D1.3 : Ethical and Legal Monitoring 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)	Burcu Yasar, Bengi Zeybek, Halid Kayhan
Contributor(s)	Kostantinos Stavridis, Panagiotis Zaparas, Rico Möckel, Nicolas Caussanel, Harri Määttä, Aleksandra Tolmačev, Lord Berko, Marc Bosch, Maria Aleksandrova, Jose Ramon Martinez
Work Package	WP1
Delivery Date (DoA)	31/03/2023
Actual Delivery Date	31/03/2023
Abstract:	This deliverable explains the methodology for the monitoring and evaluation of CoRoSect research and technologies. It also provides an understanding on the selected concepts that are relevant for the project. In addition, the deliverable provides an update on the recent developments in the EU law concerning the agriculture technologies.

Document Revision History			
Date	**Version**	**Author/Contributor/ Reviewer**	**Summary of main changes**
17/02/2023	V1	Burcu Yasar	Initial table of content
09/03/2023	V1	Burcu Yasar, Bengi Zeybek, Halid Kayhan	Substantial content
14/03/2023	V2	Ana Maria Corrêa	Review and editing
17/03/2023	V2	Burcu Yasar	Editing
24/03/2023	V3	Konstantinos Stavridis, Jarkko Niemi	Review
29/03/2023	V4	Burcu Yasar	Incorporation of feedback

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

Funding Scheme: Innovation Action (IA) ● Topic: H2020-ICT-46-2020

Start date of project: 01 January, 2021 ● Duration: 36 months

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

Table of Contents

List of figures

List of Abbreviations and Acronyms	
AI	Artificial Intelligence
AI HLEG	High-Level Expert Group on Artificial Intelligence
ALTAI	Assessment List on Trustworthy Artificial Intelligence
CI	Critical Infrastructures
CSIRT	Computer security incident response teams
DPIA	Data Protection Impact Assessment
ECI	European critical infrastructures
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
ICO	UK Information Commissioner's Office
NIS	Network Information Systems
NIS2	Amended version of the Network and Information Services Directive
OES	Operators of essential services
WP	Work Package

Executive Summary

This deliverable explains the methodology for the monitoring and evaluation of CoRoSect research and technologies. Given some of the components of the project process personal data, and involve the development of artificial intelligence and machine learning techniques, the methodology reflects the elements of impact assessment related to data protection and artificial intelligence ethics. While doing so, this deliverable takes some of the deficiencies of the existing methodologies into account, and aims to improve it by addressing these deficiencies. Furthermore, this deliverable provides a deeper understanding on the concept of accuracy, which has a particular relevance to the project to ensure that robots work in collaboration with humans accurately, and insects are handled efficiently. In addition, the deliverable reflects very recent developments in the EU in the area of cybersecurity in the agriculture sector. It finds that these new adopted initiatives do not directly apply to the CoRoSect research, nevertheless it has a potential to apply to some end-users when the final product is put in the market.

1 Introduction

CoRoSect research develops technologies to enable efficient, safe, legally and ethically compliant technologies for human-robot collaboration. This deliverable aims to explain the methodology for the monitoring and evaluation of CoRoSect research and technologies. Some of the components of the project process personal data and involve the development of artificial intelligence and machine learning techniques. For that reason, impact assessment relating to the processing of personal data (i.e. Data Protection Impact Assessment), and ethics guidelines for Trustworthy AI have been chosen to establish a monitoring and evaluation methodology. The second chapter of this deliverable explains the methodology, as well as the monitoring survey created as part of CoRoSect research.

In addition, this deliverable provides a deeper understanding some of the selected concepts that have particular importance and relevance for the CoRoSect project. The third chapter focuses on the accuracy in the context of human-robot collaboration technologies. It provides obligations of AI producers and organizational guidelines. The fourth chapter focuses on the cybersecurity in the agriculture sector. It reflects the important legislative developments in the EU introduced after the delivery of the previous deliverables of T1.1, and it discusses the relevant of these legislative developments for the CoRoSect research and its end-users.

2 Methodology for a technology impact assessment in insect farms

This Chapter explains the methodology of the monitoring and evaluation of CoRoSect technologies. Previous work has shown that some CoRoSect components need to process personal data for the research conducted as part of the project.[1] In addition, the project involves the development of artificial intelligence and machine learning techniques. Information on the definition of personal data, and the legal and ethical requirements can be found in D1.1 ad D1.2.

[1] CoRoSect D1.1 Ethical and Legal Framework: Initial Assessment Report, D1.2 Ethical and Legal Requirements Specification Report, and D11.9 Data Management Plan (revised).

As a result, impact assessment relating to the processing of personal data (the so-called Data Protection Impact Assessment), and ethics guidelines for Trustworthy AI have been chosen as methodologies for the purpose of CoRoSect research. The first sub-chapter focuses on the Data Protection Impact Assessment (DPIA), and the second sub-chapter focuses on the ethics assessment. The third chapter focuses on the monitoring survey developed as part of the CoRoSect research.

2.1 Data Protection Impact Assessment

DPIA is a risk management tool that was introduced in data protection law with GDPR. The concept of risk is at the heart of the data protection law. Article 35 of GDPR states that is necessary to conduct an impact assessment if the processing is 'likely to result in a high risk to the rights and freedoms of natural persons'. Article 25 of the GDPR data protection-by design obligation requires to take into account the 'risks of varying likelihood and severity for rights and freedoms of natural persons'. Thus, the first thing that is relevant for any attempt of processing personal data is to find out what risk(s) this would entail. The determination of risks is central to the performance of key data protection obligations.

2.1.1 The concept of risk

EU data protection law follows a risk-based approach. Risk is an abstract and vague concept which can be interpreted in different ways.[2] The GDPR does not provide a definition of risk, nor does it specify a risk model. Instead, it generally states that the risk assessment should be an objective one. It also states that the likelihood and severity of the risk should be determined by keeping the nature, scope, context and purposes of the processing in mind.[3]

The ordinary meaning of the term risk refers to a 'possibility of something bad happening'.[4] A definition can be found in risk management standards. ISO defines risk as a either positive or negative 'effect of uncertainty on objectives'.[5] The concept also finds its place in the field of cybersecurity. NIS (2) Directive defines risk as 'the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident'. In data protection context, Article 29 Working Party defines risk as "a scenario describing an event and its consequences, estimated in terms of severity and likelihood".[6]

Hence, risk has (i) a various degree of possibility of occurrence, (ii) has a various degree of magnitude or severity, (iii) has various consequences, which can be positive or negative, and which carry a various degree of severity and likelihood.[7] As such, risk has a broad meaning, which may cover a wide variety of concerns and issues. To better understand the concept of risk in the specific context of data protection, and how to assess it, let us turn to two foundational approaches to data protection, namely rights-based and risk-based approach.

[2] Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press, 2020) 27-28.
[3] Recital 76, GDPR.
[4] Cambridge Dictionary available at https://dictionary.cambridge.org/.
[5] ISO 31000 Risk management, See https://www.iso.org/iso-31000-risk-management.html/.
[6] Article 29 Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679" (2017) 6.
[7] Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press, 2020) 27-28.

2.1.2 Risk-based and right-based approach

Lynskey argues that a legal regime or system is a rights-based regime if there is at least one of the following conditions. First, the regime grants a fundamental right. Alternatively, the regime gives expression to a fundamental right, or is designed and interpretation are underpinned by a fundamental right.[8] She argues that EU data protection framework is a right-based regime because it fulfils both of these conditions, namely it grants rights to data subjects, and its design and interpretation are underpinned by the right to data protection.[9] This analysis is valid for the GDPR with the nuance that it has a dual character as it (also) clearly incorporates a risk-based approach.

Legal and social science scholars have questioned the meaning of a risk-based approach in data protection regime. Van Dijk et al. explain the inherent distinction between risks and rights stating that *'Rights and risks traditionally belong within different spheres of knowledge, practice, and social organisation. Rights typically belong to legal practices where they become articulated through legal concepts and procedures. Risks often belong to risk management practices, and are typically defined through scientific concepts of probability in dealing with the possibilities of futures events*.'[10] Conceptual differences between risk and rights create an apparent tension between risk-based and rights-based approach. The first is underpinned by the idea that different processing activities provide different level of harm to individuals. The solutions should then be adjusted to the level of harm. The right-based approach is underpinned by an opposing idea that the right to data protection should be protected irrespective of the harm.[11] In the words of Article 29 Working Party data protection regime should provide 'a minimum and non-negotiable level of protection for all individuals'.[12] Individuals are valued equally for having dignity and autonomy and enjoy the same level of fundamental rights, which are not part of a hierarchy.

Since the data protection law clearly incorporates both risk and right-based regime, the question arises on how the risk should be understood in a way that the risks posed by technologies to the fundamental rights can be assessed. One can speak of four different risk modalities.[13] (i) Government modality understands risks as a risk to (governmental) institution, and search for a trade-off between risks and individual rights (a typical example being security vs. privacy). (ii) Organisation modality sees rights as risk to the business assets since lack of privacy could bring damages to the trust and reputation of a business and tries to quantify the probability and likelihood of the occurrence of the risk. (iii) Legal (courts) modality's risk has two angles. First, the risks (to public interest) are understood as proportions that should be balanced against rights in accordance with the proportionality principle. Second, risk is understood as 'risk to the right', which emanates from a technological or other innovative development in society. The legal modality includes a substantial understanding of the right at stake, as well as a procedural understanding of what kind of a decision-making process was put in place to inform the decision of what risk is and how it should be handled. The legal modality creates a genuine link between risks and rights and feature a risk assessment that gives expression to the

[8] Orla Lynskey, *The foundations of EU data protection law* (Oxford University Press, 2015) 35-36.
[9] ibid. 35-45.
[10] Niels van Dijk, Raphaël Gellert, and Kjetil Rommetveit, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 Computer Law & Security Review 286, 289.
[11] Raphaël Gellert, 'Understanding the notion of risk' (2018) 34(2) Computer Law & Security Review 279.
[12] Article 29 Working Party, "Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)" (1998) 2.
[13] Niels van Dijk, Raphaël Gellert, and Kjetil Rommetveit, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 Computer Law & Security Review 286, 290-296.

exercise of data subject rights. It is complemented by (iv) civil society modality of risk, which reflects public's perception of whether rights are endangered at society, and includes public in decision-making processes on a wider societal level.

2.1.3 Risk in CoRoSect

CoRoSect project aims to establish a novel integrated cognitive robotic ecosystem, in which automated robotics systems will take over repetitive tasks that are also cognitively and physically demanding tasks during the insects' lifecycle. This will be developed as an environment where robots and humans will collaborate by carrying out different manipulation tasks. As the solutions that are being developed by CoRoSect consist of both human-robot collaboration schemes and sophisticated AI-based cognitive perception capabilities, both personal data processing and automated processing of personal as well as non-personal data will be required.

In particular, CoRoSect involves the following components and aspects[14]:

- **Environment analysis and registration for cognitive systems**: CoRoSect is developing an AI-enabled cognitive system with the capability of detecting and identifying insects on the surface/substrate. For this purpose, a deep learning-based analysis system is currently being developed.
- **Force-adaptive control for handling crates and insects**: CoRoSect research includes robotic components (such as M-Robot) that can autonomously learn to adapt to new situations, including handling insects and other materials without human intervention and improving their skills over time. Different machine learning and optimization techniques are being studied for this purpose.
- **Machines learning from human input**: Machine learning and optimization techniques are currently being developed with the aim of making robots learn from human input. Robots should either observe a human through a camera or be guided by humans on how to act. Robots, then, should be able to generalize the intention of humans to take such action and learn to do it by adjusting it to their own skills and capabilities.
- **Human-machine interactions with augmented reality (AR) for situation awareness and training**: To increase the safety of the workplace and the efficiency of human-robot collaboration, an egocentric task-depended dataset will be composed by using a wearable optical see-through device called HoloLens 2. This device worn by individuals will record different types of data such as audio, RGB-D, eye-tracking, hand-tracking and accelerometer, gyroscope and magnetometer values, and even heart rate or blinking rate. This dataset will allow the training of deep-learning models. The decision on the exact architecture of the optimal model to be used in the end-products, among other architectures, will be determined depending on the best overall accuracy in evaluating the attention levels of individuals that operate the HoloLens 2.

The relevant risks that should be examined in the context of CoRoSect are associated with privacy and data protection, workplace safety and security. Different levels of risks could arise depending on how technologies are developed and used. A detailed analyses of how and why these risks may emerge have been provided in previous deliverables of Task 1.[15]

[14] More information on these components can be found in Deliverables 12.3 and 12.4.

[15] CoRoSect D1.1 Ethical and Legal Framework: Initial Assessment Report, D1.2 Ethical and Legal Requirements Specification Report.

2.1.4. Article 35 GDPR

A DPIA does not need to be conducted for every processing activity but is required for certain processing activities. Article 35(1) states as follows.

'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.'

The main criterion is whether the processing is likely to result in a high risk to the rights and freedoms of individuals. The nature, scope, context, and purposes of the processing play a role in the determination of where there are high risks to individuals.

Article 35(3) GDPR provides a list of cases which the criterion for mandatory DPIA exist. The article indicates that the cases 'in particular' require a DPIA, thus the list is a non-exhaustive one. They can be extended to similar situations.

Article 35(3) provide the following examples:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
- processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences
- a systematic monitoring of a publicly accessible area on a large scale.

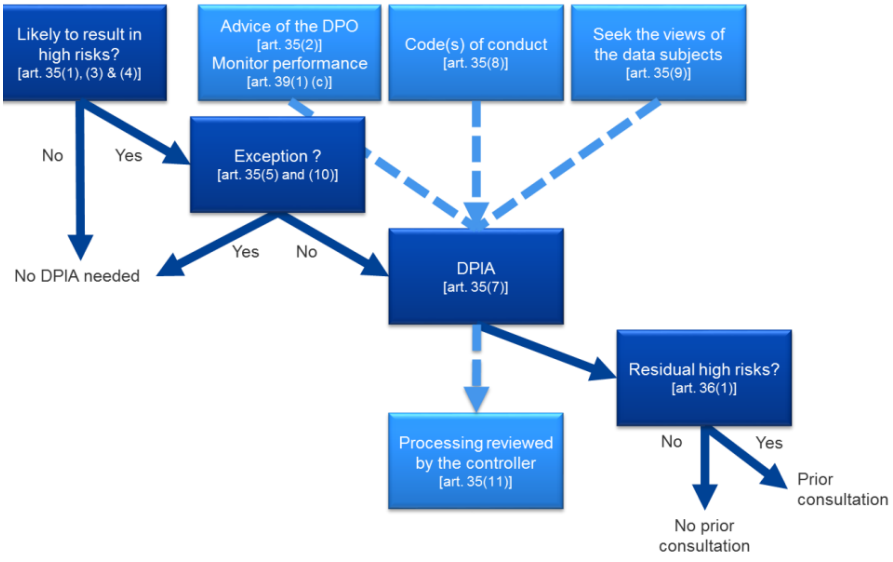

Figure 1 The basic principles related to the DPIA under GDPR.[16]

[16] The figure is available at Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679' (2017) 6, 7.

2.1.5 Article 29 Working Party

The Article 29 Working Party was the independent European working party that dealt with issues relating to the protection of privacy and personal data pre-GDPR data protection regime. In 2017, Article 29 Working Party provided guidelines on DPIA criteria as part of its mandate to support a harmonized understanding and interpretation of data protection provisions.

When GDPR entered into force on 25 May 2018, Article 29 Working Party was replaced by the European Data Protection Board (EDPB). The latter is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor. Since EDPB endorsed the data protection related- guidelines of the Article 29 Working Party in its first plenary meeting, the guidelines on DPIAs and other relevant matters provide an important source of interpretation of data protection legislation.

Article 29 Working Party confirms the understanding that the list of examples provided by Article 35(3) of GDPR is non-exhaustive.[17] The Working Party's Guidelines on Data Protection Impact Assessment (DPIA) provides a list of criteria and examples, which are further explained below. For the sake of clarity, it should be noted that these criteria do not prohibit processing of personal data. These criteria only refer to situations where a DPIA would be necessary before processing personal data. After an impact assessment is conducted, and all possible risks are mitigated (by taking technical or organisational measures), personal data can be processed.

Article 29 Working Party considers that the co-existence of at least two of the following criteria will most likely trigger a need for impact assessment. Thus, the assessment of criteria is a very context-dependent one, and there may be situations where even the co-existence of two criteria may not necessitate a mandatory DPIA. In general, the more criteria are present, it is more likely that the risks of processing will increase, and hence, an impact assessment will be necessary.[18] These criteria are the following:

- **Evaluation or scoring**

This criterion derives from Recital 71 and 91 of the GDPR. Evaluation or scoring could be in the form of profiling individuals or making predictions about their performance, behaviour or other characteristics. Evaluations or predictions based on the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements are considered particularly risky since this may deprive individuals from accessing certain services or label them against their interests. For instance, profiling a bank's customers to evaluate their creditworthiness may result in (acceptance or) denial of a loan to a particular individual. Another example is prediction of disease of a patient based on their health history.

- **Automated-decision making with legal or similar significant effect**

This criterion has two cumulative requirements. First, the criterion refers to processing of personal data to make automated decisions about individuals. This can be either fully automated or partially automated decision-making.[19] The decision-making is fully (or solely) automated if decisions are made by technological means without human involvement. Making predictions about individuals' behaviour based on the location data collected by an application is an example of an automated decision-making.

[17] ibid 9.
[18] ibid 11.
[19] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (2017) 8.

Second, the criterion refers to processing that produce significant effects. For example, automated selection of job candidates could have the significant effect of being eliminated from the selection process. Automated processing with little or no effect on individuals do not fall under this criterion.

- **Systematic monitoring**

This refers to observing, monitoring or controlling data subject in a network or publicly accessible area, for instance, through CCTV cameras. Systematic monitoring is a factor contributing to the risk to data subjects' rights because data subject may not be aware of processing and may not avoid it.

- **Sensitive data or data of a highly personal nature**

This criterion refers to processing of special categories of data, which includes:

- personal data revealing racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- processing of genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

In addition, other types of data can be considered to be sensitive such as monitoring of personal messages or e-mails, tracking of location data while individuals do personal activities (e.g. going home).

- **Data processed on a large scale**:

Large-scale processing pose particularly risks to the data subjects since they may involve a large portion of people at a regional or national level. There is not a fixed threshold for a large processing. The following can be used as an objective measurement factors:

- the number of data subjects concerned (e.g. a specific number or a proportion of population
- the volume of data and/or the range of different data items being processed
- the duration, or permanence, of the data processing activity
- geographical extent of the processing activity.

- **Matching or combining datasets**

This criterion derives from the principle of purpose limitation. The idea behind this criterion is that data originating from different sources and controllers can be used for purposes that cannot be initially foreseen by data subjects. For instance, combining data-sets collected by different applications (e.g. location, health, photos, messages…) provide a more detailed information about an individual compared with a dataset that collects only a limited type of data. A combined dataset can be used for new purposes (e.g. sharing with other parties, marketing) which could go beyond the expectations of a data subject.[20]

[20] See Irene Ioannidou and Nicolas Sklavos, 'On General Data Protection Regulation Vulnerabilities and Privacy Issues for Wearable Devices and Fitness Tracking Applications' (2021) 5 Cryptography 29.

- **Data concerning vulnerable data subjects**:

Processing of personal data of vulnerable individuals such as children or elderly can involve particular risks. Generally speaking, vulnerable data subjects are individuals who may not be able to say 'no' to data controllers or meaningfully exercise their rights because of their particular position as opposed to data controller. Employees may be considered to be vulnerable because employers have typically the power over employees on what kind of data to process and how to process it.

- **Innovative use or application of new technological or organisational solutions**

The idea behind this criterion is that technologies that go beyond the state of the art can involve novel forms of data collection and usage. The potential consequences of the use of these technologies may be unknown. For that reason, a DPIA can help to understand the potential risks. For instance, the combined use of fingerprint and facial recognition for improved physical access control could be considered as an innovative use. Certain Internet of Things applications may also fall under these criteria because they increase the possibility of collecting multiple information about individuals during their lives.

- **Prevention of data subject from using a right or service**

This criterion concerns processing operations that aims at allowing, modifying or refusing an individual's access to a service or entry into a contract. An example of this is when an employee screens employee database to decide on whether to grant employee benefits.

2.1.6 Analysis of the criteria for CoRoSect research and technologies

Both GDPR's and Article 29 Working Party's guidelines are general and not sector-specific. They can be interpreted in the context of a specific use case, and can be extended to other examples. The criteria have been interpreted below in the context of CoRoSect research, as well as the end-product that will be the outcome of the project and that will be put into market.

	Criteria	**CoRoSect research**	**Future deployment of the end-product by insect farms**
GDPR Criteria			
1)	A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person	No. CoRoSect technologies will be tested for a rather short period of time during the pilots in insect farms. Their deployment cannot be considered as systematic nor extensive. Furthermore, the testing of the developed technologies is conducted only for research purposes in line with the European Commission's guidelines. The CoRoSect research does not aim at producing any legal or other consequences for research participants.	Possibly yes where the end-product will be systematically and extensively used. (For instance, if it involves a large amount of individuals, and large periods of time).
2)	Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences	No. No special categories of data will be processed.	Possible if the end-product, in particular wearable technologies, are integrated with sensors that collect health data (e.g. heart rate) or

			if it is integrated with a product for biometric identification (e.g. identifying an individual with his or her unique characteristics such as voice or gaze.)
3)	A systematic monitoring of a publicly accessible area on a large scale.	No. Pilots will take place in insect farms and the CoRoSect research does not monitor a public area nor a public network.	Expectedly no.
Article 29 WP criteria			
1)	Evaluation or scoring (Recitals 71 and 91 of GDPR)	No. While some CoRoSect components involve processing of personal information such as behaviour or location, CoRoSect research does not make any evaluation or prediction regarding specific individuals, nor does it make profiles of individuals (for instance, to make decisions on a specific employees' performance or benefits.) CoRoSect research aims to improve human-robot collaboration for a faster and safer workplace environment. The research aims to achieve this goal by enabling robots to autonomously adapt to new tasks and to the behaviour, and habits of their human co-workers.[21] As such the 'workplace evaluation' performed by CoRoSect does not involve evaluations on individuals which may create a risk for them (e.g. being deprived of a service or being labelled against their interests.)	Possible depending on the use. The availability of a large amount of data collected through wearable technologies (HoloLens) create a possibility of processing this data for new purposes (for instance, if data is analysed to decide on the performance or social benefits of employees or if they are shared with third parties for commercial purposes). This could potentially lead to a situation where data is used for purposes that can hardly be foreseen by data subjects in advance. Therefore, this criterion could be present in the future deployment of CoRoSect technologies.
2)	Automated-decision making with legal or similar significant effect	No.	Expectedly no. (The same considerations mentioned in the previous line could be applicable here depending on the further use of data.)
3)	Systematic monitoring	No.	Expectedly no. It could be possible depending on the use.
4)	Sensitive data	No. No special categories of data are processed. Hololens component processes gaze data, which has a technical potential to be used for	Possibly yes if the wearable technology is integrated with sensors that collect special categories of data such as

[21] Input provided by UM.

		biometric identification (as in the example of DNA or fingerprint). However, this is a remote possibility, and the CoRoSect research does not process such data for biometric identification purposes. Furthermore, correlations between gaze and individuals are not recorded.[22]	health data (e.g. heart rate data) or if they are integrated with biometric technologies.
5)	Data processed on a large scale	No.	Possibly yes.
6)	Matching of combining datasets in a way that it exceeds expectations of data subjects	No. CoRoSect does not match or combine datasets that involve personal data in a way that it cannot be initially foreseen or expected by data subjects.	Possible depending on how the combination takes place. For instance, the combination of datasets from different applications (e.g. location, health, photos, messages) can provide a detailed profile of an individual compared with a dataset that collects only a limited type of data. A combined dataset can be used for new purposes (e.g. sharing with other parties, marketing) which could go beyond the expectations of a data subject.
7)	Data concerning vulnerable data subjects	No. While some of the research participants are expectedly employees of insect farms, it cannot be automatically assumed that the CoRoSect research involves vulnerable data subjects. CoRoSect partners ensures that research participants will participate in the research voluntarily, and inform participants about this in advance before participating in the research. Partners are not attached any negative consequences if they do not participate in the testing. Since some of the research participants are already involved in the research project, they have specialized knowledge on how and why CoRoSect uses personal data. Hence, the general risk of collecting data about individuals without them being aware of it does not exist during the CoRoSect testing.	Expectedly yes. The end-product will be deployed in the work environment of insect farms or other sectors, and will be used by employees of insect farms.

[22] Input from CERTH.

8)	Innovative use or applying new technological or organisational solutions	Possibly yes. CoRoSect involve processing of personal data through artificial intelligence and machine learning techniques. Some of the components could have an innovative way of processing data. At the same time no high-risks to the individuals are expected considering the purpose (e.g. ensuring a safe human-robot collaboration), context and scope of processing (e.g. no systematic or large scale processing, no public monitoring).	Expectedly yes.
9)	Preventing data subject from using a right or service	No.	No.

2.2 Ethics (assessment)

Artificial systems should comply with all applicable legal norms. However, due to the unpredictable nature of new technologies (e.g. autonomous behaviour, connectivity) such as artificial intelligence, there has been concerns that legal norms may not be sufficient to address all risks arising from the development and use of artificial intelligence. As a result, ethics have emerged as an important framework that governs artificial intelligence systems in Europe. A detailed description of this governance framework and policy developments have been provided in D1.1.

Trustworthy AI does not only comply with legal requirements only, but is also ethical and robust. Ethics Guidelines for Trustworthy AI note that four ethical values should underpin the development and use of AI throughout its lifecycle: respect for human autonomy, prevention of harm, fairness and explicability (See Figure 2).[23]

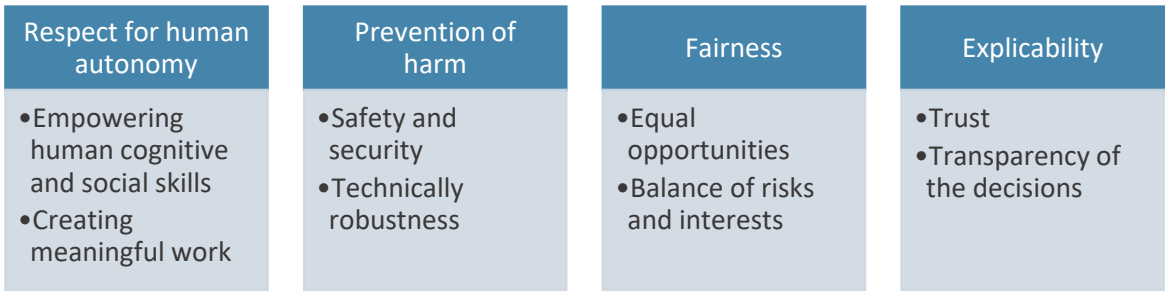

Figure 2 Ethical values

Building on these ethical values, Ethics Guidelines for Trustworthy AI establish seven requirements that a Trustworthy AI need to implement throughout its lifecycle. A detailed description of these principles can be found in D1.1 (See Figure 3).

[23] See CoRoSect D1.2 Ethical and Legal Requirements Specification Report.

Figure 3 Ethical principles for trustworthy AI

2.2.1 Assessment List for Trustworthy AI

Ethics Guidelines for Trustworthy AI is accompanied by an Assessment List Trustworthy Artificial Intelligence ('ALTAI' or the 'Assessment List')). The Assessment List helps businesses to operationalise the requirements for a trustworthy AI by means of a practical checklist. It is intended for self-evaluation purposes, and exists in two formats: a paper-based version and an online tool for self-assessment. The Assessment List can best achieve its aim if it is filled in by a multidisciplinary team of people (such as AI designers and developers, data scientists, procurement specialist, front-end staff, legal specialist and management).

While the Assessment List is an important tool for the operationalization of trustworthy AI, the research has shown some of its caveats.[24] First, the Assessment List apply generally to any AI. It is not tailored to the context in which AI will be deployed. Second, most questions are not open-ended questions (e.g. 'did you establish', 'did you ensure'), which means that they can be answered with a simple yes or no.[25] However, an assessment of a complex technology often require the consideration of a wide range of factors. It would be important to know the reasoning behind a particular answer to be able to objectively and independently assess whether the answer is well-justified.[26] For that reason,

[24] Nathalie Smuha, Towards a Practical Assessment Tool for Trustworthy AI, Presentation at the European AI Week 2022, 15 March 2022, available at https://www.youtube.com/watch?v=tb47bUlKPec&t=858s.
[25] Cybersane D10.4 Best Practices and Policy Development Guidelines for Replicability and Wider Use, 22.
[26] Ibid.

an assessment methodology should preferably include open-ended questions to be able to explain the factors that underpin the decision-making. In addition, the Assessment List often does not ask about the measure that is in place or that is considered to be taken. For instance, if the assessors think that a risk does not exist because there is or will be a technical measure that will prevent that risk, it would be important to know what that measure is.

2.3 Monitoring survey for CoRoSect research and technologies

In Task 1.3 KUL has prepared a survey for the purpose of monitoring and evaluation of the CoRoSect technologies in collaboration with the CoRoSect partners. This survey reflects the elements of two main methodologies for the assessment of new technologies: data protection impact assessment (Chapter 1.1) and the assessment list for trustworthy AI (Chapter 1.2).

The survey has been prepared keeping the caveats of the Assessment List in mind. The survey has chosen the questions that are the most relevant for the deployment of the CoRoSect end-product in insect-farms. The questions are formulated as short and open-ended as much as possible. For instance, instead of asking whether diversity and representatives of datasets were considered ('did you consider diversity and representativeness of subjects in data'), the survey asks 'how' a component would react if personal characteristics of a human worker change. Another example of this is the question that asks 'how' human beings can intervene in the system instead of asking whether a mechanism was established in accordance with human intervention.

Moreover, the survey opted for short questions, and divided questions in sub-questions as much as possible. For instance, relevant measures or metrics are to be indicated in a sub-question. The survey also provides some examples, if relevant. For instance, physical posture or gender of a worker, noise and lightning are provided as examples of factors that can affect accuracy.

In the first half, monitoring survey includes questions on the data protection impact assessment (DPIA) criteria and data governance, which are mainly addressed in Chapter 1.2 of this deliverable. In the second half, the survey includes questions on four thematic areas. These questions are indicated below. In the survey, each of these questions are followed by empty boxes with sufficient space to provide the answers to these questions.

Human agency and oversight:

- Could any component of the CoRoSect or the overall CoRoSect solution create any risk of over-reliance by end-users?
- Indicate technical measures or metrics that prevent or mitigate this risk.
- How can the users intervene or act if something goes in an unintended or undesirable way?
- Indicate technical measures or metrics that make interference by a human possible.

Safety, security and accuracy

- What are the safety risks that the end-users should be aware of?
- What organizational measures do you implement to ensure safety in your research and/or pilots? *(Organisational measure means any precaution you will implement or any arrangement you will make to run everything safely and smoothly. Examples: applying a safety distance, choosing pilot participants based on relevant expertise, providing training or information etc.)*
- Could outside factors (such as lighting, noise or other characteristics relating to the environment in which the technologies will be tested or used) negatively affect the accuracy of a robot/component? How do you avoid or mitigate these factors?

- How would a robot or another component react if personal characteristics of a human worker change? (*for instance, workers with a bigger or smaller posture or different gender)*?
- Is there a risk of reacting differently in a way that only persons with certain characteristics are negatively affected?
- Indicate technical measures that ensure the quality and representatives of datasets *(Representativeness of dataset means that the sample used reflects the real environment in which the technology will be deployed.)* Indicate any technical measures or metrics that mitigate this risk.
- How would a robot or another component react if the characteristics of the working environment change? *(for instance, different noise levels, different lightning conditions etc.)* Indicate any technical measures or metrics that mitigate this risk.
- Include measures or metrics to ensure robustness and overall security (*Examples can include encryption, pseudonymization, access controls to prevent attacks trying to manipulate the training dataset ('data poisoning'), preventing the misuse of network resources)*
- Indicate any industry standards (such as RAMI 4.0)

Transparency

- If an unexpected or unwanted event (for instance, behaviour is predicted wrongly, or a malfunctioning) happens, to what extent is it possible to trace back the source of the problem from a technical point of view?
- If an unexpected or unwanted event (for instance, behaviour is predicted wrongly, or a malfunctioning) happens, is it possible to fix it easily without great, time-consuming and costly changes to the whole system? Indicate any technical measure or metrics that can help to tackle this issue.

Impact on work

- Would deploying CoRoSect require you to make significant changes to your work arrangements and procedures? If yes, indicate what kind of changes or re-arrangements would be necessary or useful.
- How would this change affect the efficiency of the process (for instance, time for operator)
- Would you need to provide additional training and/or materials to re-skill or up-skill your workers to be able to use CoRoSect solutions? Why do you think so?
- How do you think the CoRoSect solution will affect the management of environmental impacts (for instance, impacts on waste management, energy use or impacts on other natural resources)

2.4 Summary and future steps for CoRoSect

If the processing is likely to result in a high risk to the rights and freedoms of individuals, a DPIA should be performed before processing of personal data. To determine whether there is any high risk to individuals, the nature, scope, context and purposes of the processing should be taken into account. In addition to these general rule, the GDPR and Article 29 Working Party provide some criteria and examples to help determine whether a DPIA is required in a particular situation.

This first part of this Chapter examined and applied the DPIA criteria to the CoRoSect research and the (expected) end-product based on the input received from partners through the monitoring survey, and information received from partners during meetings and project documents. It concluded that a

DPIA, based on the GDPR and Article 29 Working Party criteria, is expectedly not mandatory for the processing of personal data during the CoRoSect pilots. Nevertheless, this Chapter showed that the future deployment of the CoRoSect end-product may require a DPIA depending on the components it incorporates and the use of it. A limitation of the conclusions in this Chapter is that the study has not included the criteria of the national data protection authorities (which may include additional criteria in addition to the criteria examined in this study). This study is also not in the form of a legal advice, and does not exclude the fact that individual examination of each component and different interpretation of criteria could lead to a different conclusion.

With regard to the CoRoSect research, the research significantly differs from the non-exhaustive list of cases in GDPR. It also does not meet at least two criteria of Article 29 Working Party. Overall, CoRoSect technologies will expectedly be tested for a rather short period of time during the pilots. Some of the components do not involve processing of personal data. The components who involve processing of personal data are not in a nature of a systematic, extensive or large-scale processing. The deployment will take place in the context of insect farms for the purposes of increasing workplace safety, and decreasing arduous or time-consuming tasks that are typically performed by humans. The research does not involve monitoring of public spaces or public network. Considering the nature, scope, context and purposes of the processing in the CoRoSect technologies, no high-risks to the rights and freedoms of data subjects are expected.

In any case, the CoRoSect research makes an examination of any potential legal and ethical risks to the individuals[27], and are committed to keep the risks at minimum. For instance, personal data will be anonymized after the research has been conducted, and only anonymised results will be published. Personal data are stored in secured servers, and access is limited to ensure the confidentiality, integrity and availability of data.[28]

Furthermore, CoRoSect research implements the ethics guidelines for trustworthy AI, which are relevant regardless of whether data in question is personal or non-personal data. Technical measures are in place such as a safety switch[29] and emergency button[30]. CoRoSect uses a robot that is certified for human-robot collaboration. Newly developed robotic components will be carefully tested in a well-controlled lab environments. It has been considered that lightning may be a factor that affects the accuracy of some components, however this will not have any negative consequence on the safety of users.[31] To ensure quality and representativeness of datasets, the research will ensure to have sufficient users.[32] Last but not least, it will be ensured that the partners provide continuous input to the survey as the project makes progress to deploy the pilots. A final update on the implementation of the requirements will be provided in the D1.4.

3 Data Accuracy for Human-Robot Collaboration

Given the concept of accuracy have particular relevance to the CoRoSect project, this Chapter will provide a deeper understanding on the concept of accuracy and the related obligations of AI producers

[27] See CoRoSect D1.1 Ethical and Legal Framework: Initial Assessment Report, D1.2 D1.2 Ethical and Legal Requirements Specification Report.
[28] CoRoSect D11.9 Data Management Plan (revised).
[29] Input from UM
[30] Input from Robotnik.
[31] Input from CERTH and UM.
[32] Ibid.

and related organizational guidelines. Since some CoRoSect components[33] work in collaboration with humans, it is important for them to function accurately to avoid any situation where lack of accuracy lead to lack of safety.[34] Even other components that do not work with individuals should work accurately to make sure that insects are reared efficiently.

While the Cambridge Dictionary defines "accuracy" as "the fact of being exact or correct" and "the ability to do something without making mistakes"[35], its legal and ethical meaning should be examined for the sake of thorough legal and ethical guidance to the project.

Considering that artificial intelligence, as well as processing personal data, is core part of this project, the concept of accuracy will be examined under the GDPR and the proposed AI Act (which has not yet been adopted). It should be stressed that the proposal is not finalized or adopted yet, this means its content may undergo important changes and it will take time for this regulation to come into effect. However, the explanations in this deliverable will be based on the available proposal text in order to help the consortium to get prepared for the future regulatory framework. Even in case of potential changes in the proposed text before its adoption, the explanations here still show the direction where the EU law is going, hence provide a preliminary guidance on how to approach the concept of "accuracy" in the context of AI. In any case, the accuracy requirement is also recommended by the Independent High-Level Expert Group on Artificial Intelligence, which was set by the European Commission, (AI HLEG). The perspective of the expert group will also be provided.

3.1 Concept of Accuracy

In the data protection regime of the EU, accuracy is one of the principles of personal data protection under Article 5(1)(d) of the GDPR. According to this principle, personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay". There are currently important discussions around this concept in the literature[36]. However, the UK Information Commissioner's Office (ICO)[37] is in the idea that whether personal data is accurate will usually be obvious, despite the lack of definition of the concept "accuracy" or "accurate" data in the GDPR[38]. For the sake of brevity, the authors will avoid diving into theoretical and conceptual discussions here and give the essence of the concept as commonly understood. As the ICO rightfully noted, this principle, mainly, requires data controllers to:

- Take every reasonable step in order to ensure no incorrect or misleading data is kept.
- Update the data collected and processed where relevant/necessary.
- Take every reasonable step in order to correct or erase, as soon as possible, data that is incorrect or misleading.

[33] See above 2.1.3.

[34] It should be noted that no scientific conclusion has so far made in the project that lack of accuracy will create an unsafe situation in the context of CoRoSect components.

[35] Cambridge Dictionary, 'Accuracy' (22 February 2023) available at https://dictionary.cambridge.org/dictionary/english/accuracy.

[36] Elisabetta Biasin, 'About Accuracy (And Its Meaning In Data Protection)' (*CITIP blog*, 5 July 2022) available at https://www.law.kuleuven.be/citip/blog/about-accuracy-and-its-meaning-in-data-protection/.

[37] While UK is not a EU member anymore, the ICO's guidance is still relevant because the UK has transposed the GDPR into its national law and continues implementing it after the Brexit. Thus, ICO's understanding of a GDPR principle can still be relevant for the developers and end-users of CoRoSect.

[38] UK Information Commissioner's Office, 'Principle (d): Accuracy' (17 October 2022) available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/.

- Carefully consider data subject requests to rectify or erase inaccurate data and take all reasonable steps to fulfill these requests[39].

The proposed AI Act does not define "accuracy" either. It also does not provide any explanation on how to understand this concept. AI HLEG considers accuracy as an important aspect of "technical robustness and safety" and notes:

> *"Accuracy pertains to an AI system's ability to make correct judgements, for example to correctly classify information into the proper categories, or its ability to make correct predictions, recommendations, or decisions based on data or models. An explicit and well-formed development and evaluation process can support, mitigate and correct unintended risks from inaccurate predictions. When occasional inaccurate predictions cannot be avoided, it is important that the system can indicate how likely these errors are. A high level of accuracy is especially crucial in situations where the AI system directly affects human lives."* [40]

From an ethical perspective, "accuracy" is seen by the AI HLEG as an ability to "make correct judgements" and "make correct predictions, recommendations, or decisions based on data or models".

Lastly, from a technical perspective, accuracy is defined as the following[41]:

> *'Accuracy = Number of correct predictions / Number of total predictions*
>
> *…..*
>
> *[Accuracy= (True Positives + True Negatives) / (True Positives + True Negatives + False Positives + False Negatives)]'*

The following sub-section will shed light on the obligations of the producers of AI systems, which are relevant for the CoRoSect project.

3.2 Obligations of the AI Producers

3.2.1. GDPR

According to the principle of accuracy under GDPR Article 5(1)(d), personal data must always be kept accurate and up to date. This requires taking every reasonable step to erase or rectify any inaccurate data without any delay. This is an obligation mainly addressing the data controllers (and processors) but also the producers of any (technological) solutions that process personal data. This becomes clear if one looks closely to Article 25 on data protection by design and default (DPbDD). Although there is explicit reference only to the data controllers in this article, it should be read as a provision applicable to the producers as well. This is because the article requires "controllers" to implement appropriate (technical and organizational) measures "both at the time of the determination of the means for processing and at the time of the processing itself" to implement data protection principles (such as the principle of accuracy), and to integrate necessary safeguards reach the objectives of the regulation. Data controllers can only determine the means for processing depending on what technical

[39] Ibid.

[40] AI HLEG, 'Ethics Guidelines for Trustworthy AI' available at https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf.

[41] Noam Bressler, 'How to Check the Accuracy of Your Machine Learning Model' (2022) available at https://deepchecks.com/how-to-check-the-accuracy-of-your-machine-learning-model/.

features and capacities are provided by a producer. Thus, producers should also be subject to this article.

This division between the controllers and producers is of limited use in the CoRoSect project throughout the project's lifetime because of overlapping roles. It could be more useful after the end of the project as end-users may be different from the producers when the products are put into the market. Although compliance with Article 25 is not a strict obligation for the producers under the GDPR, it is a best practice as stated by the Recital 78 GDPR:

> *"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"*

In the same direction, the European Data Protection Board (EDPB) highlights, in its *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default,* the role of the producers (despite the article's explicit reference limited to the controllers) and recommends, among others, certification of the processing by noting that "producers should strive to demonstrate DPbDD in the life-cycle of their development of a processing solution. A certification seal may also guide data subjects in their choice between different goods and services"[42].

In brief, producers should take appropriate steps in order to implement the DPbDD approach from the outset of producing any product (with the view of allowing controllers and processors to fulfill their data protection obligations) and, in the context of accuracy, take measures to avoid, to the greatest extent possible, any possible inaccuracy and integrate the technical ability to rectify, erase and update any inaccurate data that may be present in the future. Certification of these products and systems will be the best practice as stressed by the EPDB.

3.2.2. Ethics Guidelines

Similarly, *Ethics Guidelines for Trustworthy AI* by AI HLEG suggests adopting an "explicit and well-formed development and evaluation process"[43] in order to mitigate, avoid, or correct possible risks due to inaccuracy. It further stresses that transparency, by indicating how accurate the product is, should be provided in case inaccuracies cannot be avoided.

3.2.3. AI Act Proposal

3.2.3.1 Scope of application

AI Act proposal aims to establish a requirement of accuracy for high-risk systems. Before turning to this requirement, it should be determined whether CoRoSect solutions would fall under the category of high-risk systems. AI Act proposal establishes three types of AI[44]:

- Prohibited AI practices (e.g. subliminal techniques and distortion of human behaviour)
- High-risk AI systems

[42] European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default | European Data Protection Board' (20 October 2020) 29 available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.
[43] See the previously quoted paragraph above.
[44] For a detailed information on these categories see D1.1.

- Limited risk AI with transparency requirements (e.g. deepfakes, emotion recognition)

Based on the currently available specifications regarding the CoRoSect technologies, they would not be classified either as prohibited AI practices. However, there is a possibility that certain CoRoSect components could be classified as high risk systems.

AI is a high-risk AI if (i) it is a product or safety component of a product that fall under the legislation listed in Annex II of the proposal, and (ii) it requires to undergo a third-party conformity assessment according to that legislation.[45] Machinery Directive is one of the legislation that is listed in Annex II. This directive covers machinery such as the protective device designed to detect the presence of persons. [46] If a CoRoSect cyber component can be considered to be a protective device designed to detect the presence of persons, it would fall under this legislation (the first criteria). Furthermore, such machinery may need to go through third party conformity assessment if they are not covered by the harmonized standards referred in Article 7(2) of the Machinery Directive (the second criteria). [47] As a result, cyber components of a human-robot collaborative products have a potential to classify as high-risk systems.

In addition, the European Commission may update the high-risk AI list in Annex III to cover the CoRoSect technologies. This also makes it clear that the right approach for the CoRoSect partners and future end-users is to closely follow the AI Act regulatory development process and take necessary actions to be compliant with it continuously.

Thus, it is recommended to be prepared for the AI Act proposal taking accuracy and other requirements into account. Even in the case that a CoRoSect component cannot be considered to be a high-risk AI, it is a best practice to implement the relevant requirements. Recital 81 of the AI Act supports this view:

> *"The development of AI systems other than high-risk AI systems in accordance with the requirements of this Regulation may lead to a larger uptake of trustworthy artificial intelligence in the Union. Providers of non-high-risk AI systems should be* ***encouraged to create codes of conduct*** *intended to* ***foster the voluntary application*** *of the mandatory requirements applicable to high-risk AI systems****.*** *Providers should also be encouraged to apply on a voluntary basis additional requirements related, for example, to environmental sustainability, accessibility to persons with disability, stakeholders' participation in the design and development of AI systems, and diversity of the development teams. (…)"*

As made clear in this Recital, developers of non-high-risk AI systems, such as the CoRoSect partners, are encouraged to apply the requirements for high-risk systems under the AI Act proposal.

3.2.3.2 Accuracy

Article 15(1) and (2) of the AI Act proposal stipulates:

"*1. High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an* ***appropriate level of accuracy****, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle.*

2. The levels of accuracy and the relevant ***accuracy metrics*** *of high-risk AI systems shall be* ***declared in the accompanying instructions of use****.'*

[45] Article 6 of the AI Act proposal.
[46] Annex IV, Machinery Directive.
[47] Article 12(3) and Annex IV of the Machinery Directive.

Similarly, Recital 49 notes, "[h]igh-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity in accordance with the generally acknowledged state of the art. The level of accuracy and accuracy metrics should be communicated to the users".

Regrettably, the AI Act does not provide a definition of accuracy. Nevertheless, Recital 44 provides some context by urging AI producers to take necessary measures to avoid incompleteness or incorrectness of data. Recital 44 states:

> *"High data quality is essential for the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become the source of discrimination prohibited by Union law. High quality training, validation and testing data sets require the implementation of appropriate data governance and management practices. Training, validation and testing data sets should be sufficiently relevant, representative and free of errors and complete in view of the intended purpose of the system. (…)"*

Furthermore, risks to health and safety of individuals that may be caused by AI systems should be "duly prevented and mitigated"[48]. The recital further adds "increasingly autonomous robots, whether in the context of manufacturing (…) should be able to safely operate and performs their functions in complex environments".

AI Act proposal stipulates multiple requirements for the high-risk AI producers and providers in addition to accuracy. These requirements include data and data governance, technical documentation, record keeping, transparency and provision of information to users, human oversight, and robustness, and security. The focus of this section was limited to accuracy.

3.3 Organizational Guidelines

AI has a potential to bring great benefits to various sectors including farming, as indicated in Recital 3 of the proposed AI Act, and the CoRoSect project aims to realize this vision. This sub-section will provide brief practical guidelines to the CoRoSect partners based on the explanations so far.

- The CoRoSect partners, whether they are data controller, processor or producer of the solutions, should integrate data protection by design and by default (DPbDD) in the life-cycle of their development or use of a processing solution. In the case of producers, this will be also crucial for ensuring that data controllers and processors will be able to comply with the EU data protection regime. For this purpose, the CoRoSect partners are recommended to adopt their own methodologies or organization-wide guidelines, in addition to provide necessary training to their staff.
- CoRoSect partners are recommended to use the *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment* to implement the ethics guidelines for trustworthy AI. The Assessment List, including accuracy-related questions, has already been incorporated in the CoRoSect methodology (See Chapter 2).
- Furthermore, it is recommended to take some steps to be prepared to implement the future AI Act. In particular,
    - The AI systems should be designed and developed with a high-level accuracy –thus, by making all the efforts (from the outset and including designing, training, and testing algorithms and models) with due regard to "state-of-art"– to minimize erroneous

[48] Recital 28, AI Act Proposal.

outputs. All the measures necessary to avoid incompleteness or incorrectness of data, and to ensure accuracy, should be taken. The architectures of machine learning and deep-learning models, among others, should be studied and chosen accordingly.

- Producers should declare the levels of accuracy and the relevant accuracy metrics of AI systems in the accompanying instructions of use. It is noteworthy that these levels are metrics are of technical nature, as briefly mentioned previously, and producers should adopt state-of-art methodologies to determine them.
- Even when a CoRoSect component falls under the category of high-risk AI, high-risk AI requirements could still be voluntarily implemented as a best practice. Further research could explore the possibility to establish a sector-wide code of conduct in insect farming industry.
- Any risks to health and safety of individuals that may be caused by AI systems, particularly autonomous robots as in the case of CoRoSect, should be prevented or mitigated.[49]

4 Cybersecurity in the Agriculture Sector

Since the delivery of the D1.1. and D1.2, there has been important legislative developments in the EU law concerning the cybersecurity in agriculture sector. For that reason, this Chapter will have a deeper look at these developments.

4.1 Legislative updates

Until very recently, there has not been much focus on the cybersecurity of the ICT products used in the agriculture sector. The future of the food and agriculture industry increasingly see the application of scientifically precise and automated farming techniques.[50] As a result, cybersecurity in the agriculture sector has become an increasing concern with the implementation of ICT components.

CoRoSect aims to build a sophisticated service oriented open human-robot working environment that will enhance the entire production pipeline in modern insect farms. CoRoSect solution incorporates a number of cyber and physical components. Each physical component has a respective cyber component that creates an intelligent network and ensures simultaneously high security standards with access rights to the functional/business services layer of the RAMI4.0-compliant infrastructure.

Physical and cyber components of human-robot interaction of the CoroSect tool bring into picture legal requirements related to security. With that in mind, the explanations on security in D1.1 related to those that stem from laws on the protection of personal data[51] and the cybersecurity certification schemes for ICT products.[52] D1.2 articulated security requirements with a focus on *AI-systems* and

[49] Relevant measures are currently being implemented during the pilot preparation phase.

[50] European Commission, Advanced Technologies for Industry – Sectoral Watch Technological trends in the agri-food industry, 'Technological trends in the agri-food industry' https://ati.ec.europa.eu/reports/sectoral-watch/technological-trends-agri-food-industry; Richard J Lehmann, Robert Reiche, and Gerhard Schiefer, 'Future internet and the agri-food sector: State-of-the-art in literature and research' (2012) 89 Computers and Electronics in Agriculture 158.

[51] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016

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

provided safety and security challenges to AI developers measures to safeguard the security of the system.[53]

However, D1.1 and D1.2 did not address legal requirements based on (cyber)security legislation at the EU level. This is because the currently applicable Network and Information Services Directive ("the NIS Directive")[54] and the Directive on European Critical Infrastructures ("the ECI Directive")[55] take a sector specific-approach, and do not identify at the EU-level sectors relevant to CoRoSect such as food or agriculture.[56] But these are minimum harmonisation measures and Member States are free to identify sectors other than those provided in these directives to fall within the scope of their implementation of NIS Directive. For example, Germany established food sectors covered by its implementation of the Directive.[57]

Recently, these two pieces of legislative frameworks were revised and their respective scopes were broadened (i.e. NIS2 Directive[58] and the CER Directive[59]) to include the food sector. Despite this regulatory update, the ambiguity of the applicability of these directives to CoRoSect still persists. It is still difficult to make blanket conclusion that the CoRoSect project research and end-users of the CoRoSect tool fall under the scope of the CER and NIS2 Directives. The reader is recommended to see sections below for explanations in this regard. This Chapter explores the relevance of these legislative updates for the CoRoSect solution.

4.1.1 The NIS 2 Directive

4.1.1.1 Background

The first EU-level cybersecurity legislation, the Network and Information Services Directive ("the NIS"), aims to achieve and maintain a high level of security of network and information security systems and to improve the functioning of the internal market. But the evaluation of the NIS showed a number of issues about its implementation that called for a revision. These issues were divergent security and reporting requirements for entities in different Member States, ineffective supervision and enforcement, limited information sharing between Member States, but also uneven resources for

June 2019

[53] CoroSect D1.2. Ethical and Legal Requirements Specification Report, Chapter 3.

[54] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[55] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

[56] The NIS Directive lays out obligations for operators of essential services ("OES") and digital service providers ("DSP"), the Member States identified OES and DSP in their own territories. Member States were to identify Operators of Essential Services (OES) in at least seven key-sectors: energy, transport, banking, financial market infrastructures, healthcare, drinking water, and digital infrastructure and certain digital service providers). The ECI Directive concerns energy and transport sectors, although, theoretically, its design allows for extension to other sectors.

[57] Further requirements apply, i.e. business thresholds. See below Section 4.1.1.5.

[58] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[59] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

competent authorities especially for computer security incident response teams ("CSIRTs") that varied significantly between Member States.[60] Another motivation behind the revision of the NIS was that since the adoption of the NIS, the EU economy has grown more dependent on network and information systems than ever before, and sectors and services are increasingly interconnected.[61]

Against this background, the Network and Information Services Directive 2 ("NIS2") amends the NIS to address the latter's deficiencies, and to adapt it to the current needs and to make it future-proof. It introduces measures related to cybersecurity and obliges Member States to adopt a national strategy for the security of networks and information systems.[62]

The NIS2 Directive provides cybersecurity requirements for a selected number of sectors and subjects them to regulatory oversight. The final text of the NIS2 was published in the Official Journal of the European Union in December 2022. By 17 October 2024, Member States must adopt and publish the measures necessary to comply with NIS2. These measures are to apply as of 18 October 2024. **Until 18 October 2024, the NIS continues to apply.** As further explained below (see 4.1.1.5), this means that the NIS2 will not apply during the CoRoSect project, however it may affect some of the end-users (e.g. depending on their size) of the end-product after the project.

4.1.1.2 Scope

Compared to its predecessor, the NIS2 has a broader scope that covers a wider set of sectors and services. NIS takes a differentiated approach with respect to the level of harmonisation in relation to those two groups of entities: "the operators of essential services" and "digital service providers". This categorisation is due to the fundamental differences between operators of essential services, in particular their direct link with physical infrastructure, and digital service providers, in particular their cross-border nature.[63] The Member States identify operators of essential services with an establishment on their territory based on the criteria provided in Article 4(4) of the NIS, for each sector and subsector in Annex II: energy, transport, banking, financial market infrastructure, health, drinking water supply and digital infrastructure.[64]

The NIS2 removes categories of "the operators of essential services" and "digital service providers" found in the NIS, and abolishes the identification of the OES by the Member States in their own territories. The NIS2 instead introduces "essential" and "important entities" reflecting the extent to which they are critical as regards their sector or the type of service they provide, as well as their size. The sectors within these categories are found in the Annexes of the NIS2.[65] A size-cap rule is

[60] European Commission, "Commission staff working document – Impact Assessment Report – Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148", SWD (2020) 345 final.
[61] See https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.
[62] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
[63] Recital 57, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)
[64] Article 5 NIS Directive and Annex II. Criteria for the identification OES are, "a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service" Article 5(2) NIS Directive.
[65] Ibid.

established to determine which entities qualify as operators of essential services and important entities.[66] This means that, in principle, all medium-sized and large entities operating within the sectors covered by the directive or providing services covered by the directive would fall within its scope. According to the size cap rule, the NIS2 covers large and medium enterprises in designated sectors.[67] Annex I provides sectors of high criticality, while Annex II other critical sectors (Table X). In general, all the entities in Annex I and II that do not qualify as "essential", they are considered "important".[68] Exceptions to these rules apply.[69]

NIS2 Sectors	
Sectors of high criticality (Annex I NIS2)	Other critical sectors (Annex II NIS2)
Energy	Postal and courier services
Transport	Waste management
Banks	Manufacture, production, and distribution of chemicals
Financial Markets	**Food production, processing, and distribution**
Health	Manufacturing
Drinking Water	Digital providers
Digital Infrastructure (cloud service providers, data centres, etc.)	Research
ICT Service Management	
Public administration, excluding the judiciary, parliaments and central banks	
Space	

Table 1: Sectors of high criticality and other critical sectors in NIS2

Regardless of their size, Article 2(1) provides the following entities as being *always* essential entities:

- Qualified trust providers, top-level domain name registries, and DNS service providers.
- Providers of public electronic communications networks or publicly available electronic communications services (meeting, but not exceeding the ceiling of medium-sized enterprises).
- Public administration entities of central governments and at regional level.[70]
- Critical entities in the meaning of the CER Directive (explained in detailed in the section below).
- OES identified by Member States under NIS or national law.

[66] Article 2, NIS2 Directive.
[67] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36): Large enterprises: less than 250 employees, less than 50m EUR turnover, less than 43m EUR balance and Medium enterprises: 50-250 employees, 10m-50m EUR turnover, up to 43m EUR balance.
[68] Article 2(a)(2) NIS2.
[69] This is possible if the criteria of Article 2(2)(c) to (f) are met, according to Article 2a(1)(d).
[70] Article 2(a) NIS2.

NIS2 establishes an extra-territorial scope of application. Selected providers of digital infrastructure or digital services who do not have an establishment within the EU, but offer services in the EU, will be within the scope of NIS2.[71]

The European Commission is to provide reports for the EU Integrated Political Crisis Response ("IPCR") arrangements under Implementing Decision (EU) 2018/1993, including in matters related to situational awareness and crisis response in the areas of agriculture, plant health, chemical incidents, food and feed safety, animal health.[72] The integrated political crisis response (IPCR) arrangements support rapid and coordinated decision-making at EU political level for major and complex crises, including acts of terrorism.[73]

4.1.1.3 General Obligations

The NIS2 provides measures to achieve a high common level of cybersecurity across the EU:[74] To that end, the NIS2 introduces,

- Obligations that require Member States to adopt national cybersecurity strategies;
- To designate or establish competent authorities;
- Cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);
- Cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;
- Rules and obligations on cybersecurity information sharing;
- Supervisory and enforcement obligations on Member States.

Member States may also choose to make the use of certified ICT products, processes, CSIRT good practices and services mandatory.[75]

The following measures are to be taken by **essential and important entities**:

- *Reporting obligations and information sharing*

The entities concerned by the scope of the directive will have to notify the national competent authorities.[76]

Entities with the scope of the NIS2 will have to communicate information relating to contacts and IP addresses exposed on the Internet to the national competent authorities and they have to update this information every 6 months or after each change.

Essential and important entities must immediately notify competent authorities or the CSIRT of significant incidents[77]. Member States are to ensure that notification obligations of incidents of

[71] Article 26(3) NIS2.
[72] Recital 72 NIS2.
[73] Article 21 NIS2.
[74] Article 1, NIS 2 Directive.
[75] Article 21 NIS2.
[76] Articles 23 and 30 NIS2.
[77] Article 23(3) and (4) NIS2 and "Significant incidents" are those that have the potential to cause significant operational disruption or financial loss to the entity, as well as those that have the potential to cause material and non-material losses to natural or legal persons (Article 6(11) NIS2).

significant impact are submitted to relevant CSIRTs or the competent authority without undue delay and in any event within 24 hours of becoming aware of the significant incident.[78]

In addition, if there is a breach of personal data, this should also be notified to the data protection authorities if it meets the conditions under Article 33 of the General Data Protection Regulation.[79]

- *Implementation of Security Measures*

The NIS2 establishes requirements for cybersecurity risk management. These measures are to take an *all-hazards approach* towards protecting the network and information systems and the physical environment of those systems from incidents. In this regard, entities are to take proportionate and appropriate precautions against risks associated with network and information system security. These measures will include *at least* the following:[80]

- Risk analysis and information system security policies;
- Incident handling (prevention, detection, and response to incidents);
- Business continuity and crisis management;
- Supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as the providers of data storage and processing services or managed security services;
- Security in network and information security systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- Policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;
- The use of cryptography and encryption.

If there is a personal data breach, the procedure of the Article 33 of the General Data Protection Regulation must be followed.[81]

4.1.1.4 Supervision and Enforcement

With regard to supervision and enforcement measures, a distinction is made between essential entities[82] and important entities.[83] The NIS2 requires EU member states to set up national oversight and governance mechanism for essential entities, with slightly milder supervision and enforcement regime for important entities.

NIS2 allows EU member states to implement administrative fines of at least EUR 10M or up to 2% of the total worldwide turnover of an entity for the preceding financial year (whichever is higher) for entities that fail to comply with cybersecurity risk management measures and the cybersecurity incident reporting obligations. Further, member states may implement their own national rules on penalties for infringement of the NIS2.

[78] Ibid.
[79] Article 35.
[80] Article 21(2) NIS2.
[81] Article 35.
[82] Articles 31- 34 NIS2.
[83] Article 33 NIS2.

4.1.1.5 What are the implications of the NIS and NIS2 on CoRoSect?

- *The NIS*

The ultimate question about the NIS and CoRoSect relationship is whether NIS or NIS2 applies to CoRoSect end-users or to its research activities. Under the currently applicable NIS, it is up to the Member States to designate the food or agriculture sector as an "operators of essential services". CoRoSect developers are advised to check with their national implementation of the NIS and their national competent authorities if sectors that CoRoSect end-users are within sectors are identified as "operators of essential services" in respective Member States. For example, the implementation of the NIS in Germany that currently applies (critical sectors identified through business thresholds), the food supply sector only covers entities that are over a designated thresholds for food and beverages. According to this threshold, a production plant will need to produce at least 434,500 tons of food or 350 million litres of beverages annually in order to be in scope.[84] If the NIS applies to CoRoSect end-users, they are advised to take a security by design approach to their technology development process and facilitate compliance with NIS requirements such as notification and security obligations.

The NIS is unlikely to apply to CoRoSect research activities because *inter alia* the research is conducted in controlled environments and the tool is not marketed for commercial purposes at the research stage. The NIS will also not be relevant for small and micro enterprises that do not fulfil the size requirements foreseen for relevant sectors under national laws (if applicable). If conditions for the applicability of the NIS are satisfied, CoRoSect developers are advised to facilitate the adoption of security requirements for end-users of the CoRoSect product.

- *The NIS2*

Similar to the NIS, the NIS2 will not impact CoRoSect research activities because by the time the NIS2 starts to apply in 18 October 2024, CoRoSect project will be over.

As shown in the table above, "food production, processing, and distribution" is identified as an important sector in NIS2. The Annex II point 4 of the NIS2 defines this sector as "food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council (3) which are engaged in wholesale distribution and industrial production and processingany undertaking, whether for profit or not and whether public or private, carrying out any of the activities related to any stage of production, processing and distribution of food".[85] Regulation (EC) No 178/2002 adopts the definition "any substance or product, whether processed, partially processed or unprocessed, intended to be, or reasonably expected to be *ingested by humans*."[86] "Feed" is explicitly kept out of the scope of the latter regulation.[87]

With those in mind, the NIS2 might be relevant for the end-users of CoRoSect and for the latter's developers. In order to fall under the scope of the NIS2, CoRoSect end-users must fulfill the size-cap

[84] OpenKritis, see https://www.openkritis.de/; Thomas Sievers, "Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations" (2021) *Int. Cybersecur. Law Rev.* 2 223.
[85] Annex II point 4, NIS2.
[86] Article 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.
[87] Article 2(a) 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.

rule and operate within one of the sectors covered by the NIS2. If an entity using CoRoSect solution is small or micro sized (exceptions apply, see above 4.1.1.2), *regardless of the sector,* it will not be within the scope of the NIS2. Insect farms that produce edible insects allowed for human consumption (e.g. crickets) and that fulfill the size-cap rule may fall in the scope. Given this possibility, and taking into account the broad range of marketability options an innovative solution like CoRoSect provides, the NIS2 may concern end-users of CoRoSect after the project ends. With that in mind, CoRoSect developers are advised to facilitate compliance with the obligations of end-users with security-by design solutions.[88]

4.1.2 CER Directive

4.1.2.1 Background

Currently, the main piece of legislation related to the protection of critical infrastructures ("CIs") is the Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, ("the ECI Directive").[89] The ECI Directive provides requirements for the physical protection of the CIs[90] in the EU. This Directive establishes "*a procedure for the identification and designation of ECIs, and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people"*.[91] The scope of the directive is limited to two sectors, namely energy and transport, albeit excluding nuclear energy.

The ECI Directive was evaluated by the European Commission in 2019,[92] following the conclusions of the 2017 assessment of the EU's security policy.[93] The evaluation concluded that while the directive had brought benefits in awareness raising, exchange of good practice, and increased cooperation and coordination, its overall impact had remained "more limited than initially expected".[94] Against this

[88] This aspect is also addressed in Chapter 2 on methodology for monitoring and evaluation.

[89] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[90] European critical infrastructure (ECI) means "an asset, system or part thereof located on EU territory, which is essential for the maintenance of vital societal functions, health, safety, security, economic or wellbeing of people, and the disruption or destruction of which would have a significant impact on at least two Member States, as result of the failure to maintain those functions". Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Articles 2 and 3.

[91] Article 1, ECI Directive.

[92] European Commission, Commission Staff Working Document Evaluation of Council Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection {SWD(2019) 310 final} Brussels, 23.7.2019 https://home-affairs.ec.eunopa.eu/system/files/2019-07/20190723_swd-2019-308-commission-staff-working-document_en.pdf

[93] European Commission, Comprehensive Assessment of EU Security Policy Accompanying the document Communication From the Commission to the European Parliament, The European Council and the Council Ninth progress report towards an effective and genuine Security Union, SWD/2017/0278 final Brussels, 26.7.2017 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0278.

[94] Erbach G., Cybersecurity of critical energy infrastructure, EPRS, European Parliament, 2019. Lazari A., European Critical Infrastructure Protection, Springer, 2014. Markopoulou, Dimitra, and Vagelis Papakonstantinou. "The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular." Computer law & security review 41 (2021): 105502.

background, on 16 December 2020, the European Commission presented a new proposal for a directive on the resilience of critical entities.[95]

On December 14, 2022, the final text of the Critical Entities Resilience Directive ("the CER" or "the CER Directive") was published in the Official Journal of the European Union as Directive. Member States have until 17 October 2024, to adopt and publish the measures to comply with the CER Directive and notify these measures to the EC. These measures shall apply as of 18 October 2024. Until 18 October 2024, the ECI Directive continues to apply unless Member States have implementing laws earlier. By 17 January 2026, Member States are to adopt a strategy for enhancing the resilience of critical entities.

4.1.2.2 Scope

The CER Directive will protect providers of critical processes by increasing their resistance and resilience, thereby guaranteeing the continuity of these processes more effectively.[96] The focus of the CER Directive is on the physical security and protection of critical processes.

The CER Directive is a minimum harmonisation measure and Member States identify the critical entities for the sectors and subsectors set out in the Annex within their own territories.[97] To identify critical entities, the following criteria apply:[98]

> *a) the entity provides one or more essential services;*
>
> *(b) the entity operates, and its critical infrastructure is located, on the territory of that Member State; and*
>
> *(c) an incident would have significant disruptive effects, as determined in accordance with Article 7(1), on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors set out in the Annex that depend on that or those essential services.*

It expands its scope to cover eleven sectors, that are, energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space and food. Recital 5 states that "the process for identifying critical entities in the food sector should adequately reflect the nature of the internal market in that sector and the extensive Union rules relating to the general principles and requirements of food law and food safety."[99] To ensure proportionality, "critical entities should only be identified among food businesses, whether for profit or not and whether public or private, that are engaged exclusively in logistics and wholesale distribution and large-scale industrial production and processing with a significant market share as observed at national level."[100]

---

[95] European Commission, Proposal for a Directive of the European Parliament And Of The Council on the resilience of critical entities, COM/2020/829 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0829&from=EN.

[96] Christer Pursiainen and Eero Kytömaa 'From European critical infrastructure protection to the resilience of European critical entities: what does it mean?' (2023) 8(sup1) Sustainable and Resilient Infrastructure 85.

[97] Annex, CER Directive.

[98] Article 6(2) CER Directive.

[99] Recital 4 CER.

[100] Recital 4 CER.

CER Directive does not apply to matters covered by the NIS2 without prejudice to Article 8 on ”Critical entities in the banking, financial market infrastructure and digital infrastructure sectors.” In light of the relationship between the physical security and cybersecurity of critical entities, Member States shall ensure that the CER Directive and the NIS2 are implemented in a coordinated manner.[101]

4.1.2.3 General Obligations

- Member States are to adopt a strategy[102] to ensure the resilience of critical entities, carry out a national risk assessment[103] and identify critical entities based on the risk assessment and national strategy. By 17 July 2026, each Member State shall identify the critical entities for the sectors and subsectors set out in the Annex.[104]
- Critical entities are to carry out risk assessments[105] of their own, take appropriate technical and organisational measures in order to boost resilience,[106] and report significant disruptions and incidents in their critical services to national authorities.[107]
- These technical and organisational measures include measures necessary to:[108]
    - prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;
    - ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;
    - respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;
    - recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;
    - ensure adequate employee security management, duly considering measures such as setting out categories of personnel
- All measures and controls should be documented in a single, coherent Resilience Plan. Specific measures can be further defined by the European Commission.[109]
- Critical entities providing services to or in at least one-third of Member States are subject to specific oversight,[110] including advisory missions organised by the Commission.[111]
- The Commission would offer different forms of support to Member States and critical entities, a Union-level risk overview, best practices, methodologies, cross-border training activities and exercises to test the resilience of critical entities.

[101] Article 1(2) CER Directive.
[102] Article 4 CER Directive.
[103] Article 5 CER Directive.
[104] Article 6 CER Directive.
[105] Article 12 CER Directive.
[106] Article 13 CER Directive.
[107] Article 15 CER Directive.
[108] Article 13(1) CER Directive.
[109] Article 13 (5) CER Directive.
[110] Article 17 CER Directive.
[111] Article 18 CER Directive.

- Critical Entities Resilience Group facilitates the regular cross-border cooperation with regard to the implementation of the CER Directive.[112]

4.1.2.4 Implications of CER Directive on CoRoSect

CER requirements might only be relevant for CoRoSect end-users after the project ends because similar to the NIS2, it starts to apply only after the project ends. Then, the CER might be relevant only for the CoRoSect end-users. Following is a brief explanation on how this might be the case.

Different from the NIS2, according to the CER, Member States identify critical entities to fall under the scope of the CER. "Food" is identified as one of the relevant sectors in the Annex of CER, but entities in the food sector may not be identified as "critical entities" by Member States if identification criteria is not fulfilled. Then, CER will not apply.

Another issue that must be taken into account when considered whether CER applies is the definition of the sector. The CER Directive and the NIS2 adopt the same definition of "food".[113] The aforementioned explanations on the definition of the food sector in Section 3.2.5 are also valid and they will not be repeated here.

It was also mentioned above in Section 4.1.2.2 "Scope", that the CER Directive recommends Member States to ensure the principle of proportionality when identifying entities in the food sector – meaning that identified entities should be food businesses that exclusively engage in logistics and wholesale distribution and large-scale industrial production and processing with a significant market share at national level.[114] This means that not all entities within the food sector will have to comply with the CER requirements. Small and medium sized entities are likely to be out of the scope of the CER Directive. If a CoRoSect end-user operates within the food sector as adopted in the CER Diective and operates on a large scale, it will have to fulfill the CER requirements. Similar to our recommendations above about NIS2, because there is a possibility that the CER might apply, CoRoSect developers are recommended to provide secured-by-design solutions.[115]

On a final note, as the aforementioned explanations show, the NIS2 and the CER contain similar obligations, which necessitate a clarification on their relationship to prevent any confusion about entities' responsibilities under the scope of these legislations. To give some background info, the NIS2 and CER are essentially meant to complement each other given the interconnection and interdependency between physical and digital infrastructures.[116] As mentioned above, the CER does not apply to matters covered by the NIS2. The NIS2 aims to establish a common level of security for network and information systems- and provides obligations towards resilience of network and information systems, as well as the physical components and environment of those systems. The CER, however, aims to reduce the vulnerabilities and strengthen the physical resilience of critical entities.

But some entities in the digital infrastructure sector under the NIS2 can be identified as critical entities under the CER. In such a case, some obligations that the CER Dir identifies (i.e. those in Article 11 "Cooperation between Member States" and Chapters III "Resilience Of Critical Entities", IV "Critical Entities Of Particular European Significance" and VI "Cooperation And Reporting" of the CER) will not apply to entities belonging to the digital infrastructure sector in order to avoid duplication and

[112] Article 19 CER Directive.
[113] See section 4.1.1.5 for in-depth explanations.
[114] Recital 4 CER.
[115] This aspect is also addressed in Chapter 2 on methodology for monitoring and evaluation.
[116] Recital 30 of the NIS2 and Recital 20 of the CER Dir.

unnecessary administrative burden. [117] But the strategies, the Member State risk assessments and the support measures set out in Chapter II ”National Frameworks On The Resilience Of Critical Entities” of the CER continue to apply. Further policy considerations and recommendations in the issue will be addressed more in detail in D1.4.

5 Conclusion

The key result of this deliverable is the explanation of the methodology for the monitoring and evaluation of CoRoSect research and technologies. Since some of the components of the project process personal data and involve the development of artificial intelligence and machine learning techniques, the methodology reflects the elements of the Data Protection Impact Assessment (DPIA) and ethics guidelines for Trustworthy AI. While doing so, it has taken some of the deficiencies of the ethics guidelines into account, aimed to improve it by addressing these deficiencies in the monitoring survey that was prepared as part T1.3.

Another key result of this deliverable is the analysis of whether a DPIA would be necessary for the CoRoSect research during the lifetime of the project, as well as the future deployment of the end-product. The deliverable found that the CoRoSect research expectedly does not require a mandatory DPIA for the processing of personal data during the CoRoSect pilots. It further found that the future deployment of the CoRoSect end-product may require a DPIA depending on the components it incorporates and its use. A limitation of the conclusions in this deliverable is that the study has not included the criteria of the national data protection authorities. Importantly, this deliverable showed that the CoRoSect research assesses any potential legal and ethical risks to the individuals in any case, and is committed to keep the risks at minimum. Further analysis on this assessment will be provided in D1.4.

Moreover, this deliverable provided a deeper understanding on the concept of accuracy, which is particularly relevant for the project to ensure that robots work in collaboration with humans accurately, and insects are handled efficiently. The deliverable focused on the concept of accuracy in the General Data Protection Regulation and the upcoming Artificial Intelligence proposal with a particular focus on the obligations of AI producers and organisational guidelines. In addition, the deliverable reflected recent developments in the EU in the area of cybersecurity in the agriculture sector. It found that these new adopted initiatives do not directly apply to the CoRoSect research, nevertheless it has a potential to apply to some end-users (e.g. depending on the market size and production of insects for food) when the final product is put in the market. Some policy implications of these developments have been provided. A more detailed account of policy considerations and recommendations will be provided in D1.4.

[117] Recital 20 CER Directive.

6 Bibliography

AI HLEG, 'Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment' (2020) https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

AI HLEG 'Ethics Guidelines for Trustworthy AI' (2019) https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf

Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (2017) 8.

Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679' (2017)

Article 29 Working Party, 'Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)' (1998)

Biasin E, 'About Accuracy (And Its Meaning In Data Protection)' (*CITIP blog*, 5 July 2022) https://www.law.kuleuven.be/citip/blog/about-accuracy-and-its-meaning-in-data-protection/.

Bressler N, 'How to Check the Accuracy of Your Machine Learning Model' (2022) available at https://deepchecks.com/how-to-check-the-accuracy-of-your-machine-learning-model/

European Commission, Advanced Technologies for Industry – Sectoral Watch Technological trends in the agri-food industry, Technological trends in the agri-food industry' available at https://ati.ec.europa.eu/reports/sectoral-watch/technological-trends-agri-food-industry

European Commission, Commission Staff Working Document Evaluation of Council Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection {SWD(2019) 310 final} Brussels, 23.7.2019 available at https://home-affairs.ec.eunopa.eu/system/files/2019-07/20190723_swd-2019-308-commission-staff-working-document_en.pdf

European Commission, Commission Staff Working Document – Impact Assessment Report – Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, SWD (2020) 345 final.

European Commission, Comprehensive Assessment of EU Security Policy Accompanying the document Communication From the Commission to the European Parliament, The European Council and the Council Ninth progress report towards an effective and genuine Security Union, SWD/2017/0278 final Brussels, 26.7.2017 available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0278

European Commission, Proposal for a Directive of the European Parliament And Of The Council on the resilience of critical entities, COM/2020/829 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0829&from=EN

European Commission, Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises

European Data Protection Board (EDPB), 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default | European Data Protection Board' (2020) available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

European Parliament, "The NIS2 Directive: A high common level of cybersecurity in the EU" Briefing, 08 February 2023 available at https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

Erbach G, 'Cybersecurity of critical energy infrastructure' EPRS, European Parliament, 2019 available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642274/EPRS_BRI(2019)642274_EN.pdf

Gellert R, *The Risk-Based Approach to Data Protection* (Oxford University Press, 2020)

Gellert R, 'Understanding the notion of risk' (2018) 34(2) Computer Law & Security Review 279

Ioannidou I and Sklavos N, 'On General Data Protection Regulation Vulnerabilities and Privacy Issues for Wearable Devices and Fitness Tracking Applications' (2021) 5 Cryptography 29

Lazari A, *European Critical Infrastructure Protection* (Springer, 2014)

Lehmann RJ, Reiche R, and Schiefer G, 'Future internet and the agri-food sector: State-of-the-art in literature and research' (2012) 89 Computers and Electronics in Agriculture 158

Lynskey O, *The foundations of EU data protection law* (Oxford University Press, 2015)

Markopoulou D and Papakonstantinou V 'The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular.' Computer law & security review 41 (2021): 105502

Nathalie Smuha, Towards a Practical Assessment Tool for Trustworthy AI, Presentation at the European AI Week 2022, 15 March 2022, available at https://www.youtube.com/watch?v=tb47bUlKPec&t=858s

Pursiainen C and Kytömaa E 'From European critical infrastructure protection to the resilience of European critical entities: what does it mean?' (2023) 8(sup1) Sustainable and Resilient Infrastructure 85.

Sievers T, "Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations" (2021) Int. Cybersecur. Law Rev. 2 223

UK Information Commissioner's Office, 'Principle (d): Accuracy' available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/

van Dijk N, Gellert R, and Rommetveit K, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 Computer Law & Security Review 286

CoRoSect

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