Interests

Processing of personal data is lawful if it is necessary to protect the interests of the data subject or of another natural person.[175] Recital 46 of the GDPR clarifies that the aim of this legal ground is to

[168] Art29WP, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (2014) 844/14/EN WP 217, p. 17.
[169] GDPR Art. 6(1)(c).
[170] Art. 6(1)(f), GDPR.
[171] Art29WP, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (2014) 844/14/EN WP 217, p. 24-25.
[172] In Google Spain case, economic interest of Google has not been accepted as a justification to not to delete the search results concerning data subject due to the serious consequences of profiling individuals through search engines to data subject's right to privacy and data protection. See CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014.
[173] Art29WP, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (2014) 844/14/EN WP 217, p. 23.
[174] Art29WP, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (2014) 844/14/EN WP 217, p. 23-43.
[175] Art. 6(1)(d), GDPR.

''protect an interest which is essential to the data subject's life'', implying that it is applicable in exceptional situations where the data subject's life or health is in danger.[176]

5.4.6. Public Task

Processing personal data to perform a task in the interest of the public is lawful, which is typically the case of public authorities (such as a tax authority or law enforcement).[177] Private enterprises authorized to perform a public task in an official capacity can also rely on this legal ground.

In the context of the CoRoSect project and the developed technologies, consent and legitimate interest are the most likely legal basis that can justify the processing of personal data. In case of a request from public authorities to have access to information, as in the case of tackling cybersecurity threats, the basis may also be legal obligation. Controllers processing personal data during the development or use of CoRoSect technologies should carefully assess which legal basis suits the best to the processing activity at stake. The question of which legal ground is the most suitable for a particular processing activity is context-dependent. Based on the nature and purpose of processing, and dataset involved, consortium members processing personal data should assess which legal ground is the most appropriate to rely on. It is possible that more than one legal ground can be applicable to a processing activity. It would be recommended to keep track of all information regarding all applicable grounds.

5.5 Rights of Data Subjects

To ensure the implementation of data protection principles in an effective manner, GDPR sets out a number of rights that can be claimed by data subjects. Data subject's rights aim to empower the individual relating to whom data is processed, granting them a way in which they can exercise control over their data. While GDPR sets the minimum threshold that should be respected at the EU level, each country may expand the protection afforded to individuals residing under their territory in their national laws.

5.5.1 Right to Be Informed

In order to ensure transparency of data processing, data subjects should be made aware of the fact that data relating to them is or will be collected and used. The principle of transparency implies the data subject's right to know who use their data for which purposes and through which mean. Therefore, data controllers have an obligation to inform data subjects regarding the processing activities with clear and plain language in an easily accessible and understandable format.[178] This is particularly important because non-compliance with this principle may hinder the data subject from exercising her other rights, such as the right to rectify or the right to object.[179]

Depending on how personal data is or will be received, data controllers should provide the data subject with a number of information. If personal information is collected **directly** from the data subject, the following information should be provided to the data subject **at the time when personal data are obtained**:[180]

- the identity and the contact details of the controller;

[176] Recital 46, GDPR.
[177] Art. 6(1)(e), GDPR.
[178] Article 12/1 and Recital 39, GDPR.
[179] CJEU, C-201/14, Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others, 1 October 2015.
[180] Art. 13, GDPR.

- the contact details of the data protection officer (if applicable);
- the purposes and legal basis of the processing;
- the legitimate interests pursued by the controller or by a third party (if applicable);
- the recipients or categories of recipients of the personal data;
- information on the transfer of personal data to a third country or international organisation;
- information regarding storage period;
- the rights of data subject;
- Information on whether the data subject is obliged to provide the personal data under a contract or a law;
- Information on automated decision-making, including profiling (if applicable).

If personal data is **not directly** obtained from the data subject, in addition to the above list of information, data subject should be provided with the categories of personal data collected and information on the source of personal data and whether it came from a publicly accessible source.[181]

In the CoRoSect project, individuals may directly provide their personal information to a partner in the consortium, for example this might be the case for those who will participate in the pilots. In this situation, the required information should be provided to the data subject providing the data at the time when personal data are obtained from data subject. On the other hand, the use of AI, robotics and connected devices may result in capturing data relating to individuals without their knowledge or intention. To ensure the effective use of the right to be informed during the project and any future use, the technology should be developed and used in a way that will enable controllers to properly inform data subjects about the processing of data relating to them.

5.5.2 Right to Access

Right to access entitles data subject to obtain from the controller information as to whether or not personal data relating to him or her are being processed, and, if any, information regarding the processing activities such as purposes of the processing, categories, sources and recipients of personal data, storage period and data subjects rights.[182] Data subjects have a right to receive a copy of the personal data undergoing processing.[183] It is an essential principle that empowers individuals to verify whether data concerning them are being processed lawfully.[184]

The right to access can be limited to a certain extent if its exercise would negatively affect trade secrets or intellectual property and especially the copyright protecting the software, although such limitations should not completely prevent data subjects from receiving information.[185]

The design of CoRoSect technologies should allow data controllers to respond to any potential information request by data subjects who wish to exercise their right to access protected by GDPR. Data controllers should be able to keep records about the data collected and processed relating data subjects and trace back any processing activity relating to a given individual.

[181] Art. 14, GDPR.
[182] Art. 15(1), GDPR.
[183] Art. 15(3), GDPR.
[184] Recital 63, GDPR.
[185] Recital 63, GDPR.

5.5.3 Right to Rectification

Data subject has a right to request from the data controller to rectify or complete any personal data relating to her. Right to rectification imposes an obligation on data controllers to rectify without undue delay the inaccurate personal data.[186]

5.5.4 Right to Erasure

In line with the data minimisation principle (requiring that no data that is more than necessary for the purpose of processing should be collected), data subject has a right to request from data controller to erase their own data under certain circumstances. For example, where the processing is based on the consent of data subject, and the data subject withdraws such consent, the data controller should delete the processed data unless there is another legal basis that can justify processing. Data controller is entitled to reject the request of erasure if one of the exceptions in GDPR applies.[187]

In the context of artificial intelligence, the question arises whether the request to erase the personal data used to train an algorithmic model imposes an obligation on data controller to also delete the personal data or group data (i.e. trained algorithmic model) that are **inferred** from such personal data. It has been noted that inferred personal data would fall under the obligation of erasure because it still qualifies personal data relating to a natural person. On the other hand, inferred group data do not trigger such obligation as ''data that are embedded in an algorithmic model are no longer personal''.[188]

5.5.5 Right to Restriction of Processing

Data subject has the right to restrict the processing of his or her personal data in one of the below situations:[189]

- The accuracy of the personal data is contested and needs to be verified;
- the processing is unlawful;
- data subject needs the personal data for the establishment, exercise or defence of legal claims;
- data subject has objected to the processing and the verification of the data subject's claims need to be made.

If processing is restricted, personal data can be still processed if data subject consents to it.[190] Data controller should inform the data subject before lifting the restriction of his or her data.[191] If the data in question was disclosed to third parties before its processing was restricted, data controller has an obligation to communicate the restriction to them. Data controller is disposed of this obligation if communicating with other parties is impossible or requires excessive effort.[192]

5.5.6 Right to Data Portability

Right to data portability entitles the data subject to receive his or her personal data from the controller in a structured, commonly used, and machine-readable format and have the data transferred to another controller.[193] However, data subject can exercise the right to data portability only when he or

[186] Art. 16, GDPR.
[187] Art. 17(3), GDPR.
[188] European Parliamentary Research Service 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020), p. 57.
[189] Art. 18, GDPR.
[190] Art. 18/2, GDPR.
[191] Art. 18/3, GDPR.
[192] Art. 19, GDPR.
[193] Art. 19(1) and (2), GDPR.

she knowingly provided the personal data to the controller in the form of consent or a contract, and the data is processed in an automated manner.[194] In other words, if the processing is based on another legal basis such as public interest or legitimate interests of the controller, data subject does not have the right to data portability. The right resembles the right to access, although the latter can be exercised in relation with all processing activities, regardless of their legal ground.

As the data portability concerns personal data which individual ''provided'' to a controller, data entered by the data subject, such as credentials or voice would fall under this right. However, in the context of processing through AI-based applications, there is uncertainty as to whether the right also covers the data collected by AI when tracking the data subject's activity or data inferred from the data entered by the data subject.[195] These uncertainties may create a challenge for the determination of the scope of the right to data portability in the development and the use of CoRoSect technologies. In any case, where consent or a contract forms the basis of processing, development of the technology should make it possible to provide the individuals with their data in a structured, commonly used, and machine-readable format.

5.5.7 Right to Withdraw Consent and Right to Object

Where the processing is carried out based on the consent of the data subject, data subject has a right to withdraw her consent at any time.[196] In all other cases, where processing has a legal basis different than consent, data subject can rely on her right to object to the processing. **Where data subject exercises this right, the controller should stop the processing of the personal data of the data subject objects to the processing.** Right to object does not grant the data subject a general right to terminate the processing in all circumstances. Data subject can request the termination of the processing carried out for direct marketing purposes, and the processing carried out in an automated manner in the context of information society services.[197] Data subject can also request to stop the processing carried out for scientific, historical, or statistical purposes as long as such processing is not necessary for the performance of a task carried out for reasons of public interest.[198] This means data subject can object to the processing for research carried out for private commercial purposes.[199]

Further, right to object can be claimed if personal data are processed for the performance of a task carried out in the public interest or the **controller's legitimate interest**. In this case, the data controller needs to weight the legitimate interests underpinning the processing activity against the interest of the data subject. **If the interests of the data subject prevail over the interest pursued by the controller, processing activities should be terminated.** Especially if the processing involves profiling of individuals, it would generally be more challenging to argue that a controller's interest to profile the individual would prevail over the data subject's rights due to the intrusive nature of profiling on the data subject's privacy and rights.

Where consortium members process personal data during the pilots or other research activities based on consent, they should facilitate the exercise of the right to withdraw the consent upon the request of the data subject.

[194] Art. 19(1), GDPR.
[195] European Parliamentary Research Service 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020), p. 57.
[196] Art. 7(3), GDPR.
[197] Art. 21, GDPR.
[198] Art. 21/6, GDPR.
[199] European Parliamentary Research Service 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020), p. 59.

5.5.8 Right not to Be Subject to Automated Individual Decision-Making

Article 22 of GDPR introduces the data subject's right ''not to be subject to a decision based solely on automated processing, which produces legal effects concerning him or her or similarly significantly affects him or her'' (profiling, analysis of behaviour or work performance). The provision sets out a general prohibition of fully automated processing, except when there is explicit consent, the necessity for a performance of a contract to which data subject is party or a legal basis under EU or national law.[200] Decision-making based on solely automated means are subject to measures and safeguards of data subjects' rights such as 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.[201]

5.6 International Data Transfers

As indicated in **D1.1 Ethical and Legal Framework: Initial Assessment Report**, international transfers are restricted to a number of occasions in EU law and are subject to the conditions prescribed under GDPR. Transfer from European Economic Area (EEA) members to non-EEA members will be handled in accordance with GDPR.

In the context of any potential personal data transfers from CoRoSect members established in the EU to Norway and Serbia, it is worth referring to the explanation made in **D1.1 Ethical and Legal Framework: Initial Assessment Report**:

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).

FSH, the only consortium partner established in Serbia, is involved in the dissemination, communication and community building activities in accordance with the project's D11.9 Data Management Plan and through the direct involvement of its Data Protection Officer (DPO) in the project. As of 17 November 2021, KU Leuven has been informed that the Consortium does not expect to transfer any datasets involving personal data to FSH. The consortium is aware that in case of any transfer to third countries, it should be ensured that the data subject will be sufficiently protected by the recipient.

5.6.1 Update Regarding the United Kingdom

With regards to the United Kingdom, **D1.1 Ethical and Legal Framework: Initial Assessment Report** noted that the draft adequacy decisions concerning transfers from EU to the UK are in the process of approval. In fact, on 28 June 2021, EU Commission published adequacy decisions in respect of the UK, finding the UK provides adequate protection for personal data transferred from the EU to the UK under the EU GDPR.[202] This means that transfer of personal data to the UK can take place based on

[200] Art. 22(2), GDPR.
[201] Art. 22(3), GDPR.
[202] Information Commissioner's Office, What is adequacy? <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/adequacy/> accessed 19 November 2021.

these adequacy decisions. The so-called adequacy decisions are expected to be valid until 27 June 2025. They will expire on this date, unless the European Commission will extend them.

6 Conclusion

Building upon D1.1 Ethical and Legal Framework: Initial Assessment Report, this report specified the legal and ethical framework applicable to the development and use of CoRoSect technologies. The challenges arising from factors such as data quality, biased training data and safety deficits make AI systems vulnerable to risks. This report identified the potential risks to workplace safety, workers' physical safety and integrity, privacy and data protection. It further suggested technical and non-technical measures that can be implemented by the members of the CoRoSect consortium to ensure the mitigation of these risks. The recommendations and suggestions in this report will guide the development of the CoRoSect technologies and will provide a basis to further evaluate the implementation of the requirements in the next phases of the project.

Technologies developed by the CoRoSect project will constitute the pieces of equipment that will be used in the insect farm premises in the production and handling of insects. This cutting-edge equipment will be important tools to carry out the management procedures and decision-making in the production practices, feeding, watering and measuring the environmental conditions such as temperature, humidity and light. They should be therefore designed in a manner that they ensure that the insect producers can comply with their obligations regarding health and workplace safety, food and feed safety, animal wellbeing and data protection. The development of legally and ethically compliant, robust AI and robotics is important to ensure that unforeseen risks to food and feed hygiene, workers' privacy and occupational risks are prevented and insect production practices are managed in an appropriate manner.

It should be noted that the implementation of the identified ethical and legal requirements is a continuous process. It must start in the development phase and continue through the usage period. At this point, a rigorous analysis of the requirements must be conducted and re-designing possibilities must be considered if it is necessary. The highly skilled technical teams and organisational arrangements will play a crucial role in the implementation and evaluation of the mitigation measures.

References

Legislation/Proposals/Communication

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391

Commission Implementing Regulation (EU) 2016/1141 of 13 July 2016 adopting a list of invasive alien species of Union concern pursuant to Regulation (EU) No 1143/2014 of the European Parliament and of the Council C/2016/4295, *OJ L 189, 14.7.2016*

Commission Regulation (EU) 2021/382 of 3 March 2021 amending the Annexes to Regulation (EC) No 852/2004 of the European Parliament and of the Council on the hygiene of foodstuffs as regards food allergen management, redistribution of food and food safety culture (Text with EEA relevance)

C/2021/1312, *OJ L 74, 4.3.2021*

Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM(2019) 250 final

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Building Trust in Human-Centric Artificial Intelligence Brussels, 8.4.2019 COM(2019) 168 final

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: Artificial Intelligence for Europe Brussels, 25.4.2018 COM (2018) 237 final

Consolidated text: Regulation (EU) 2016/429 of the European Parliament and of the Council of 9 March 2016 on transmissible animal diseases and amending and repealing certain acts in the area of animal health (Animal Health Law)

Council Directive 98/58/EC of 20 July 1998 concerning the protection of animals kept for farming purposes *OJ L 221, 8.8.1998*

Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)

Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety OJ L 11, 15 January 2002

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

Proposal for a Regulation of the European Parliament and of the Council on Machinery Products COM/2021/202 final

Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 Final

Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety, *OJ L 31, 1.2.2002,* p. 1–24

Regulation (EC) No 183/2005 of the European Parliament and of the Council of 12 January 2005 laying down requirements for feed hygiene (Text with EEA relevance), *OJ L 35, 8.2.2005*, p. 1–22

Regulation (EC) No 1069/2009 of the European Parliament and of the Council of 21 October 2009 laying down health rules as regards animal by-products and derived products not intended for human consumption and repealing Regulation (EC) No 1774/2002 (Animal by-products Regulation) *OJ L 300, 14.11.2009*, p. 1–33

Regulation (EU) 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, 28.11.2018

Articles and others

Anderson M, *Machine Ethics* (CUP, 2011)

Art29WP, 'Guidelines on consent under Regulation 2016/679' (2017) 17/EN WP259

Art29WP, ‘Opinion 05/2014 on Anonymisation Techniques’ (2014) 0829/14/EN

Art29WP, ’Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC’ (2014) 844/14/EN WP 217

Art29WP, ‘Opinion 1/2010 on the concepts of “Controller” and “Processor”’ (2010) 00264/10/EN

Art29WP,’Opinion 2/2017 on data processing at work at Work’ (2017) 17/EN WP 249

Art29WP, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance

Art29WP, ‘Opinion 4/2007 on the concept of personal data’ (2007) 01248/07/EN

Art29WP, ’Opinion 8/2014 on the on Recent Developments on the Internet of Things’ (2014) 14/EN WP 223

Comiter M, ‘Attacking Artificial Intelligence: AI’s Security Vulnerability and What Policy Makers Can Do About It’, (2019) Harvard Kennedy School Working Paper, < https://www.belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf> accessed 15 October 2021.

Cavoukian A, *Privacy by Design*, Leading Edge, IEEE Technology and Society Magazine, 2012, 31/4.

Council of Europe, Committee of Ministers (2015), Recommendation Rec(2015)5 to member states on the processing of personal data in the context of employment, April 2015

De Bruyne J and Valeenhove, Artificial *Intelligence and the Law* (Intersentia, 2021).

Devitt J, Insects and Ethics, <https://aucklandecology.com/2017/04/29/insects-and-ethics/> accessed 19 November 2021

EDPB ’Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications’ (2021)

EDPB ‘Guidelines 02/2021 on virtual voice assistants‘ (2021)

EDPB, ‘Guidelines 05/2020 on consent under Regulation 2016/679’ (2020)

EDPB, ’Guidelines 3/2019 on processing of personal data through video devices’ (2019)

EDPB, ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default’ (2019)

EDPS ’Technology report No 1 Smart glasses and data protection’ (2019)

European Commission, Animals used for scientific purposes <https://ec.europa.eu/environment/chemicals/lab_animals/index_en.htm> accessed 19 November 2021

European Commission, Farm to Fork Strategy, <https://ec.europa.eu/food/horizontal-topics/farm-fork-strategy_en> accessed 19 November 2021

European Commission, Free flow of non-personal data, Available at: https://digital-strategy.ec.europa.eu/en/policies/non-personal-data accessed 21 October 2021.

European Commission, High-level Expert Group on Artificial Intelligence, <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai> accessed 1 September 2021.

European Commission, 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 19 November 2021

European Commission, White Paper on food safety, <https://op.europa.eu/en/publication-detail/-/publication/6d4b523b-dad8-4449-b2b4-9fa9b0d6e2be/language-en> accessed 19 November 2021

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

European Parliamentary Research Service 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020)

Finck M and Pallas F, 'They Who Must Not Be Identified—Distinguishing Personal from NonPersonal Data under the GDPR' (2020) 10 International Data Privacy Law, p. 11-12.

Fischer B and Larson BMH, 'Collecting insects to conserve them: a call for ethical caution, Insect Conservation and Diversity' (2019) 12 Insect Conservation and Diversity 173

Hamon R, Junklewitz H and Sanchez Martin JI, Robustness and Explainability of Artificial Intelligence, (Publications Office of the European Union, 2020)

Hendrickx F, 'Privacy 4.0 at Work: Regulating Employment, Technology and Automation' (Regulating for Globalization, 23 September 2019) http://regulatingforglobalization.com/2019/09/23/privacy-4-0-at-work-regulating-employment-technology-and-automation/ accessed 19 November 2021

HLEG AI, Ethics Guidelines for Trustworthy AI, 8 April 2019, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419> accessed 19 November 2021

IBM, Everyday Ethics for Artificial Intelligence (IBM, 2019) <https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf>, accessed 10 October 2021

International Platform of Insects for Food and Feed (IPIFF), Ensuring High Standards of Animal Welfare in Insect Production, <https://ipiff.org/wp-content/uploads/2019/02/Animal-Welfare-in-Insect-Production.pdf> accessed 19 November 2021

International Platform of Insects for Food and Feed (IPIFF), Guide on Good Hygiene Practices, <https://ipiff.org/wp-content/uploads/2019/12/IPIFF-Guide-on-Good-Hygiene-Practices.pdf> accessed 19 November 2021, p. 35

Lin P, Abney K, Bekey AG, *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press, 2014)

Microsoft, Putting Principles into Practice, <https://www.microsoft.com/en-us/ai/our-approach?activetab=pivot1%3aprimaryr5> accessed 10 October 2021

National Institute for Occupational Safety and Health, Warehouse Worker Crushed by Forks of Laser Guided Vehicle (Washington State Face Program, 2018) <https://elcosh.org/record/document/4342/d001598.pdf> accessed 1 October 2021.

Ohm P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 UCLA Law Review 1701.

Osborne Clarke, GDPR and "consent" in employment contracts: employers must take a new approach' <https://www.osborneclarke.com/insights/gdpr-and-consent-in-employment-contracts-employers-must-take-a-new-approach>, accessed 7 December 2021.

Redelinghuys AJH, Basson AH and Kruger K, 'Cybersecurity Considerations for Industry 4.0' (International Conference on Competitive Manufacturing, February 2019).

Stalla-Bourdillon S and Knight A, 'Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2016) 34 Wisconsin International Law Journal 284.

Yaacoub JPA, Noura HN, Salman O and Chebab A, 'Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations' (2021) International Journal of Information Security Mar 19: 1-44

Wilkins DB, *Animal Welfare in Europe: European Legislation and Concerns* (Kluwer Law International, 1997)

Case Law

CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014

CJEU, C-201/14, Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others, 1 October 2015

CJEU, C-342/12, Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), 30 May 2013.

CJEU, C-582/14, Patrick Breyer v Bundesrepublik Deutschland, 12 May 2016

Copland v. the United Kingdom, No. 62617/00, 3 April 2007

Niemietz v. Germany, No. 13710/88, 16 December 1992 (ECtHR)

CoRoSect

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