Legal, Regulatory and Ethical Framework – M18

D7.2

Person responsible / Author:	Marina Cugurra – EAI
Deliverable N.:	D7.2
Work Package N.:	WP7
Date:	30.06.2024
Project N.:	101092069
Classification:	PU - Public
File name:	"Legal, Regulatory and Ethical Framework – M18"
Number of pages:	120

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Health and Digital Executive Agency (HaDEA). Neither the European Union nor HaDEA can be held responsible for them.

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Health and Digital Executive Agency (HaDEA). Neither the European Union nor HaDEA can be held responsible for them.

AI REDGIO 5.0

Status of deliverable

Action	By	Date (dd.mm.yyyy)
Submitted (author(s))	Marina Cugurra (EAI)	12.08.2024
Responsible (WP Leader)	Veronica Antonello (TXT)	29.07.2024
Approved by Peer reviewer	Ángel Ortiz Sánchez (HOPU/Libellium)	5.08.2024

Revision History

Date (dd.mm.yyyy)	Revision version	Author	Comments
28.03.2024	V0.1	EAI	ToC – initial version
15.04.2024	V0.2	EAI	ToC – final version
20.05.2024	V0.3	AI REDGIO Experiment Leaders, EAI, SUITE5	First round contributions
29.05.2024	V0.4	EAI	First draft of the document
21.06.2024	V0.5	AI REDGIO Experiment Leaders, EAI, JSI	Second round contributions
25.06.2024	V0.6	EAI	Second draft of the document
09.07.2024	V0.7	AI REDGIO Experiment Leaders, EAI	Third round contributions
19.07.2024	V0.8	AI REDGIO Experiment Leaders	Fourth round contributions
26.07.2024	V0.9	EAI	Document ready for Peer Review and Quality Check
29.07.2024	V0.10	TXT	WP7 leader Quality Check
05.08.2024	V0.11	Libelium/HOPU	Peer Review and Quality Check
12.08.2024	V1.0	EAI, POLIMI	Official release and submission to the EC

Author(s) contact information

Marina Cugurra	EAI	Marina.cugurra@expertai-lux.com
Valentin Charreton	PERNOUD	v.charreton@pernoud.com
Mateja Senk	POLYCOM	Mateja.Senk@polycom.si
Nima Rahmani	POLIMI	nima.rahmani@polimi.it

Miha Glavan	JSI	miha.glavan@ijs.si
Sara Manders	BI	s.manders@brainportindustries.nl
Chen Li	AAU	cl@mp.aau.dk
Martin Dan	PBN	martin.dan@pbn.hu
Christophe Bruynseraede	MAKE	Christophe.Bruynseraede@flandersmake.be
Marielena Márquez Barreiro	GRADIANT	mmarquez@gradiant.org
Christian Conficoni	UNIBO	christian.conficoni3@unibo.it
Christian De Brida	PALMEC	christian.debrida@gpalmec.it
Martin Macas	CVUT	Martin.Macas@cvut.cz
Alissa Zaccaria	IMECH	alissa.zaccaria@intellimech.it
Rachel Davies	DMIW	rae@dmiw.co.uk
Marius Hagan	TUIASI	marius.hagan@etti.tuiasi.ro
Dan Martin	PBN	martin.dan@pbn.hu
Miguel Pincheira Caro	FBK	mpincheiracaro@fbk.eu
Cezara Zbancă	Katty Fashion	project.management@katty-fashion.ro
Shun Yang	University of Twente	s.yang-1@utwente.nl
Francesco Dellino	MADE	francesco.dellino@made-cc.eu

Table of Contents

Tables

Abbreviations and Acronyms:	
AI	Artificial Intelligence
AIA	Artificial Intelligence Act
AILD	Artificial Intelligence Liability Directive Proposal
ALTAI	Assessment List for Trustworthy Artificial Intelligence
API	Application Programming Interface
CI	Collaborative Intelligence
COBOT	Collaborative Robot
DIH	Digital Innovation Hub
DF	Didactic Factory
DMP	Data Management Plan
DOA	Description of Actions
DSA	Digital Service Act
EC	European Commission
EDPIA	Ethics and Data Protection Impact Assessment
EEM	Ethics Experiment Manager
EFFRA	European Factories of the Future Research Association
ELSEC	Ethical, Legal, Socio-Economic and Cultural
EM	Ethics Mentor
ePD	ePrivacy Directive
ePR	ePrivacy Regulation
GDPR	General Data Protection Regulation (Regulation EU 2016/679)
HF	Human Factor(s)
HMI	Human-Machine Interface
HRIA	Human Rights Impact Assessment
IEEE	Institute of Electrical and Electronics Engineers
IPR	Intellectual Property Rights
N/A	Not Applicable
RPLD	Revised Product Liability Directive Proposal
SME	Small Medium Enterprise
TC	Technical Coordinator
TEF	Testing and Experimental Facilities
TERESA	Technology and Regulatory SAndboxes
UI	User Interface
VF	Virtual Factory
WISE	Well-being, Comfort and Acceptance; Inclusion and Special categories of workers; Safety of the worker, Ergonomics and improving working conditions
WP	Work Package

1. Executive summary

This document identifies and analyses the key legal and ethical challenges relevant for the AI REDGIO 5.0 technologies, exploring and interpreting the applicability of responsible, ethical, and trustworthy AI within this manufacturing context. Such challenges range from those related to the human-centric approach, to the liability and safety issues, to the data ownership and data sovereignty, to the concerns related to the privacy and data protection, as well as the risk of algorithmic biases, the psychological issues of human-machine interaction and the uncertainties related to the possible use of Generative AI solutions.

The document also identifies and analyses the European legal, regulatory and ethical sources applicable to the AI REDGIO 5.0 system and technological assets, relevant to address these challenges. Such sources were classified in instruments pertaining to the Artificial Intelligence, instruments pertaining to the data and miscellaneous, including for instance the human rights law. In addition to this project-level regulatory framework, the document provides for each of the experiments of the project the relevant complementary legal and ethical sources related to the technologies involved in it, including legislations, standards, sector-specific policies, company/institution practices/policies and other kind of non-binding sources.

On the basis of this comprehensive legal review and analysis of the AI REDGIO 5.0 key technologies and assets, as well as of the AI REDGIO 5.0 experiments, the legal and ethical requirements for the AI REDGIO 5.0 technologies and each of the experiments have been defined and are reported in the document, including related guidelines.

These requirements are contributing (and will continue to contribute in the next period) to make the design, deployment and validation of AI REDGIO 5.0 solutions legal compliant, human-centric and trustworthy. They take into account also the recent regulatory developments, such as the AI Act, the AI Liability Directive Proposal, the Revised Product Liability Directive Proposal and the recently adopted EC's Living guidelines on the Responsible use of Generative AI in research, beside, for instance, the Ethics Guidelines for Trustworthy and the Assessment List for Trustworthy Artificial Intelligence (ALTAI).

This document is aimed at representing a unique reference point for the legal and ethical implications and requirements related to the design, development and validation of AI REDGIO 5.0 technologies and their validation. The legal and ethical requirements might be refined, enriched or updated in the next months and, at the end of the project, in D7.7, the guidelines for the legally compliant, responsible and trustworthy adoption and use of AI REDGIO 5.0 solutions will be provided, mainly relying on the lessons learnt during the project and the running of its 21 experiments.

2. Objective of the deliverable

This document pertains to T7.1 "Legal, Regulatory and Ethical Issues", which is directed to identify and examine the relevant regulatory and ethical framework relevant for the AI REDGIO tools and experimentations, as well as to putt forward blueprints and recommendations for EU policy development towards the sustainability, growth, competitiveness, inclusion and empowerment of human beings within the manufacturing domain. It also pertains to T2.4 "Legal and ethical requirements for AI Collaborative Intelligence Scenarios", which is devoted to define the set of legal and ethical requirements with which the AI REDGIO 5.0 tools and experiments must comply.
In particular, the deliverable is aimed at:

- providing insights on the main legal and ethical challenges raised by AI REDGIO 5.0 technologies;
- analysing the European legal, regulatory and ethical sources relevant for AI REDGIO 5.0 system and technological assets, relevant to address these challenges, as well as the complementary regulatory framework relevant for each of the project's experiments and the technologies involved in it, including legislations, standards, sector-specific policies, company/institution practices/policies and other kind of non-binding sources;
- eliciting the legal and ethical requirements and related guidelines for the AI REDGIO 5.0 technologies and each of its experiments, in order to make the design, deployment and validation of AI REDGIO 5.0 solutions legal compliant, human-centric and trustworthy, also taking also into account the recent regulatory developments, such as the AI Act and the EC's Living guidelines on the Responsible use of Generative AI in research.

3. Factual basis for the legal and ethical analysis and for the requirements elicitation

This section comprises a brief description of the main technologies of AI REDGIO 5.0 and their functionalities, underlying the facts and aspects relevant for the legal analysis and to elicit the legal and ethical requirements elicitation.

3.1. WP4 technologies and tools

WP4, known as the Industry 5.0 Data4AI Platform & Data Spaces, is developing an infrastructure designed to enable AI functionalities at the edge of industrial systems. This infrastructure blueprint has been meticulously planned through a reference architecture, detailed in D4.1. The reference architecture serves as a comprehensive guide for connecting systems from the shop floor's edge to the cloud, ensuring continuous security and computation mobility throughout the entire process.
A critical aspect of this infrastructure is the seamless integration of technologies from WP5, such as the Collaborative Intelligent Platform and the AI Pipeline Designer. These technologies can be effortlessly incorporated into the infrastructure, enhancing the overall capability of the system. The reference architecture illustrates how these integrations can be achieved, promoting a cohesive and efficient technological ecosystem.
Given the sensitive nature of industrial and personal information, security is paramount. The reference architecture supports a robust public key infrastructure, ensuring security from the edge to the cloud. This approach safeguards data integrity and privacy, preventing unauthorized tampering. Additionally, the architecture addresses the need for a computation continuum to handle changes in processing loads and component failures, thereby maintaining resiliency and efficiency across the systems.
Data within this infrastructure is securely stored in Data Spaces at various levels, employing standard data models and ontologies. This structured approach to data management facilitates interoperability and ensures that information can be easily accessed and utilized within the AI ecosystem. The use of standardized models and ontologies is crucial for maintaining consistency and reliability in data handling.

Practical examples of this reference architecture are demonstrated through open-source implementations using various technologies, such as FIWARE, APACHE, and the Arrowhead framework. These implementations provide valuable insights into the functionality and potential applications of the reference architecture, showcasing its versatility and adaptability in different industrial scenarios. Through these examples, stakeholders can better understand the practical benefits and operational efficiencies offered by the Industry 5.0 Data4AI Platform & Data Spaces.

3.2. WP5 technologies and tools

WP5 designs and deliver technologies that will enable the different pilots of the project (e.g. SMEs, DFs, Open Call winners, etc) to design, deploy, execute and evaluate their AI models on either edge or cloud infrastructures, placing the human factor in the loop, as a decisive factor the evaluation of the AI models outputs.

As such, WP5 delivers the following artefacts:

- The **Collaborative Intelligence platform**. The AI REDGIO 5.0 Collaborative Intelligence Platform is a solution at the forefront of Industry 5.0. The idea is to combine various technological advancements to redefine industrial landscapes. The platform facilitates Human-AI collaboration by integrating cutting-edge AI capabilities. In this way, the platform is intended to illustrate the potential of connected devices, sensors, and machines through real-time data fusion and analysis, driving optimal decision-making and resource allocation. The platform is ingesting data coming from the execution of the different AI models, evaluates the outcomes and also receives human input, to validate the AI model's output.
- The **Open Hardware** platform. The Open Hardware Platform for Embedded Artificial Intelligence and AI-at-the-Edge represents a significant advancement in technology and artificial intelligence (AI). This platform is based on open hardware, which allows users and developers to modify and enhance hardware according to their specific needs. The Open Hardware Platform for Embedded AI and AI-at-the-Edge have a wide range of applications; it can be used in autonomous drones for image processing and real-time decision-making, in personal assistance devices for voice recognition and real-time interaction, or industrial sensors for monitoring and independent decision making. As such, the Open Hardware platform can be seen as a use-case agnostic offering by the project, that allows developers and engineers to take advantage of the power of open hardware for edge execution to design and deploy their solutions on top of this platform.
    - The **AI Pipeline Designer**. The AI Pipeline Designer is a cloud-based infrastructure that is offered to the engaged users as a facility that allows them to design their AI models and construct an AI pipeline. Essentially, users are offered with existing and pre-configured elements coming out of known AI/ML libraries and using those they can define their AI models and train them using sample data. Finally, the tool offers the ability to either execute the pipeline on the cloud resources available and retrieve the results using an API or download them as a file, or to deploy the designed models directly on the Open Hardware and thus prepare the ground for the edge execution of the models. As such, one can see that the AI Pipeline Designer lies at the heart of the WP5 outputs, as it is the connecting link between all the other tools, namely it can be used to ingest/export assets using the AIoD Connectors (see below), can design AI pipelines and train and execute AI models on the cloud or even deploy them to the Open Hardware, and is able to ingest the outputs of the CI in terms of calibrating an already designed model.
- The **AIoD Connectors**. These are actually connectors tasked to transfer assets from the AIoD platform to the AI REDGIO 5.0 Ai Pipeline designer as well as the Open Hardware platform, as well as to publish assets back to the AIoD platform. In the former case, the connectors enable the re-use of existing knowledge and models to accelerate the design of different use-case specific solutions, and on the latter the propagation of the by the project generated knowledge back to the reference EC platform for AI implementations coming out of research project.

The above mentioned technologies, and especially the AI Pipeline Designer and the Open Hardware are linked to the technologies delivered by WP4, and in particular with the ones that do manage data and can offer them as input for the AI models to be developed, and finally the AI pipelines to be executed.

4. The ethical and legal framework and requirements for AI REDGIO 5.0 Technology

4.1. Key Aspects and Challenges

This section describes the key legal and ethical risks and challenges raised by AI REDGIO 5.0 technology and its human-machine-interaction tools, exploring and interpreting the applicability of responsible, ethical, and trustworthy AI within this manufacturing context[1][2] [1] [2]. The main aim is to ensure that the use of AI in AI REDGIO 5.0 (and the future applications of its solutions) works for society and is not detrimental to human well-being. In the manufacturing domain such a theme is still under-explored, as well as the main vulnerabilities that this domain might suffer from, during the AI development and deployment cycle. AI is helping to improve productivity by increasing efficiency and tackling major challenges facing the sector. However, this could lead to risky AI practices and ethical concerns, such as those related to surveillance practices around worker monitoring and incorrect maintenance predictions leading to wasted operational "corrections".

The topics described below, in line with the taxonomy provided by Newman[3] [3], are the main areas of attention specific to the AI lifecycle inherent to AI REDGIO 5.0 socio-technical system, considering the technical, organisational, and human processes aspects throughout the technology development, operation and use, as well as their supply chains.

I. Human centricity

The human centricity paradigm is paramount within the AI REDGIO 5.0 Ethical Strategy and workplan, including its technological development and validation operations. Like in the previous project AI REGIO[4], the Consortium's effort are directed to prioritize at the maximum possible extent the human well-being within the Industry 5.0 workplace of the future and its CI-driven paradigm, putting the innovations at the service of human needs and interests for adapting the production process to the needs of the worker and fostering his/her flourishing. The human-centric approach in AI REDGIO 5.0 goes beyond the safeguard of human values and ethical principles towards human empowerment, enhancement and augmentation. This means that the operator and the knowledge worker should be empowered by machines through really inclusive solutions, capable of a continuous adaptation of workplaces to their physical, sensorial and cognitive capabilities. In this way, also ageing, disabled and apprentice operators could be effectively assisted and, in general, the working capabilities are enhanced.

The European Commission, as well as other important players and ecosystems within the European Union, such as EFFRA, boosts the human-centric approach. This is mentioned in several Communications and is at the basis of the "International Outreach for human-centric Artificial Intelligence Initiative" (InTouchAI.eu)[5], launched by the European Commission's Service for Foreign Policy Instruments (FPI), the Directorate General

[1] A. Brintrupa, G. Baryannisb, A. Tiwaric, S. Ratchevd, G. Mart´ınez-Arellanod, J. Singhe, "Trustworthy, responsible, ethical AI in manufacturing and supply chains: synthesis and emerging research questions", 2023.

[2] AI REGIO D7.1 "AI REGIO Human-AI Interaction Framework – M12", AI REGIO D7.2 "AI REGIO Human-AI Interaction Framework – M24".

[3] J. Newman, "A taxonomy of trustworthiness of Artificial Intelligence. Technical report", 2023

[4] AI REGIO - "Regions and Digital Innovation Hubs alliance for AI-driven digital transformation of European Manufacturing SMEs" Project was funded by the European Union Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement n° 952003

[5] International Outreach for human-centric Artificial Intelligence Initiative (InTouchAI.eu), https://digital-strategy.ec.europa.eu/en/policies/international-outreach-ai

for Communications Networks, Content and Technology (DG CONNECT) and the European External Action Services (EEAS). The InTouchAI.eu is a large foreign policy instrument project to engage with international partners on regulatory and ethical matters and to promote the responsible development of trustworthy AI at global level. By fostering the human-centric paradigm and the promotion of the ethical values, the InTouchAI.eu is expected to prepare the ground for global coalition building in this field.

In order to promote human-centricity and relying on AI REGIO findings, in AI REDGIO 5.0 both the WISE Implications and the WISE indicators are used, both for the TERESA Experiments and for the SME-driven experiments, for identifying and addressing the main ethical, legal, regulatory, psychological and societal impacts of the project's artefacts in the different contexts.

The WISE implications, concerning the key legal and ethical issues relevant within a AI-empowered workplaces and human-machine collaboration environment and potentially testable in a TERESA, are classified in the following categories:

- Well-being, Comfort and Acceptance, which refer to the impact on mental well-being and self-esteem, frustration, feeling of usefulness, emotional dependence and overconfidence on the machine, human dignity, autonomy and oversight, concerns/willingness in collaborating with a machine;
- Social inclusion and special categories of workers, which refers to the effects on older workers, effects on novices, effects on workers with cognitive or physical disabilities/impairment, social isolation, risk of discrimination/bias;
- Safety of the worker, including health and safety of the workers, risks of harm, privacy and other.
- Ergonomics and improving working conditions, comprising the impact on stress reduction, fatigue reduction, effects on workers' skills

Figure 1. WISE Implications

On the other hand, the WISE Indicators are human well-being indicators specifically relevant for AI-empowered workplaces and human-machine collaboration in the Manufacturing domain. As comprehensively described in D6.4, the WISE Indicators "consist of different metrics covering multiple dimensions of the human wellbeing and empowerment, aimed at capturing the factors which allow the comprehensive assessment of the benefits and possible challenges of CI artefacts to monitor that such artefacts contribute to the operator's flourishing and do not bring unintended negative consequences that could diminish human comfort. The role of them is, also in a post-project phase, to contribute to identify the risks for the workers and the challenges raised by the CI uptake from an ethical and societal viewpoint in view of taking the appropriate mitigating actions when necessary"

We refer to well-being metrics allowing the benefits of CI artefacts to be more evaluated to test and monitor that the innovation at stake doesn't bring unintended negative consequences that could diminish human well-being, and that new routes to a human-centric AI are identified.

The figure below shows the wellbeing metrics identified for AI REGIO purposes and which are and will be further used by the AI REDGIO 5.0 TERESA (but in some cases also by some SME-driven experiments) to monitor and assess the WISE Implications:

Figure 2. WISE Indicators

II. Liability and Safety

It is paramount the clear understanding of responsibilities between different actors when using an AI system, like in AI REDGIO 5.0, in the productive process in case it makes mistakes producing damages or injury to property and human beings.

The potential harms include, for instance, unavoidable or inherent harms, defect-driven harms, misuse harms, unforeseen harms, systemic harms, as well as collateral harms.

According to the White Paper on Artificial Intelligence – A European Approach to excellence and Trust[6] [1] and the Report on safety and liability[7] [2], in order to strengthen the AI growth and its wide uptake it is key to address the liability aspects at policy level, especially the liability for damage caused by AI-systems, including the uncertainty regarding the allocation of responsibilities between different actors. Likewise, the Resolutions adopted by the European Parliament in October 2020[8] [3], covering ethics and civil liability, called for the harmonization of the legal framework for civil liability claims and for a regime of strict liability on operators of high-risk AI systems. In the Report on Artificial Intelligence Liability, the specific challenges posed by artificial intelligence to existing liability rules are described.

The EU Parliament[9] [4] acknowledged that "the complexity, connectivity, opacity, vulnerability, the capacity of being modified through updates, the capacity for self-learning and the potential autonomy of AI systems, as well as the multitude of actors involved represent nevertheless a significant challenge to the effectiveness

[6] European Commission, «COM (2020) 65 final "White Paper on Artificial Intelligence – A European Approach to Excellence and Trust,» 2020.

[7] European Commission, «COM(2020) 64 final. "Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics",» 2020

[8] European Parliament, «Resolution on a civil liability regime for artificial intelligence, (2020/2014 (INL),» 2020 and European Parliament, "Resolution on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012 (INL)", 2020

[9] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))

of Union and national liability framework provisions" and therefore specific and coordinated adjustments to the "liability regimes are necessary to avoid a situation in which persons who suffer harm or whose property is damaged end up without compensation".

In case of harm, questions of attribution and remedies might arise at the intersection of products liability and AI. They might regard, for instance, the attribution for AI-induced harms and the identification adequate mechanisms to mitigate possible AI harms. Examples of them are: "Whose fault is it if an AI system takes a decision which causes harm?", "How to apportion such a fault?", "What sort of remedies should be imposed or measures should be taken to avoid the repetition of such mistakes in the future?"

The difficulties are increase by the fact that the AI systems are able to learn, going beyond the simple implementation of human-designed algorithms.

In some cases the harm caused by an AI system could be the direct consequence of its programming or of its negligent design, training, or operation (e.g., lack of adequate cybersecurity protections), as well as of an unforeseeable harm generated by an interaction with unforeseeable real-world data.

On the other hand, in other cases, the products evolve: it might make difficult, in relation to products liability, to understand whether companies need to bear responsibility for the AI products they create, even when those products evolve in ways not specifically desired or foreseeable by their manufacturers, as well as to apportion blame and responsibilities when there are multiple companies that have had a hand in designing an AI system (or in shaping the post-sale algorithm evolution)[10].

The liability risk associated with AI systems might differ depending on the function of the AI output: for instance, the predictive systems differ from fully autonomous systems, where humans seems to be "out of the loop".

The existing legal framework is characterized by the partially harmonised EU legislation on liability for defective products (Directive 85/374/EEC on liability for defective products), applicable to any product marketed in the European Economic Area.

The existing liability framework comprises:

- the partially harmonised EU legislation on liability for defective products (Directive 85/374/EEC), applicable to any product marketed in the European Economic Area, harmonising at EU level the claims against the producer for damage caused to a consumer due to the defectiveness of a product. The producer is strictly liable for damage caused by a defect in their product, provided that the injured party proves the damage, the defect and the causal link between the two. The Directive applies to a vast range of products, including complex AI-driven devices.
- National liability regimes, which are still fragmented, lacking of clear liability rules specifically applicable to damage resulting from the use of emerging digital technologies such as AI (with the limited exception of highly or fully automated vehicles). Nowadays, the harmful effects of AI can be compensated under the tort law of EU Member States, which is largely non-harmonised (with the exception of product liability law under Directive 85/374/EC) and this might give rise to different outcomes depending on which jurisdiction is applicable. Part of the liability claims for damages caused by products and services are based on a liable person's conduct ('fault-based liability'), such as a producer, service provider or individual user of a product, whilst others claims are independent by the fault ('strict liability'), being the person identified by law (usually the operator, user or owner) held liable independently of fault.

Within the evolving regulatory framework under development, the issue of civil liability for AI systems is addressed by:

- AI Act
- Revised Product Liability Directive
- AI Liability Directive

[10] AI REGIO D7.1

AI Act [11]

As regards the issue of civil liability for AI systems, the AI Act imposes specific obligations upon providers, importers, users, distributors, and even third parties (Articles 16 to 29). It follows the approach established in the October 2020 (in the Resolution of the European Parliament on the civil liability regime for AI), based on the assumption that "AI-systems have neither legal personality nor human conscience".
The Recital 53 sets that "it is appropriate that a specific natural or legal person, defined as the provider, takes the responsibility for the placing on the market or putting into service of a high-risk AI system, regardless of whether that natural or legal person is the person who designed or developed the system."
The AI Act opts for a risk-based approach, aiming at classifying the AI applications according to a typology of risks from none to high-risk, in line with both the Report on the civil liability regime for AI and the White Paper. The classification of the risks according to the AI Act is as follows[12]:

- i) unacceptable risk AI systems, with harmful uses of AI that contravene EU values. These systems are banned, with some exceptions;
- ii) High risk AI systems, negatively affecting safety or fundamental rights, for which a range of mandatory requirements (including a conformity assessment) are foreseen. All high-risk AI systems will be assessed before going to the market and throughout their lifecycle. "High-risk" AI-system means "a significant potential in an autonomously operating AI-system to cause harm or damage to one or more persons in a manner that is random and goes beyond what can reasonably be expected; the significance of the potential depends on the interplay between the severity of possible harm or damage, the degree of autonomy of decision-making, the likelihood that the risk materialises and the manner and the context in which the AI-system is being used". To determine whether an AI-system is high-risk, it is necessary to take into account also the sector in which significant risks could arise and the nature of the activities to be undertaken. The AI Act provides a list of high-risk applications, sets clear requirements for AI systems for high risk applications and defines specific obligations for AI users and providers of high risk applications, besides a conformity assessment before the AI system is put into service or placed on the market, as well as enforcement after such an AI system is placed in the market and a governance structure at European and national level.
- iii) Limited risk AI systems, such as those that generate or manipulate image, audio or video content, are subject to a limited set of obligations (e.g. transparency);
- iv) Minimal risk AI systems. Comprising all other AI systems, can be developed and used in the EU without additional legal obligations than existing legislation.

The operator of the "High-risk system" is subject to strict liability for any damage that results in harm to life, health, damage to property or harm that results in economic loss. In other words, the strict liability regime applies and they will be liable for any harm caused by an autonomous activity, device or process driven by their AI system, even if they did not act negligently. In case of more than one operator, all operators are jointly and severally liable, and have the right to recourse proportionately against each other.
The AI Act defines the "Operator" as "both the frontend and the backend operator as long as the latter's liability is not already covered by the Product Liability Directive". The frontend operator is "any natural or legal person who exercises a degree of control over a risk connected with the operation and functioning of the AI-system". The backend operator is "the natural or legal person who, on a continuous basis, defines the features of the technology, provides data and essential backend support service and therefore also exercises a degree of control over the risk connected with the operation and functioning of the AI-system".
Considering that the operator can exercise a certain level of control over the risk that the item poses, any of his/her action might affect the manner of the operation from the beginning to the end, by determining the input, output or results, or might change specific functions or processes within the AI-system.

[11] Regulation (EU) 2024/1689

[12] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Revised Product Liability Directive (RPLD) Proposal[13]

This proposal, together with the AI Liability Directive, was adopted by the European Commission in September 2022 to adapt liability rules to the digital age, circular economy and the impact of global value chains, bringing the EU's liability regime up to speed with the digital age. Both of them will now needed to be adopted by the European Parliament and the Council.

This instrument is aimed at modernizing the liability rules for products in the digital age, in particular the rules on the strict liability of manufacturers for defective products. The final aims is to provide the businesses with legal certainty and to ensure that victims get fair compensation when defective products cause harm.

It covers all tangible and intangible unsafe products, including embedded or standalone software and digital services necessary for the products' functioning.

The existing rules, based on the strict liability of manufacturers, for the compensation of personal injury, damage to property or data loss caused by unsafe products, are updated and reinforced. Its provisions include, among others:

i) allowing compensation for damage when products like robots, drones or smart-home systems are made unsafe by software updates, AI or digital services that are needed to operate the product, as well as when manufacturers fail to address cybersecurity vulnerabilities. The products in scope include all products placed on the market or put into service in the course of commercial activity. The meaning of "product" includes digital manufacturing files (e.g. for 3D printers), software and AI-systems.

ii) alleviating the burden of proof for victims in complex cases, such as those involving AI. In certain circumstances, the burden of proof could be eased by the Courts, including in technically complex cases where it would be difficult for the victim to prove liability (including cases involving AI, as highlighted in the accompanying document). In five scenarios, where the causal link between defectiveness and damage is impossible to prove due to the technical or scientific complexity of the product, it is presumed. This last scenario is aimed to prevent the so-called 'black box' effect of AI systems: in such circumstances, the claimant will only need to prove that the AI at hand contributed to the damage and that the product is likely to be defective.

iii) as regards the time limit for bringing claims, it is still 3 years (from the earlier of either the day on which the claimant becomes aware, or should reasonably have become aware, of the damage, the defect and the identity of the relevant economic operator who is liable). However, the liability period expires after ten years since the defective product was placed into the market or, in case the injury is not immediately apparent, after 15 years;

iv) the existing strict liability (i.e. no fault) regime for defective products across the EU (meaning claimants seeking compensation for defective products across the EU do not need to establish fault to claim successfully) extended as regards the scope of claims that can be brought and the range of damages that can be recovered, whilst it is simplified for consumers to prove their case. The strict liability also applies for defects resulting from cybersecurity risks, connectivity risks, software updates (or lack of updates), with limited exceptions for software updates beyond a manufacturer's control, e.g. due to the user not installing the update.

v) The recoverable damages are extended from personal injury, death and damage to personal property and now includes loss or corruption of data and medically recognised harm to psychological health.

vi) The extension of the non-exhaustive list of factors to take into account in assessing defect, including, for instance, product safety requirements (including safety-relevant cybersecurity requirements), foreseeable misuse and self-learning abilities.

[13] COM (2022) 495 final, "Proposal for a Directive of the European Parliament and of the Council on liability for defective product"

AI Liability Directive (AILD) Proposal

This proposal is meant to provide a new set of liability rules specifically targeted at AI, tackling consumers' liability claims for damage caused by AI-enabled products and services. It will complement the AI Act, setting a new liability regime for ensuring greater legal certainty and so enhancing consumer trust in AI.

Under most of the national liability rules, currently in place across the EU Member States, the victims bear the burden of proof a wrongful action or omission of an action by a person who caused the damage and this is complex (or even impossible) in case of AI systems, often characterized by 'black box' effect or, at least, high complexity. Therefore the current framework is not sufficient for adequately dealing with liability claims for damage caused by AI-enabled products and services. Furthermore, the overall framework on liability for AI-caused damages is, as mentioned before, fragmented and doesn't ensure legal certainty, rotating around a case-by-case approach: the national courts have to adapt the way in which they apply existing rules, making it difficult for businesses to predict how existing liability rules might be applied, as well as to assess and ensure their exposure to potential liability claims. This situation might hinder the innovation of European businesses.

The AILD proposal, with the main objectives of making it easier for victims of AI-related damage to get compensation and to ensure that victims benefit from the same standard of protection across the EU when harmed by AI products or services, sets for the first time a targeted harmonisation of national liability rules for AI, laying down uniform rules for access to information and alleviation of the burden of proof for damages caused by AI systems.

It also aims to ensure an easier access to redress for the victims and provides broader protection for victims (individuals or businesses), whilst increasing guarantees.

In particular, the AILD provides:

- the **right of access to evidence**: subject to certain conditions, a court (or, in limited circumstances, third parties) can order to a provider of a high-risk AI system (defined in the EU AI Act) to disclose relevant and necessary evidence about their product. Furthermore, the victims have the right of access to evidence from companies and suppliers when high-risk AI is involved;
- a rebuttable **presumption of causality**, when a relevant fault has been established and a causal link to the AI performance seems reasonably likely. This is expected to simplify the legal process for victims, who are experiencing difficulties in explaining in detail how harm was caused by a specific fault or omission (this can be hard in case of complex AI systems). However, there is the right to fight a liability claim based on a presumption of causality, seeking a balance between protecting consumers and fostering innovation. Subject to certain conditions and in narrow circumstances, national courts will presume, for the purposes of applying liability rules to a claim for damages, that the output produced by the AI system (or the failure of the AI system to produce an output) was caused by, for example, the fault of the AI provider. Following a long debate as to who should be accountable in the event of a failure by an AI system, the AILD concludes that it should be the providers of AI systems and, in some cases, the user of AI systems (each as defined in the EU AI Act).

Both the updated product liability rules and the AI Liability Directive reverse the burden of proof for damage caused by AI applications (such as cobots) under certain conditions but, whilst the Product Liability Directive is based on strict liability (meaning the presumption of malfunctioning applies under specific condition, and constitutes a legal basis for claims), the AILD merely harmonises certain aspects of legal proceedings initiated under national fault-based liability regimes and requires the complaint to prove the defendant is at fault for breaching the requirements of the AI Act.

III. Data ownership

Important critical barriers and uncertainties to the development of the data economy and the use of IoT, robots and autonomous systems pertain to the regulatory and ethical challenges related to share, access or (re-)use of third party data and the data ownership. They are an impediment to data sharing. Data are

nowadays considered a resource in their own right, have their own commercial value and their importance is growing: they are seen as the "new oil". Data, unlike oil, might be used by multiple actors and for multiple purposes.

In the European manufacturing industry and its shift to the Industry 4.0 and 5.0 vision, the digitalization is gaining relevance to face the increasingly competitive global landscape. In this context, the data exchange within factories and in the wider manufacturing ecosystems, the data are expected to improve the operations and contributing to the strategic positioning of the companies.

The three main categories of stakeholder involved in the Data Economy are:

- Actors co-producing data (product/service providers and product/service users), with a different degree of control over the data: usually, the product/service provider retains the greatest degree of control over the data, whilst the user has more limited control. These two players are the most relevant "data sharers" and the debate on "data ownership" mainly affects them;
    - Actors interested in accessing data (providers' competitors and same sector down-stream providers), which are economic players (most often in the same value chain) that need the data for their business. They can also be competitors of the service producer and players downstream or upstream in the same value chain, despite they do not participate in the production of data. This category is the one suffering most from lack of access to data as their business model depends on the availability of them: they are especially interested in the access to data and in the terms and conditions of access, rather than in the data ownership itself.
    - Actors interested in re-using data, not necessarily in the same sector (data analytics companies and re-users of public interest data, but also universities, statistical offices etc.). The lack of data aggregation from many sources is suffered by data analytics companies is detrimental to development of innovative artificial intelligence solutions. On the other hand, data scientists might need the access to the data held by private players for reasons of public interest and for tackling with societal challenges.

The concept of "ownership" is not clearly defined, considering that there is no an official legal definitions of it. The working definition of data ownership is an alienable legal construct allowing one or more persons (the owners) to control access to or use of a single piece or set of data, excluding others.

There is also legal uncertainty surrounding data ownership in the manufacturing domain in relation to data produced by machines or devices, as well as non-personal data. Besides the uncertainties about the concept of "ownership'" of data, there are barriers to access and (re-)use of data, which are perceived as far more important. Many companies' worry of sharing sensitive information and losing their competitive advantage and do not feel confident in sharing their data, beyond what is legally binding, with other downstream players in the same value chain.

The machinery data in global value chains might be generated by component suppliers, customers, and other sub-contracted service suppliers, such as through sensors in the production chain, or in the after sales services, or through additional services, with smart machines coordinating manufacturing processes by themselves, smart service robots cooperating with people on assembling the products, and smart (driverless) transport vehicles covering the logistics side on their own.

Data generated in the Industry 4.0/Industry 5.0 dynamic value networks can be analysed by a third party service provider and be sent back to the respective client. They can also, once anonymized, be sent to the whole sector platform community (or other third parties) within the global value chains. The free movement of the different types of data originated at each step of such global value chain is essential to any efficient production process, also remotely monitoring and maintaining the machines including the transfer at least some rudimentary data across production sites and most likely across countries.

The main open questions regard what is the legal basis of the ownership claims, who "owns" data and what data "ownership" entails and which kind of protection should be sought.

As regard the legal basis, there are different approaches, ranging from the Confidential information/Trade secrets (data may be protected as confidential information in certain circumstances, described in article 39(2) of the TRIPS Agreement), the Copyright in Data (copyright law represents therefore an important source of

contemporary claims to ownership rights in data), the need for enacting s "Sui generis" right in data and the contract law (individual contracts already cover data ownership, exchange, access to and use of data among the actors along the value chain)
Manufacturers often seem to want to control data within the boundaries of their machines but also beyond, i.e. via a platform. The data generator can give access to "machine data" on a contractual basis to anyone.
There are still many challenges and concerns around data exchange and data ownership.
However the contractual approach seems to currently be the more adopted and it is often link with technical solutions capable of enforcing it. Currently, there is strong reliance on contractual tools for sharing and accessing data and it is likely that these tools will remain the key vehicle for organizing and regulating commitments within the Data Economy[14] [5].
This is linked to the data sovereignty concept and standard[15] [6]. The data sovereignty concept offers the opportunity of sharing data in a secure and sovereign manner, providing the trust and security between partners in a data centered ecosystem. The Data sovereignty relates to both access control and usage control. The owner can decide with whom, how long and under which conditions he wants to share his data and he also can control the further usage of the data, once the data has been accessed.
The technical infrastructure should be able to enforce data sovereignty, facilitating through flexible and pragmatic solutions the execution of contractual provisions on the use of data. These provisions can enforce the data policies in terms of processing, allow (or disallow) linkage or analysis of data-by-data users, or allow (or disallow) third parties access to data, and other use limitations, flow control, data transfer restrictions, etc.
The successful data sharing in industrial contexts could therefore rely on the data sovereignty concept as described by the International Data Spaces (IDS): this would enable the manufacturing companies to retain control over the collection and usage of their data and, as a consequence, to scale and grow with data.
In this environment, IDS-RAM and DIN SPEC 27070 standard[16] [6]come at stake: the former is the reference architectural model for data sovereignty, used when interchanges are desired to be carried out maintaining the property and governance of those items to be exchanged (data, models, etc.). The latter is the IDS standard, published on February 21st, 2020.
The contractual approach implies that data ownership, as well as data access and (re-)use, will remain defined with pragmatic and de facto arrangements on a case-by-case basis and through bilateral relations.

IV. Privacy, Data protection, risk of stigmatization and social sorting, risk of algorithmic biases

Other legal and ethical challenges relevant to the human-machine-interaction technologies and human-centric aspects of AI-based manufacturing systems within AI REDGIO 5.0 regard the Data Protection and Privacy and the related risk of stigmatization and social sorting.
The Human-machine CI workplace requires to ensure that participants are aware that their data are being collected and give informed consent to this.
In the workplace, the employees still expect a certain level of privacy. Nevertheless, the concepts of privacy and trust requires some evolution as CI tools and robots become part of our employees' daily life and workplace: industrial devices and machines are capable of recording everything, being often equipped with sensors and they will likely be able in the future to read minds using electroencephalogram (EEG). The cobots collect data to adapt to the abilities, work-rate and needs of their human coworkers. The full exploitation of the potential of the CI paradigm along the human-manufacturing system interaction in the project entails the data collection, processing and use in several ways: it regards the real-time monitoring solution of the

[14] Martina Barbero, Diana Cocoru, Hans Graux and other, "Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability. Study prepared for the European Commission DG Communications Networks, Content & Technology by Deloitte", 2017; Teresa Scassa, "Data Ownership", CIGI Papers No. 187, 2018

[15] IDSA, "Data Sovereignty – Critical Success Factor for the Manufacturing Industry", 2021; IDSA, «White Paper "Sharing data while keeping data ownership. The potential of IDS for the data economy,» 2018.

[16] IDSA, «DIN SPEC 27070,» 2021.

human-centered processes, as well as the worker's digital replica/twin to capture worker's skills, preferences, even the mood, fear/excitement and the analysis of the past behaviour. This will enable a continuous and autonomous improvement of the collaboration. The in-depth consideration of the human component within the Digital Twin (DT) loop enables to tailor the interaction modalities to the status, preferences and behaviour of a person: this also requires for additional personal data collection and use, towards the successful human-centric engineering and adaptive automation that fits the specific needs of different employees (e.g. for novice, older and disabled people)[17] [4]. This includes for instance "the human role, goals and tasks; demographics, key anthropometrics, functional (sensorial, physical and cognitive) capabilities; knowledge and skills; needs and preferences; physical, cognitive and emotional status (e.g., based on physiological measures) & dynamic behaviours"[18] [4]. The collected data can be processed in cloud services. The data themselves and the models/insights derived from them can be stored and used by other machines within robot systems consisting in a network of distributed processes.

In the AI REDGIO 5.0 environment the machines might be able to capture data about people, besides about equipment and environments: it is therefore key using data ethically and in an informed manner. The participants have to be clearly aware that data were being collected, handled and stored and the AI REDGIO Consortium is committed in ensuring this. Nevertheless, there might be challenges, especially after the end of the project during the uptake of the solutions in real industrial plants, in gathering informed consent according to the European Data Protection Framework (GDPR) and in be compliant with the underlying ethical principle for these data collection, processing and storage.

In addition, the employee can change their behaviour in the field when they are aware to be monitored or observed, also considering that the AI systems, which often evaluates performance and are designed to better fit to the human co-worker, can be perceived as a treat and the workers could worry about being stigmatized for their performance (with the consequent mental stress of being held to the productivity standards of a robot)[19] [5]. The work environments can be perceived as coercive and the workers may feel under pressure/forced to conform to what the management asks, suppressing their desire to avoid surveillance/observation for the fear of being negatively evaluated: the worker may be implicitly pushed by the working environment to adopt the innovating technologies.

Furthermore, it must be ensured that the system does not infringe human rights and avoid algorithmic biases, for instance towards groups or races. This also applies to datasets, in case of data-driven models. For instance they have contain both male and female participants, with different anthropomorphic structures and have to take into account individual differences and providing models respecting such differences, without privileging one group.

Special attention for addressing the challenges which might arise regarding the personal data will be given to the GDPR ("General Regulation on data protection") provisions, to the "ePrivacy Directive" (Directive 2002/58/EC on privacy and electronic communications) and the standardization projects of the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, namely those on Transparency, Accountability and Openness (IEEE P7001™) and Protection of Personal Data (Data Privacy Process, IEEE P7002™; Data Governance in the workplace, IEEE P7005™; Personal Data AI Agent, IEEE P7006™).

As regards the GDPR[20], it sets a comprehensive framework aimed at ensuring that personal data enjoy the same high standard of protection everywhere in the EU, giving back individual the control over his/her personal data.

V. Psychological issues

[17] Gianfranco Modoni, Marco Sacco, AI REGIO D5.1 "Collaborative Intelligence and Industry 5.0", 2021

[18] Gianfranco Modoni, Marco Sacco, AI REGIO D5.1 "Collaborative Intelligence and Industry 5.0", 2021

[19] Gordon Briggs, Matthias Scheutz, "How Robots Can Affect Human Behavior: Investigating the Effects of Robotic Displays of Protest and Distress", 2019

[20] "General Regulation on data protection 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", repealed the Directive 95/46/EC

Another important aspect to take into account regards the possible phycological issues on the workforce, resulting from the Human-Machine interaction in the CI-driven environment within an industrial setting.
The main psychological issues are:

- *"robophobia" or a "technostress",* consisting in the risk that workers experience increasing stress when working with a robotic partner, which might generate a decrease of their engagement and pleasure in performing their tasks, as well as of the satisfaction at work. They might feel less useful and in control at work and not comfortable, as well as there might be a sort of mistrust towards robots when the workers must share decisions with machines, since they might be perceived as antagonists, even in collaborative scenarios. These psychosocial factors of stress might increase the risk of developing musculoskeletal disorders (MSD) at work, which are more often evaluated in relation to the exposure to biomechanical factors capable of generating them (high efforts and awkward postures). it is important to leave job control (such as the work pace) to the worker and preserve some "human added value" in one's job. It is related to the mental health and well-being of the workers, which relies also on self-esteem. In human-robot co-working environments where robots are placed in positions complementing what humans do, humans will likely not feel threatened by robots (the machines will help humans in completing tasks without the burden of managing a human assistant, leaving more time for tasks requiring creativity and higher intelligence). On the contrary, the humans' reaction is still unclear in case robots take positions that humans compete for. However, this aspect arises especially for future scenarios, not within AI REDGIO 5.0. This issue is not expected to be likely in case of AI REDGIO 5.0, considering the human-centric approach and the vision towards empowering humans;
- *Risk of the so-called "Master-Slave dependency"*, regarding the human temptation to delegate more and more functions and tasks to machines even without a real need, with the risk of become progressively dependent on the machines and of loss of skills to carry out the allocated functions and tasks, which might be important in case a problem occurs;
- *Risk of Emotional Dependency,* concerning the tendency, especially if a machine is perfectly tuned and adapted to support humans, to develop a kind of empathy and thankful emotion towards the machine, as well as the increase of people's expectations about machines' capacities. In the CI workplace, where people and machines interacts on a regular bases through human-centered model in an increasingly complex and humanlike flavour, some workers could start to develop some kind of relationship with the machines. In addition, there is the risk of creation of emotional dependence, accompanied by overconfidence in the ability of the machine to solve problems and facilitate one's tasks, even in unexpected situations. This might diminish the social abilities of the operator, who could find it easier and more enjoyable to interact with a machine, rather than with humans. The emotional or social bonds between humans and machine paves the way for the risk of social isolation and of diminished willingness to deal with the complexity of real human relationships. The ethical acceptability of the subtle form of deception related to the subconscious processes involved in human–robot interactions, in particular related to the human attitude to form unidirectional emotional bonds with the technological artefacts.

V. Generative AI

"Generative AI refers to the use of AI to create new content, like text, images, music, audio, and videos: the GenAI models are trained on very large datasets from which they learn the patterns and structure and then generate new synthetic content that has similar characteristics" [12]. The GenAI systems are a specific subset of foundation models "specifically intended to generate, with varying levels of autonomy, content such as complex text, images, audio or video".
Generative AI, underpinned by new foundation models and yielding output based on patterns and insights gleaned from vast amounts of data, is reshaping the manufacturing domain, offering unprecedented opportunities for revolutionizing various aspects of manufacturing enhancing the quality and efficiency of

work and bringing innovation in product design, process optimization and supply chain management, whilst potentially increasing job satisfaction by automating mundane tasks and enabling focus on meaningful work. Thus, the integration of AI presents an opportunity to enhance the quality and efficiency of work across a multitude of sectors. By automating routine and mundane tasks, AI can potentially allow workers to focus on the core aspects of their roles that require human insight, creativity, and specialized skills.
The potential applications of GenAI in manufacturing include[21]:

- Product Design and Development, where GenAI can rapidly create and refine product designs, significantly accelerating the design process for manufacturers and taking into account performance requirements, manufacturing constraints, cost factors and other parameters;
- Process Optimization, where suggestions for optimizing the manufacturing processes — including machine settings, production schedules and resource allocation- might be elaborated but the GeNAI by analyzing vast amounts of production data. This might lead to increased efficiency, reduced waste and improved overall productivity;
- Quality Control, where the use of GenAI can create sophisticated models for predicting and detecting defects in real time, as well as can provide optimal inspection strategies. This might lead to higher product quality, whilst reducing the time and cost associated with quality control processes.
- Predictive Maintenance, where GenAI can be used to generate models that can predict equipment failure and thereby enable manufacturers to implement proactive maintenance strategies. This might lead to the reduction of downtime and to the extension of the equipment lifespan;
- Supply Chain Management, where GenAI can create models for demand forecasting, inventory optimization and risk assessment. This might lead to allow the manufacturers to effectively navigate complex global supply chains;
- Decarbonization, where GenAI can boost decarbonization efforts thanks to its ability to design more environment-friendly products and processes requiring minimum energy. This might lead to the reduction of the overall environmental impact of manufacturing operations.

For predictive maintenance and quality control, the advanced capabilities of GenAI can be used for data integration, pattern recognition from historical data, predictive modeling based on patterns, as well as real-time monitoring and alerts.
The automation of routine and mundane tasks potentially allow workers to focus on the core aspects of their roles, requiring human insight, creativity, and specialized skills. This is in line with the CI vision.
Thanks to the implementation of GenAI, the manufacturers are expected to not only enhance their current operations but also to unlock new possibilities to create value and drive progress. This will provide significant competitive advantages in efficiency, decarbonization goals and market responsiveness.
Despite these advantages and benefits, the adoption of GenAI in manufacturing raises several challenges and concerns, ranging from data quality, to system integration, and cost of acquisition and implementation, which can represent a deterrent to the adoption of GenAI. They include, for instance, the skill gaps, due to the shortage of experts with the required skillsets to develop, implement, and maintain generative AI systems in manufacturing, as well as the resistance to the adoption of this kind of solutions, particularly in critical situations and due to the lack of transparency of some AI models, and the need to adopt change management strategies to pre-existing processes and workflows. Furthermore, the limitations of GenAI include a propensity for bias in the outputs, reflecting biases present in training data, as well as the GenAI systems can also give rise, in some cases, to unpredictable or nonsensical results, due to their reliance on patterns in data rather than true comprehension. GenAI might also be susceptible to hallucinations, or instances where the AI systems produce false or misleading information, due to the misinterpretation of their training data or to attempt to fill gaps in their knowledge.
However, in order to fully leverage the power of GenAI, the manufacturers must address several challenges, as described above. It is important to understand these limitations for maximizing GenAI's benefits while mitigating the potential risks. Legal and ethical considerations have therefore to be considered, including

[21] https://www.gep.com/blog/how-generative-ai-reshaping-manufacturing

intellectual property rights, liability for AI-generated designs or decisions, and the ethical implications of AI-driven automation on the workforce.
Furthermore, it is important to take into account the AI Act provisions concerning the GenAI, as well as the indications set by the "Living guidelines on the responsible use of Generative AI in research" [13].

4.2. Ethical and legal reference framework

The key European legal, regulatory and ethical sources relevant for AI REDGIO 5.0 system and technological assets, functional also to address the challenges described in the previous paragraph, are described below. They have been taken into consideration to elicit the legal and ethical requirements outlined in the next paragraph and will be monitored in the next phase of the project, in order to get aligned with their provisions.

Artificial Intelligence

AI Act (AIA), Regulation (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
The AI Act builds upon the European Commission's White paper on AI and is the first-ever legal framework for AI, moving forward towards trustworthy and ethical AI systems in the European market.
It follows a balanced approach to innovation, safety, security, and privacy.
On 8 December 2023 a provisional political agreement on the wording of the AI Act was reached by the European trilogue (European Commission, the Council of the European Union and the European Parliament), paving the way to the acceptance by the European Parliament and Council to become law.
On 2 February 2024 the representatives from member states unanimously voted on the adoption of the EU AI Act, thereby confirming such political agreement.
On 21 May 2024 the European Council gave its final endorsement for the EU AI Act to be signed into law.
On 13 June 2024 the AI Act was formally signed.
On 12 July 2024, the AI Act has been published in the EU's Official Journal and will take effect in 20 days.
From the date of the entry into force, the following milestones will follow according to Article 113:

- 6 months later – Chapter I and Chapter II (prohibitions on unacceptable risk AI) will apply.
- 12 months later – Chapter III Section 4 (notifying authorities), Chapter V (general purpose AI models), Chapter VII (governance), Chapter XII (confidentiality and penalties) and Article 78 (confidentiality) will apply, with the exception of Article 101 (fines for GPAI providers).
- 24 months later – The remainder of the AI Act will apply, except;
- 36 months later – Article 6(1) and the corresponding obligations in this Regulation will apply.
- Codes of practice must be ready 9 months after entry into force according to Article 56.

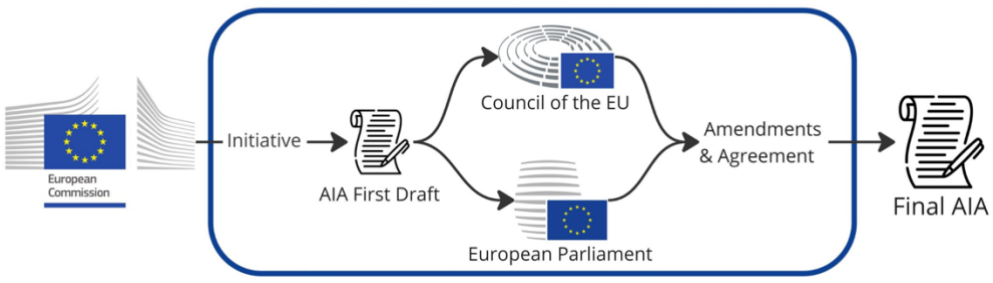

Figure 3: **A high-level view of the Ordinary Legislative Procedure by which the AI Act was formed (source: *https://artificialintelligenceact.eu*)**

Among the key provisions of the AI Act, in relation to AI REDGIO 5.0 it is worth mentioning[22]:

- **Classification of the AI systems according to their risks**. The AI Act classifies AI according to its risk, rotating around the so-called risk-based approach. It classifies the AI applications according to a typology of risks from:
  I. **unacceptable risk AI systems**, which implies harmful uses of AI, contravening the EU values. These systems are banned, with some exceptions; The prohibited AI systems (Chapter II, Art. 5) include, among others, the AI systems:
     - social scoring, i.e., evaluating or classifying individuals or groups based on social behaviour or personal traits, causing detrimental or unfavourable treatment of those people;
     - inferring emotions in workplaces or educational institutions, except for medical or safety reasons;
     - "real-time" remote biometric identification (RBI) in publicly accessible spaces for law enforcement, except in limited cases

  II. **High risk AI systems**, negatively impacting fundamental rights and safety. Several mandatory requirements (including a conformity assessment) are provided for them. All high-risk AI systems will be assessed before going to the market and throughout their lifecycle. The High risk AI systems (Chapter III) are those (Art. 6):
     - used as a safety component or a product covered by EU laws in Annex I and required to undergo a third-party conformity assessment under those Annex I laws; or
     - those under Annex III use cases (below), except if: i) the AI system performs a narrow procedural task; ii) improves the result of a previously completed human activity; ii) detects decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review; or iv) performs a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III;
     - AI systems are always considered high-risk if it profiles individuals, i.e. automated processing of personal data to assess various aspects of a person's life, such as work performance, preferences, reliability, behaviour, location or movement. Among the use cases under Annex III, the following might be relevant for AI REDGIO 5.0:
       - Non-banned biometrics: Remote biometric identification systems, excluding biometric verification that confirm a person is who they claim to be. Biometric categorisation systems inferring sensitive or protected attributes or characteristics. Emotion recognition systems;
       - Critical infrastructure: Safety components in the management and operation of critical digital infrastructure and the supply of water, gas, heating and electricity;
       - Vocational training: AI systems determining access, admission or assignment to vocational training institutions at all levels. Evaluating learning outcomes, including those used to steer the student's learning process;
       - Employment, workers management and access to self-employment: AI systems used for recruitment or selection, particularly targeted job ads, analysing and filtering applications, and evaluating candidates. Promotion and termination of contracts, allocating tasks based on personality traits

[22] https://artificialintelligenceact.eu

or characteristics and behaviour, and monitoring and evaluating performance.

In case the providers whose AI system falls under the use cases in Annex III believe it is not high-risk, they have to document such an assessment before placing it on the market or putting it into service.

III. **Limited risk AI systems**, which for instance generate or manipulate image, audio or video content. For these systems, a limited set of obligations (e.g. transparency) are provided. The developers and deployers must ensure that end-users are aware that they are interacting with AI (such as chatbots and deepfakes).

IV. **iMinimal risk AI systems**. This category comprises all the other AI systems and are the majority of AI applications currently available on the EU single market. They can be developed and used in the EU without additional legal obligations (besides those posed by the existing legislation).

- **the majority of obligations fall on providers (developers) of high-risk AI systems**, including both those that intend to place on the market or put into service high-risk AI systems in the EU and third country providers where the high risk AI system's output is used in the EU. According the the AI Act (Art. 8–17), the requirements for providers of high-risk are the following:
  - Establish a risk management system throughout the high risk AI system's lifecycle;
  - Conduct data governance, ensuring that training, validation and testing datasets are relevant, sufficiently representative and, to the best extent possible, free of errors and complete according to the intended purpose.
  - Draw up technical documentation to demonstrate compliance and provide authorities with the information to assess that compliance.
  - Design their high risk AI system for record-keeping to enable it to automatically record events relevant for identifying national level risks and substantial modifications throughout the system's lifecycle.
  - Provide instructions for use to downstream deployers to enable the latter's compliance.
  - Design their high risk AI system to allow deployers to implement human oversight.
  - Design their high risk AI system to achieve appropriate levels of accuracy, robustness, and cybersecurity.
  - Establish a quality management system to ensure compliance.
- **Users are natural or legal persons deploying an AI system in a professional capacity**: they are not the affected end-users. In particular, the users (deployers) of high-risk AI systems have some obligations, though less than providers (developers). Such obligations apply to users located in the EU, and third country users where the AI system's output is used in the EU.
- **General purpose AI (GPAI)**: GPAI model is an AI model displaying significant generality and capable to competently perform a wide range of distinct tasks, regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. A GPAI system is an AI system based on a general purpose AI model, with the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems. The GPAI model providers must provide technical documentation, instructions for use, comply with the Copyright Directive, and publish a summary about the content used for training. Free and open licence GPAI model providers only need to comply with copyright and publish the training data summary, unless they present a systemic risk. In case of GPAI models that present a systemic risk – open or closed, the providers must also conduct model evaluations, adversarial testing, track and report serious incidents and ensure cybersecurity protections. During the lifetime of AI REDGIO 5.0 the provisions regarding the GPAI are not applicable, since they apply only to AI models that are used before release on the market for research, development and prototyping activities. GPAI systems may be used as high risk AI systems or integrated into them.

The AI Act will be updated, amended and implemented through implementing acts and delegated acts. The former tend to focus on implementation of the act (such as by providing official guidance on compliance). The latter are closer to legislative amendments, changing details written into the AI Act. Both are powers given to the Commission to update the act in response to technological developments, as well to provide non-essential details at a later date. Furthermore, the AI Office is expected to continue bringing expertise to the EU and advise on some implementing and delegated acts, as well as on many other areas where expertise might be needed during implementation and enforcement.

The AI@EC Communication(COM(2024) 28 final) was adopted in January 2024 and outlined the Commission's strategic vision to foster the internal development and use of lawful, safe and trustworthy AI systems, preparing internally for the implementation of the AIA. On the other hand, pending the formal adoption of the AI Act, the AI Pact was adopted, which anticipated the implementations of some AI Act requirements with voluntary companies.

Furthermore, the AIA gave relevance to the recognized standards on AI, which are expected to be generated in the next couple of years by the European Standard Organisations (ESOs), such as CEN/CENELEC and ETSI, in response to the AIA provisions.

Other important provisions regard the AI Regulatory Sandboxes (Title V, art. 53 ss.), which are expected to be key to support companies, especially SMEs and start-ups, in applying the AIA provisions during this transition period. The Spanish AI Sandbox Pilot was the first of these instruments: it was launched in November 2023 and will run until 2025.

AI Liability Directive (AILD) Proposal, COM (2022) 496 final "Proposal for a Directive of the European Parliament and of the Council on adapting non- contractual civil liability rules to artificial intelligence". It lays down uniform rules for certain aspects of non-contractual civil liability for damage caused with the involvement of AI systems for ensuring that persons harmed by AI systems enjoy the same level of protection as persons harmed by other technologies. Despite the AILD was published as part of a package proposal alongside the PLD, the PLD has outpaced in its development: it seems unlikely the AILD will be agreed before the end of the current term summer 2024.

The AILD is meant to provide a new set of liability rules specifically targeted at AI, tackling consumers' liability claims for damage caused by AI-enabled products and services. It will complement the AI Act, setting a new liability regime for ensuring greater legal certainty and so enhancing consumer trust in AI.

Under most of the national liability rules, currently in place across the EU Member States, the victims bear the burden of proof a wrongful action or omission of an action by a person who caused the damage and this is complex (or even impossible) in case of AI systems, often characterized by 'black box' effect or, at least, high complexity. Therefore the current framework is not sufficient for adequately dealing with liability claims for damage caused by AI-enabled products and services. Furthermore, the overall framework on liability for AI-caused damages is, as mentioned before, fragmented and doesn't ensure legal certainty, rotating around a case-by-case approach: the national courts have to adapt the way in which they apply existing rules, making it difficult for businesses to predict how existing liability rules might be applied, as well as to assess and ensure their exposure to potential liability claims. This situation might hinder the innovation of European businesses.

The AILD proposal, with the main objectives of making it easier for victims of AI-related damage to get compensation and to ensure that victims benefit from the same standard of protection across the EU when harmed by AI products or services, sets for the first time a targeted harmonisation of national liability rules for AI, laying down uniform rules for access to information and alleviation of the burden of proof for damages caused by AI systems.

It also aims to ensure an easier access to redress for the victims and provides broader protection for victims (individuals or businesses), whilst increasing guarantees.

In particular, the AILD provides:

- the **right of access to evidence**: subject to certain conditions, a court (or, in limited circumstances, third parties) can order to a provider of a high-risk AI system (defined in the EU AI Act) to disclose

relevant and necessary evidence about their product. Furthermore, the victims have the right of access to evidence from companies and suppliers when high-risk AI is involved;

- a rebuttable **presumption of causality**, when a relevant fault has been established and a causal link to the AI performance seems reasonably likely. This is expected to simplify the legal process for victims, who are experiencing difficulties in explaining in detail how harm was caused by a specific fault or omission (this can be hard in case of complex AI systems). However, there is the right to fight a liability claim based on a presumption of causality, seeking a balance between protecting consumers and fostering innovation. Subject to certain conditions and in narrow circumstances, national courts will presume, for the purposes of applying liability rules to a claim for damages, that the output produced by the AI system (or the failure of the AI system to produce an output) was caused by, for example, the fault of the AI provider. Following a long debate as to who should be accountable in the event of a failure by an AI system, the AILD concludes that it should be the providers of AI systems and, in some cases, the user of AI systems (each as defined in the EU AI Act).

Both the updated product liability rules and the AI Liability Directive reverse the burden of proof for damage caused by AI applications (such as cobots) under certain conditions but, whilst the Product Liability Directive is based on strict liability (meaning the presumption of malfunctioning applies under specific condition, and constitutes a legal basis for claims), the AILD merely harmonises certain aspects of legal proceedings initiated under national fault-based liability regimes and requires the complaint to prove the defendant is at fault for breaching the requirements of the AI Act.

Revised Product Liability Directive (RPLD) Proposal, COM (2022) 495 final, "Proposal for a Directive of the European Parliament and of the Council on liability for defective product". Also this instrument is aimed to properly address the needs of the digital age, circular economy business models and global value chains, renovating the existing Product Liability Directive (adopted in 1985).

This proposals, together with the AI Liability Directive, was adopted by the European Commission in September 2022 to adapt liability rules to the digital age, circular economy and the impact of global value chains, bringing the EU's liability regime up to speed with the digital age. Both of them will now needed to be adopted by the European Parliament and the Council. The Parliament confirmed its negotiating position in October 2023, while the Council adopted its negotiating mandate in June 2023. The Parliament and the Council are now working towards a compromise text.

The RPDL addresses liability for products such as software (including artificial intelligence systems) and digital services, affecting how the product works (e.g. navigation services in autonomous vehicles), providing the companies with legal certainty and ensuring that victims get fair compensation when defective products cause harm. It alleviates the burden of proof for victims under certain circumstances and recognize the liability rules for companies that substantially modify products before resale to extend the product lifecycle (circular economy). The recoverable damages comprise not only personal injury, death and damage to personal property, but also loss or corruption of data and medically recognized harm to psychological health. The non-exhaustive list of factors to take into account in assessing defect includes also, for instance, self-learning abilities. This instrument is aimed at modernizing the modernizing the liability rules for products in the digital age, in particular the rules on the strict liability of manufacturers for defective products. The final aims is to provide the businesses with legal certainty and to ensure that victims get fair compensation when defective products cause harm.

It covers all tangible and intangible unsafe products, including embedded or standalone software and digital services necessary for the products' functioning.

The existing rules, based on the strict liability of manufacturers, for the compensation of personal injury, damage to property or data loss caused by unsafe products, are updated and reinforced. Its provisions include, among others:

i) allowing compensation for damage when products like robots, drones or smart-home systems are made unsafe by software updates, AI or digital services that are needed to operate the product, as well as when manufacturers fail to address cybersecurity vulnerabilities. The products

in scope include all products placed on the market or put into service in the course of commercial activity. The meaning of "product" include digital manufacturing files (e.g. for 3D printers), software and AI-systems.

ii) alleviating the burden of proof for victims in complex cases, such as those involving AI. In certain circumstances, the burden of proof could be eased by the Courts, including in technically complex cases where it would be difficult for the victim to prove liability (including cases involving AI, as highlighted in the accompanying document). In five scenarios, where the causal link between defectiveness and damage is impossible to prove due to the technical or scientific complexity of the product, it is presumed. This last scenario is aimed to prevent the so-called 'black box' effect of AI systems: in such circumstances, the claimant will only need to prove that the AI at hand contributed to the damage and that the product is likely to be defective.

iii) as regards the time limit for bringing claims, it is still 3 years (from the earlier of either the day on which the claimant becomes aware, or should reasonably have become aware, of the damage, the defect and the identity of the relevant economic operator who is liable). However, the liability period expires after ten years since the defective product was placed into the market or, in case the injury is not immediately apparent, after 15 years;

iv) the existing strict liability (i.e. no fault) regime for defective products across the EU (meaning claimants seeking compensation for defective products across the EU do not need to establish fault to claim successfully) extended as regards the scope of claims that can be brought and the range of damages that can be recovered, whilst it is simplified for consumers to prove their case. The strict liability also applies for defects resulting from cybersecurity risks, connectivity risks, software updates (or lack of updates), with limited exceptions for software updates beyond a manufacturer's control, e.g. due to the user not installing the update.

v) The recoverable damages are extended from personal injury, death and damage to personal property and now includes loss or corruption of data and medically recognised harm to psychological health.

vi) The extension of the non-exhaustive list of factors to take into account in assessing defect, including, for instance, product safety requirements (including safety-relevant cybersecurity requirements), foreseeable misuse and self-learning abilities.

The **AI innovation package** to support Artificial Intelligence startups and SMEs[23], adopted in January 2024. It comprises an array of measures to support European startups and SMEs to develop trustworthy AI, respectful of EU values and rules. Furthermore, it comprises the amendment of the EuroHPC Regulation to set up AI Factories, expected to be paramount within the EU's supercomputers Joint Undertaking activities with provisions, for instance, on AI-dedicated supercomputers to enable fast machine learning and training of General Purpose AI (GPAI) models. The European AI Start-Up and Innovation Communication foresees additional key activities, such as the "GenAI4EU" initiative, aiming to support the development of novel use cases and emerging applications in Europe's 14 industrial ecosystems (in diversified application areas, such as robotics, biotech, health, manufacturing and mobility), as well as the public sector.

Ethics Guidelines for Trustworthy AI and ALTAI Assessment List.

In 2018 the European Commission appointed an independent High-Level Expert Group on Artificial Intelligence (AI HLEG), made of 52 experts, with the mandate of elaborating ethics guidelines on AI, in order to foster a trustworthy approach towards the responsible and sustainable AI innovation in Europe. The European Commission considered the ethical, trustworthy approach as a core element for positioning Europe and European organizations as global leaders in cutting-edge AI solution.

The HLEG prepared the **"Ethics Guidelines for Trustworthy Artificial Intelligence"** in 2019, taking also into account over 500 recommendations received on the 'Draft Ethics Guidelines' of 2018.

[23] COM(2024) 28 final, Communication on boosting startups and innovation in trustworthy artificial intelligence

Such Guidelines neither are legally binding nor offer advice on legal compliance for AI. They describe ethical principles relevant to build a trustworthy AI, which must display the following three characteristics:

- **Lawfulness**, relying upon the "human-centric approach" to AI, where fundamental human rights are deemed as the foundation of Trustworthy AI. In this direction, the EU Charter and European Convention of Human Rights are considered the key for any legislative source in the field of AI;
- **Robustness**, considering the ability of AI to operate in any situation, especially if unpredictable events or malicious attacks occur;
- **Ethically-soundness**, requiring that technological design, development and use of AI are compliant with the EU ethical values listed in the Guidelines themselves.

The Guidelines identify ethical principles governing AI on the basis of fundamental human rights and translate them into seven requirements that AI systems must fulfill in order to be considered trustworthy:

1. **Human agency and oversight**: AI system must be supportive to human action, human autonomy and decision-making. They have to act "as enablers to a democratic, flourishing and equitable society by supporting the user's agency and foster fundamental rights, and allow for human oversight"[24]. AI systems must promote fundamental rights, benefitting people, reducing risk of infringement on such rights in order to respect the rights and freedoms of others. Any kind of unfair manipulation, deception, herding, diminishing, limiting, or misleading human autonomy and/or conditioning must be avoided. The principle of user autonomy must be central to the AI system's functionality. It is paramount ensuring that the AI technology does not undermine human autonomy or causes other adverse effects: thereby human oversight must be allowed, through governance mechanisms (such as a human-in-the-loop, human-on-the-loop or human-in-command approaches) and in varying degrees, taking into account the application area and the potential risk of the AI solution;
2. **Technical robustness and safety**: safe, reliable algorithms must be in place and must be capable to handle errors or inconsistencies during all phases of the AI systems' life cycle. This is closely linked to the principle of prevention of harm and requires a preventative approach to risks in AI systems' development, so that to reliably behave as intended, whilst minimizing unintentional and unexpected harm. It is important to consider the potential changes in the AI system's operating environment or the presence of other agents (human and artificial) potentially interacting with the system in an adversarial manner.. The AI system must ensure the physical and mental integrity of humans and must be resilient to attack and security, with safeguards for a fallback plan in case of problems.

   Depending on the magnitude of the risk posed by an AI system and on the application area, appropriate level of safety measures must be ensured. The AI system must also be able to make correct judgements, for example to correctly classify information into the proper categories, ensuring accuracy. Its results must be reproducible, exhibiting the same behavior when repeated under the same conditions, as well as reliable, working properly with a range of inputs and in a range of situations and preventing unintended harms.
3. **Privacy and data governance**: in compliance with the GPDR and in line with the principle of prevention of harm, citizens should have full control of their data. The privacy is a fundamental right particularly affected by AI systems. The data must not be used against the citizens or in any discriminatory way. Adequate data governance mechanisms must be adopted, covering the quality and integrity of the data used, their relevance in the specific case, their access protocols and data processing in a manner that guarantee privacy and data protection throughout the AI system's entire lifecycle. The personal data collected must not be used to unlawfully or unfairly discriminate against the data subjects. The quality and integrity of the datasets must be guaranteed, without biases, inaccuracies, errors and mistakes, especially in case of self-learning

[24] HLEG, Ethics Guidelines for Trustworthy AI, 2019.

systems. Proper data protocols governing data access must be foreseen and respected, outlining who can access data and under which circumstances.

4. **Transparency**: It is key to ensure the traceability and explainability of the AI systems, encompassing also transparency of elements relevant to an AI system (the data, the system and the business models). The traceability implies that the datasets, processes and decision of the AI system's decision must be documented to the best possible extent. The explainability refers to the ability of the AI system to explain both the its technical processes and the related human decisions (e.g. application areas of a system): the decisions made by an AI system can be understood and traced by human beings. It must be clear to the humans that they are interacting with an AI system and it must be identifiable as such.

5. **Diversity, non-discrimination, and fairness**: the AI system's lifecycle must ensure inclusion, diversity, equal treatment and access. The inclusive design processes must be followed, avoiding unfair bias, including inadvertent historic bias, incompleteness and bad governance models which could give rise to unintended (in)direct prejudice and discrimination or exacerbate prejudice and marginalization. This is related with the principle of fairness and also pertains to the way in which AI technology is developed: it is key to avoid unfair bias by putting in place proper oversight mechanisms in relation to the system's purpose, constraints, requirements and decisions, as well as to adopt a user-centric approach and to follow the universal design principles. Efforts must be directed to allow to all people to use the AI service, regardless of their age, gender, abilities or characteristics, avoiding one-size-fits-all approach. Stakeholder involvement should be encouraged for this purpose;

6. **Societal and environmental wellbeing**: the sustainability and ecological responsibility of AI systems must be promoted at the maximum extent, as well as measures strengthening the environmental friendliness of AI systems' supply chain. Likewise, the positive social impact and enhancement of social skills must be fostered with a wide perspective taking into account possible effect on democracy and society at large.

7. **Accountability**: the responsibility and accountability for AI systems and their outcomes, both before and after their development, deployment and use, must be ensured. Mechanisms must be put in place on this purpose, including auditability. Auditability entails the enablement of the assessment of algorithms, data and design processes (paying attention to safeguard the business models and intellectual property related to the AI system). It also refers to the evaluation by internal and external auditors with the preparation of evaluation reports, as well as the ability to identify, assess, document and minimize the potential negative impacts of AI systems. The use of impact assessments, such the Algorithmic Impact Assessment, both prior to and during the development, deployment and use of AI tool, is recommended, in a proportionate manner in relation to the risk that the AI systems pose. In case of trade-offs, a rational and methodological approach must be used to tackle with them, explicitly acknowledged and assessed any risk to ethical principles and fundamental rights, with the limit of ethically acceptability. In case of unjust adverse impact, adequate redress mechanisms must exist and be applied.

As regards the **"Assessment List for Trustworthy Artificial Intelligence" (ALTAI) for self-assessment**, it was elaborated by the same the High-Level Expert Group on Artificial Intelligence (AI HLEG) and presented in its final release on the 17 of July 2020, after a piloting process involving over 350 stakeholders. ALTAI is aimed at supporting the actionability of such ethical priciples and requirements, by translating them into an accessible and dynamic checklist. In AI REDGIO 5.0, special attention is and will be given to such principles and requirements, which are at the basis of the Ethics and Data Protection Impact Assessment in WP1 and the Human Rights Impact Assessment on selected AI tools in WP2.

Data

Data Governance Act, Regulation (EU) 2022/868

The DGA, which is already applicable, is functional to oversee the reuse of publicly or protected data across various sectors, facilitating data sharing by the data intermediaries and promoting data sharing for

altruistic reasons and enhancing trust in the sharing and reuse of data. It provides a framework to it make it easier to share data in a trusted and secure manner, enhancing trust in voluntary data sharing for the benefit of businesses and citizens, contributing to exploit the economic and societal potential of data. The DGA is expected to boost the development of trustworthy data-sharing systems, contributing the removing the main barriers to data sharing in the EU (including low trust in data sharing, issues related to the reuse of public sector data and data collection for the common good, as well as technical obstacles), through the following sets of measures:

- Mechanisms to facilitate the reuse of certain public sector data that cannot be made available as open data, such as health data;
- Measures to facilitate data sharing, making it possible for data to be used across sectors and borders, and to enable the right data to be found for the right purpose, also thanks to measures aimed at increasing the trust in data-sharing
- Measures to ensure that data intermediaries will function as trustworthy organisers of data sharing or pooling within the Common European Data Spaces. It states obligations on providers of various types of intermediation services within data-sharing services;
- Measures to make it easier for citizens and businesses to make their data available for the benefit of society, such as the data altruism provisions.
- Measures for giving back the individuals the control on the use of their data;

The definition of data is wide: "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording." Both personal and non-personal data are in scope of the DGA, and wherever personal data is concerned, the General Data Protection Regulation (GDPR) applies: as highlighted in the explanatory memorandum accompanying the proposal, the same is fully compliant and aligned with GDPR and it is aimed at increasing in practice the control that individuals have over the data that they generate.

Data Act (Regulation EU 2023/2854)

It is aligned with the European data strategy which set out the path for the EU to become a leader in the data economy. The Data Act, complementing the Data Governance Act by ensuring fairness in the allocation of the value of data amongst stakeholders, is key to create a European single market for data in which data can flow between sectors and Member States in a safe and trusted manner for the benefit of the economy and society. This is expected to harness the potential of the ever-increasing amount of industrial data.

It was published in the Official Journal of the EU on 22 December 2023, entered into force on 11 January 2024 and will become applicable on 12 September 2025.

The European Commission plans to recommend by autumn 2025 a set of model contractual terms to help businesses conclude data-sharing contracts that are fair, reasonable and non-discriminatory (Chapters II and III of the Data Act) and will also provide guidance on reasonable compensation and the protection of trade secrets. Furthermore, a set of non-binding standard contractual clauses for cloud computing contracts between cloud service users and providers will be provided. An expert group has been set up to prepare such terms and clauses. The impact evaluation of the Data Act will be conducted within 3 years of its entry into application and this might lead to its amendment.

The Data Act is directed to make data (in particular industrial data) more accessible and usable, i) encouraging data-driven innovation and increasing data availability, ii) ensuring fairness in the allocation of the value of data amongst the different actors and iii) clarifying who can use what data and under which conditions.

The rapid growth in the availability of products connected to the internet ('connected products'), which together compose a network known as the Internet-of-things (IoT), significantly increase the volume of data available for reuse in the EU.

Under the Data Act, users of connected products (businesses or individuals that own, lease or rent such a product) have a greater control over the data they generate. At the same time, incentives are maintained

for those who invest in data technologies and there are situations where a business has a legal obligation to share data with another business.

Furthermore, among other provisions (less relevant for AI REDGIO 5.0), the Data Act i) sets measures for increasing the fairness and competition in the European cloud market and for protecting companies from unfair contractual terms related to data sharing imposed by stronger players and ii) defines the requirements regarding interoperability to ensure that data can flow seamlessly between sectors and Member States, facilitated by Common European Data Spaces, as well as between data processing services providers.

The Data Act is without prejudice to the laws on the protection of intellectual property rights as well as it is fully compliant with the GDPR

The Data Governance Act increases trust in voluntary data-sharing mechanisms, whilst the Data Act provides legal clarity regarding the access to and use of data.

The Data Act comprises six main chapters[25]:

- **Chapter II on the business-to-business and business-to-consumer data sharing in the context of IoT**: the Data Act states that the users of IoT objects / connected products (including industrial machines) can access, use and port data that they co-generate through their use of a connected product or related services. This will create fairness in the data economy and empower users to reap value from the data they generate using the connected products that they own, rent or lease. The data in scope of Chapter II are all raw and preprocessed data generated from the use of a connected product or a related service that is readily available to the data holder (e.g. manufacturer of a connected product/ provider of a related service). This means data that can be easily accessed without disproportionate effort. Chapter II applies to both personal and non-personal data, including relevant metadata, data collected from a single sensor or a connected group of sensors (such as temperature, pressure, flow rate, position, acceleration or speed, etc.), whilst inferred or derived data and content (e.g. highly enriched data, audiovisual material) are out of scope. The users (i.e. any legal or natural person who owns, rents or leases a connected product) can access the data that they generate through their use of the connected product or related service. If the users want to share this data with another entity or individual ('third party'), they can either do so directly or they can ask the data holder to share it with a third party of their choice (excluding gatekeepers under the Digital Markets Act). The data holder is typically the company that developed the connected product or that provided the related service. The data holder must have a contract with the user (e.g. sales contract, rental contract, related service contract, etc.) setting the rights regarding the access, use and sharing of the data that is generated by the connected product or related service. The data holder cannot use any non-personal data generated by the product without the user's agreement. Under the Data Act there are several mechanisms for making it easier for users to be able to make use of its provisions:
    - data holders must give information to the users on the type of data that they will generate when using the connected product or related service (including the volume, collection frequency, etc.);
    - users must be able to request access to the data through a simple process;
    - the data holders must make the data available to users for free.

  There are also limitations on the use of the data, as follows:
    - the data obtained cannot be used to develop a competing connected product. This is functional not to deter businesses from investing in data-generating products;
    - in case the user is not the data subject whose data is being requested, personal data can only be made available if there is a valid legal basis (e.g. consent). This is paramount since

[25] European Commission, "Data Act explained. A comprehensive overview of the Data Act, including its objectives and how it works in practice", 2024

the co-generated data often contains both personal and non-personal data (which may be difficult to separate);

- it is incentivized the development of connected products and services based on new flows of data. This is of particular value to the SMEs. Furthermore, the micro and small companies, when manufacturers or providers of related services, are not subject to the same obligations as larger companies;
- the data holder and the user/ third party may agree on certain measures to preserve the confidentiality of the trade secrets. In case of infringement of these measures, the data holder may withhold or suspend the data sharing. The data holder may only refuse to share data if demonstrating that it is highly likely to suffer serious economic damage from the disclosure of trade secrets.
- In case of risk that the security requirements of the connected product could be undermined, resulting in serious adverse effects to the health, safety or security of people, the data holder and user may agree to limit data sharing. Such requirements must be laid down in EU or national law.

In case the data holder suspends, withholds or refuses to share data on the grounds of trade secrets protection or security requirements, it must notify the national competent authority and the users may challenge such a decision via a complaint with the competent authority (or in front of a dispute settlement body, if there is the agreement with the data holder).

- **Chapter III on the mandatory business-to-business data sharing**, defining the data-sharing conditions wherever a business is obliged by law to share data with another business. This applies to all data (both personal and non-personal) held by a business (including the situation covered by the Chapter II of the Data Act). In some cases a business ("data holder") has a legal obligation under EU or national law to make data available to another business ("data recipient"), including in the context of IoT data. The data-sharing terms and conditions must be fair, reasonable and non-discriminatory: the data holders that are obliged to share data may request "reasonable compensation" from the data recipient, such as costs incurred for making the data available and the technical costs related to dissemination and storage. The reasonable compensation, in case of micro-companies, SMEs and non-profit research organisations, is limited to the costs incurred for making the data available. There is also a non-exhaustive list of measures to remedy situations where a third party or user has unlawfully accessed or used data: this is directed to protect the data holders. Furthermore, the data-sharing obligations preceding the Data Act remain unaffected. And the obligations in future (sectoral) legislation should be aligned with Chapter III;
- **Chapter IV on unfair contractual terms**, which protects all businesses, in particular SMEs, against unfair contractual terms imposed on them. Measures are foreseen to intervene in situations where, for example, one of the businesses is in a stronger position, for instance due to its market size, and imposes a non-negotiable term ('take-it-or-leave-it') related to data access and use on the other. Also in this case, Chapter IV applies to all data, both personal and non-personal. There is a non-exhaustive list i) of terms that are always considered to be unfair (which are no longer valid, if possible simply severing them from the contact) and ii) of terms that are presumed to be unfair (in this case, the entity that imposed the term can try to demonstrate that the term is not unfair);+
- **Chapter V on business-to-government data sharing**: there are measures to allow, in certain situations, the public sector bodies to access certain data held by the private sector. These provisions are not expected to be specifically relevant in relation to AI REDGIO 5.0;
- **Chapter VI on switching between data processing services**. The Data Act sets minimum requirements that providers of cloud and edge computing services must meet to facilitate interoperability and enable switching providers, making switching free, fast and fluid. The customers of data processing services (including cloud and edge services) should be able to switch seamlessly from one provider to another, overcoming the existing barriers to this (such as high

charges associated with data egress, lengthy procedures and a lack of interoperability between providers with the possible loss of data and applications).The relevant data for switching comprises input and output data (including metadata), generated by the customer's use of the service, excluding data protected by intellectual property rights or constituting a trade secret of the service provider. The customers will benefit from much greater contractual transparency. The measures to ensure that customers can smoothly switch from one provider of data processing services ("source provider") to another ("destination") include, for instance:

  - The providers of Platform and Software as a Service must make open interfaces available and, at a minimum, export data in a commonly used and machine-readable format;
  - The providers of Infrastructure as a Service must take measures to facilitate that, when switching to a service of the same type, the customer gets materially comparable outcomes in response to the same input for features that both services share ("functional equivalence").
  - All providers must remove obstacles that their customers may face when they want to switch to another provider or use several services at the same time;
  - the switching charges , including charges for data egress, will be entirely removed from 12 January 2027.

- **Chapter VII on unlawful third country government access to data**: which protects non-personal data stored in the EU against unlawful foreign government access requests. These provisions are not expected to be specifically relevant in relation to AI REDGIO 5.0;
- **Chapter VIII on interoperability**, regarding the standards and interoperability as key to ensure that data from different sources can be used within and between Common European Data Spaces. It regards, besides the participants of data spaces offering data or data-based services to other participants, vendors of smart contracts as well as data processing services providers. The Chapter promotes the data sharing practices within the data spaces. Some requirements for the participants in data spaces are set, such as the need to ensure the public access to a description of the data structures, data formats and vocabularies, where available: such requirements will likely be further specified through delegated acts. The Chapter is also directed to ensure interoperability between data processing services, as a key element for easier switching. It also foster tools for ensuring the interoperability of data-sharing agreements, such as smart contracts. Harmonised standards and open interoperability specifications should prepare the ground for increasing the interoperability of data processing services. The vendors of smart contracts for the automated execution of data-sharing agreements have to comply with requirements. European standardisation organisation(s) might be asked to draft harmonised standards that comply with the abovementioned requirements. An European repository will lay down relevant standards and specifications for cloud interoperability.
- **Chapter IX on Enforcement and overarching provisions**: Member States must designate one or more competent authority(ies) to monitor and enforce the Data Act. Where more than one authority is designated, a 'data coordinator' must be appointed to act as the single point of contact at the national level. The Member States will designate one or more competent authorities to ensure the efficient implementation of the Data Act. In case of multiple competent authorities, one of them will be designated as "data coordinator", acting as a "one-stop shop" for all issues related to the implementation of the Data Act at the national level. A public register of competent authorities and data coordinators will be established. The penalties will be set by competent authorities and will be effective, proportionate and dissuasive. It will be made easy easier for companies, particularly small businesses, to enforce their rights under the Data Act, through simple, fast and low-cost solutions offered by the specialised competent authorities.

General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

This comprehensive regulatory framework lays down provisions for ensuring that personal data enjoys a high standard of protection everywhere in the EU and for giving individuals back control over of their personal data.

The following **GDPR definitions and concepts** are particularly relevant to AI REDGIO 5.0:

- **Data subject**: "identified or identifiable natural person[s]". Only natural persons (human beings) are beneficiaries of the data protection rules;
- **Personal data**: data relating to an identified or identifiable person (the "data subject"). They concern information about an individual whose identity is either manifestly clear or can be established from additional information. All reasonable means that are likely to be used to directly or indirectly identify the natural person need to be considered, being the GDPR applicable if the person concerned is identifiable, in a direct or indirect way. The special categories of personal data outlined by the Art 9 (the so-called "sensitive data") need enhanced protection: personal data revealing racial or ethnic origin; personal data revealing political opinions, religious or other beliefs, including philosophical beliefs; personal data revealing trade union membership; genetic data and biometric data processed for the purpose of identifying a person; personal data concerning health, sexual life or sexual orientation.
- **Data processing**: "'processing of personal data' [...] shall mean any operation [...] such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" of personal data. The automated data processing refers to the operations performed on "personal data wholly or partly by automated means";
- **Users of the personal data**, include: i) the "Data Controller", determining the means and purposes of processing the personal data of others. If several persons take this decision together, they may be 'joint controllers'; the "Data Processor" (natural or legal person), processing personal data on behalf of a controller; the "Recipients", the person to whom personal data are disclosed; "third party": a natural or legal person (other than the data subject, the controller, the processor and persons who are authorised to process personal data under the direct authority of the controller or processor.
- **Anonymisation**, consisting in the process allowing that all identifying elements are eliminated from a set of personal data so that the data subject is no longer identifiable. No element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned;
- **Pseudonymisation**, consisting in the process of removal from the personal information any attributes (name, date of birth, sex, address, or other elements) that could lead to identification and their replacement by a pseudonym. For the GDPR it is "the processing of personal data in such a man ner that the personal data can no longer be attributed to a specific data subject with out the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". The pseudonymised data are still personal data and are there fore subject to the GDPR and other data protection rules.

The **key GDPR principles governing the processing of personal data** are relevant and will be followed by the Consortium in the design, development and deployment of AI REDGIO 5.0 technology and its application within its experiments. They are set by art. 5 and cover:

- **Lawfulness, fairness and transparency**: under the GDPR, the lawfulness of the processing requires either the consent of the data subject or other lawful basis (necessity to enter a contract; a legal obligation; necessity to protect the vital interests of the data subject or of another person; necessity for performing a task in the public interest; necessity for the legitimate interests of the controller or a third party, if they are not overridden by the interests and rights of the data subject). The AI REDGIO 5.0 Consortium will rely on the processing of personal data for research

purposes, notably as regards the contact details and opinions of volunteers participating to workshops and validation tests in the experiments/pilots. The Consortium will collect and process data only if and to the extent that it is necessary for its research activities and communication/dissemination/exploitation of project's results. The main legal basis for data collection for research activities will primarily be consent (though in exceptional cases, where seeking consent would be inadequate to the processing activity, the relevant legal basis will be the legitimate interest). The handling of personal data will be done in a fair manner and the data subjects will be informed of the privacy risk, whilst the transparency of the processing will be ensured. In case of need to re-purpose existing datasets, this will be done on the basis that scientific research is compatible with its original intended purpose, so that there is no need for an additional separate legal basis from that which allowed their collection. In some of the AI REDGIO 5.0ìn experiments, it is possible that employment data will be collected and/or processed. Such data collection and processing in the context of employment will be carefully considered, since, due to the economic imbalance between employer and employees, the free nature and validity of consent as a legal basis for processing data about employees might be questionable. Therefore, the circumstances surrounding consent will be assessed carefully, adhering to the Article 29 Working Party's indications. The national legislations will be also examined by the experiment leaders concerned, since, according to Art. 88 GDPR, the Member States can establish more specific rules to ensure the protection of employees' rights and freedoms. On the other hand, for communication/dissemination/exploitation activities, the legal basis will also be consent.

- **Purpose limitation**: this principle implies that any processing of personal data must be done for a specific well-defined purpose and only for additional, specified, purposes that are compatible with the original one.
- **Data minimisation**: The processing of personal data will be limited to what is strictly necessary to fulfill the purpose of the processing: the Consortium will process only adequate, relevant and not excessive data in relation to the purpose for which they are collected in AI REDGIO 5.0 experiments and/or further processed. The personal data will be collected and/or processed on a "need to know" basis, both in relation to the amount of personal data collected, and concerning the extent to which they may be accessed, further processed and/or shared, the purposes for which they are used, and the period for which they are kept. The personal data will be fully anonymized or pseudonymised wherever possible and securely stored. When possible, the experiments will use fictional data..
- **Data accuracy**: the partners will ensure that in all processing operations inaccurate data will be erased or rectified without delay and that data will be checked regularly and kept up to date to secure accuracy.
- **Storage limitation**: The Consortium will delete or anonymize the personal data as soon as they are no longer needed for the purposes for which they were collected. Lawful storage of data which are no longer needed could happen throughout their anonymization. Personal data may be retained for up to five years in order to comply with auditing constraints.
- **Security, integrity and confidentiality**: the appropriate technical or organisational measures have to be implemented when processing personal data to protect the data against accidental, unauthorised or unlawful access, use, modification, disclosure, loss, destruction or damage", taking into account "the state of the art, the costs of implementation and the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons". Examples include pseu¬donymization and encryption of personal data. The level of data security will be commensurate to the risks faced by the research participants in case of un-authorised access to, or disclosure, accidental deletion or destruction of, their data.

- **Accountability**: Compliance of the processing operations with the GDPR requirements must be ensured and appropriate measures have to be taken to promote and safeguard data protection in the processing activities.

Furthermore, in AI REDGIO 5.0 it is important to respect the **data subjects' rights** and ensure their exercise. These rights, provided by GDPR, will be guaranteed in AI REDGIO 5.0 and AI REDGIO 5.0 project partners will execute the duties upon data controller in adherence with the requirements of the GDPR. Chapter 3 of the GDPR include the following rights:

- Right to Information: the data controllers have to inform data subjects i) about the processing of their personal data at point of collection (art. 13 GDPR) and ii) about the processing of their personal data where it was collected by an entity other than the controller;

Right of Access: the right of data subjects to know whether data concerning him or her are being processed and, if so, grant the data subject the right of access to such data (art. 15 GDPR);

- **Right to Rectification**: in case the personal data are inaccurate or incomplete, the controllers have the duty to correct or complete them (art. 16);

- **Right to Erasure or Right to be forgotten:** the right to erasure of personal data at the request of the data subject concerned, for instance from datasets or contact lists (art. 17 GDPR);

- **Right to Restriction of Processing:** right to limit, under particular circumstances, the processing of his/her personal data (Art. 18 GDPR);

- **Right to Data Portability**: right to receive his/her personal data, upon request, in a "…structured, commonly used and machine-readable format" as well as the right to "…transmit those data to another controller without hindrance from the controller to which the personal data have been provided" (art. 20 GDPR);

- **Right to Object**: the data subject is allowed, within specific conditions, to exercise the right to object to the processing of his/her data (art. 21 GDPR);

- **Right in relation to automated decision-making and profiling**: right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Nevertheless, the data subjects can give the consent to such automated profiling or decision-making.

Regulation on the free flow of non-personal data (Regulation 2018/1807)

The Regulation was adopted in November 2018 and applies from 28 May 2019. It lays down rules applicable to any kind of data other than personal data for giving rise to a harmonized approach to the free movement and portability of data in the EU, as well as for improving legal certainty and create a level playing field for all market players. The Free Flow of Non-Personal Data Regulation recognizes the importance of data for business processes in companies of all sizes and in all sectors, as well as the opportunities which the new digital technologies are opening up. Since the GDPR already stated the principle of free movement of personal data, there is now a comprehensive framework for a common European data space and the free movement of all data within the European Union. This Regulation therefore complements the GDPR provisions in aspects related to non-personal data within the Digital Single Market: thanks to these two legal instruments, the data can flow freely between Member States, allowing users of data processing services to use the data gathered in different EU markets towards improving their productivity and competitiveness.

It creates legal certainty for businesses to process their data wherever they want in the EU, whilst raising trust in data processing services and countering vendor lock-in practices.

In particular, this regulation ensures: i) the free movement of non-personal data across borders, being every organisation able to store and process data anywhere in the EU; ii) the availability of data for regulatory control; iii) easier switching between cloud service providers for professional users, also via encouraging the self-regulation; iv) consistency with the cybersecurity package, with the clarification that any security requirements already applicable to businesses storing and processing data will continue to do so when they store or process data across borders in the EU or in the cloud. The European Commission

also provided the Practical guidance[26] for businesses on how to process mixed datasets (including personal and non-personal data), illustrating with practical examples the rules to follow in these situations of interaction between the free flow of non-personal data regulation and the GDPR.
Its main notable features regards i) the prohibition for Member States to impose requirements on where data should be localized (except in justified cases to ensure public security, in compliance with the proportionality principle; ii) a cooperation mechanism that ensures that the competent authorities continue to be able to exercise any access rights to data that are being processed in another Member State; iii) incentives for industry to develop self-regulatory codes of conduct on the switching of service providers and the porting of data (supported by the European Commission).
A Guidance document[27] [14] was adopted, according to art. 8 (3) of the Regulation, regarding the interaction between such Regulation and the GDPR, with special attention to the mixed datasets, composed of both personal and non-personal data. An example of mixed dataset pertains to the analysis of operational log data of manufacturing equipment in the manufacturing industry. In case of mixed datasets, the Free Flow of Non-Personal Data Regulation applies to the non-personal data part of the dataset, the GDPR applies to the personal data part of the dataset, and, in case of inextricably linked non-personal data part and the personal data parts, the rights and obligations stemming from the GDPR fully apply to the whole mixed dataset (also in case personal data are only a small part of the dataset itself).
Furthermore, the art. 4 (1) of the Regulation prohibits the data localization requirements (the same occurs under the GDPR), covering both direct and indirect measures that would restrict the free movement of non-personal data, and without prejudice to already existing restrictions laid down by EU law. Such requirements shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality. Article 3(5) of the Regulation defines such requirements as "any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU, which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State". Therefore, the measures restricting the free movement of data within the EU may be set out in laws, in administrative regulations and provisions or even result from general and consistent administrative practices.
Examples of data localizations requirements comprises the obligation to store data in a specific geographic location (e.g. servers must be located in a particular Member State) or to comply with unique national technical requirements (direct data localisation requirements), as well as requirements to use technological facilities certified or approved within a specific Member State or other requirements with the effect of making it more difficult to process data outside of a specific geographic area or territory within the European Union (indirect data localisation requirements). Furthermore, there are no obligations on businesses (or limit their contractual freedom) to decide where their data are to be processed.
One of the purposes of the Regulation is to promote data portability between businesses, avoiding vendor lock-in practices. Such practices occur when users cannot switch between service providers because their data are "locked" in the provider's system (for instance because of a specific data format or contractual arrangements), and cannot be transferred outside of the vendor's IT system. Porting data without hindrance is paramount to allow users to choose freely between providers of data processing services (thereby ensuring effective competition).
Both the GDPR and this Regulation refer to data portability in view of making it easier to port data from one IT environment to another one (i.e. either to another provider's systems or to on-site systems),

[26] COM (2019) 250 final, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union

[27] EC, COM(2019) 250 final, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union

preventing vendor lock-in and fostering competition between service providers. Nevertheless, their approaches are different:

The right to portability of personal data (art. 20 GDPR) focuses on the relationship between the data subject and the controller and regards the right of the data subject to receive his/her personal data in a structured, commonly used and machine-readable format, and to smoothly transmit those data to another controller or to their own storage capacities.

Under this Regulation (art. 6), data portability concerns business-to-business interactions between a professional user and a service provider. There is no right for professional users to port data, but a self-regulatory approach is fostered, with voluntary codes of conduct for the industry, and targets a situation where a professional user has outsourced the processing of its data to a third party offering a data processing service.

Considering these different approaches, some challenges might arise in case of mixed datasets.

The development by industry of self-regulatory codes of conduct at EU level on the switching of service providers and the porting of data between different IT systems was encouraged by the European Commission to support the free flow of data. The SWIPO Working Group - Switching from Provider and Porting non-personal data developed two self-regulatory codes of conduct, respectively on data portability and on Cloud switching. Both of them envisage adherence by industry players on a completely voluntary basis. These codes were complemented by model contractual clauses to allow sufficient technical and legal specificity in their practical implementation and application, which is especially relevant for small and medium-sized enterprises.

e-Privacy Directive (Directive 2002/58/EC on privacy and electronic communications, replacing the Directive 97/66/EC and partially amended by Directive 2009/136/EC). It focuses on the privacy and protection of personal data in electronic communications, telecommunications networks and internet services, complementing the GDPR in this domain. Its provisions relevant to AI REDGIO 5.0 mainly regard the security of networks and services, the confidentiality of communications, the access to stored data, the processing of traffic and location data. All EU member states have transposed the ePrivacy Directive into their national legal frameworks, making its provisions legally binding within each country. The ePrivacy Directive applies to entities providing electronic communication services in the EU and might be relevant to AI REDGIO 5.0 in a direct or indirect way. Pursuant to art. 5(3), the storing or accessing information on a user's device requires prior consent, unless it is strictly necessary for providing a service explicitly requested by the user. Among the provisions to be considered for AI REDGIO 5.0 purposes, the following can be mentioned: i) Article 4, regarding the obligation of adopting security measures appropriated to the risk; ii) Article 5, regarding the protection to confidentiality of the communications among individuals; iii) Article 2, regarding the traffic data and location data; iv) Article 6 on user's consent; v) Art. 15 on data retention, and others.

The Directive focuses on the confidentiality of electronic communications, consent requirements and on the protection of online privacy in the electronic communications sector. One of its main component regard the cookies, whilst it is necessary to gain the user's consent after the provision with information about the purpose of the data storage and the opportunity to accept or opt-out. Furthermore, the providers of electronic communication services must ensure that their services are secure, which in turn secures the personal data potentiallyn shared through them, as well as must inform their users whenever a risk (for instance of a data breach) might leave their personal data vulnerable to misuse. As regards data retention, when the providers of services no longer need personal data, they must be erased or anonymized. Except in specific situation (such as for billing services or issues of national security), the personal data may only be retained upon user's consent, informing him/her why the data are being processed and the length of time they will be stored. The location data obtained through electronic communications must be processed with informed consent and should be anonymized when no longer needed. The companies providing electronic communication services must implement appropriate security measures to safeguard users' data, besides notifying the users and the relevant authorities in case

of a security breach involving personal data. The Directive also states rules on how traffic data, which includes information about communication between individuals, can be processed and stored.
As regards the consent, both the ePrivacy Directive and the GDPR require it, but the GDPR also outlines other principles of lawful processing (such contractual necessity, legitimate interests, and legal obligation). On the other hand, both the ePrivacy Directive and the GDPR require robust security measures to protect user's information.
Considering that the digital communications industry has evolved rapidly, in 2017, The European Commission proposed **ePrivacy Regulation**: COM(2017) 10 final 2017/0003, "Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC". It is directed to modernize the framework depicted by the ePrivacy Directive, better aligning with the GDPR provisions and addressing new challenges to privacy. On 10 February 2021 the Council agreed its position on ePrivacy rules. The next steps foresee the involvement of the European Parliament. It is not clear when it will enter into force.
The objectives and principles of the existing framework remain sound and relevant. The Art. 2 states that it "applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users". The "electronic communication network" and "electronic communications service" are broadly conceived: this is functional to bring also within the scope of the ePR the "over-the top" services, and machine-to-machine communications in IoT and smart-environments context. Due attention is given to cookies. Art. 5 states that electronic communications data are to be kept confidential and "listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing" is prohibited. However, there are a number of exceptions, to provide some flexibility (Art.6). Communication content and metadata are covered by Article 7 and other provisions regulate other significant aspects.
Despite the uncertainties regarding its entry into force, it is advisable to follow the developments of this proposal, to develop its services and technological components in accordance with its rules.

Open Data Directive (including High Value Datasets). Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast). It applies to the open data and the re-use of public sector information, laying down common rules for a European market for government-held data for making public sector and publicly funded data re-usable, building around two key strands of the internal market: transparency and fair competition. It replaced the Public Sector Information (PSI) Directive. In January 2023 the EC published a list of high-value datasets that public sector bodies to be made available for re-use, free of charge, within 16 months.

European Data Strategy (COM 2020 66 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European strategy for data". It is one of the cornerstones of the EU's digital strategy for creating a solid data-driven economy. It is the enabling legislation for the development of common European data spaces and is directed to promote the creation of a single market for data relying on data sovereignty, ensuring a wider availability of data for use in the economy and society, whilst paying attention to keep the companies and individuals who generate the data in control.

IDSA Rulebook 2023[28] [15]**,** concerning the IDS Data Sovereignty paradigm. This paradigm id directed to help in building trust in data sharing thanks to the technological enforcement of contractual provisions for enabling the data providers to keep a certain control and self-determination over the reuse of the data they provide. Its version 2.0 has been elaborated to facilitate the application of the IDS architecture as a basis for data spaces, supporting the data space initiatives in defining their rules, governance mechanisms, and legal basis. This Rulebook i) offers guiding principles for building and defining data spaces with

[28] IDSA Rule Book, Version 1.0, November 2020 and the draft IDSA Rule Book, version 2.0, 2023 (retrieved at https://docs.internationaldataspaces.org/idsa-rulebook-v2/front-matter/frontmatter)

architectures and rules rotating around the data sovereignty principle and ii) provides the requirements to develop. and operate data spaces based on IDS, listing mandatory and optional functionalities that a data space can have.

Miscellaneous

NIS 2 Directive EU 2022/2555) aiming to achieve a high common level of cybersecurity across the European Union. It was adopted in November 2022 and became enforceable as of 16 January 2023. By 17 October 2024, Member States must adopt and publish the measures necessary to comply with the NIS 2 Directive.

Cybersecurity Act 2019/881/EU, strengthening ENISA (the EU Agency for cybersecurity) and setting a cybersecurity certification framework for products and services, as well as its proposed amendment of 18 April 2023.

Digital Services Act (DSA) (Regulation (EU) 2022/2065) is applicable to the online intermediaries and platforms (marketplaces, social networks, content-sharing platforms, etc.) and is aimed at preventing illegal and harmful activities online and the spread of disinformation.

2030 Digital Compass & Path to the Digital Decade

COM(2021) 118 final. "2030 Digital Compass: the European way for the Digital Decade". It outlines the EC's priorities for a successful digital transformation of Europe's economy and society by 2030, encouraging to agree on a set of digital principles and to prepare a legislative proposal setting out a robust governance framework, empowering businesses and people in a human-centred, sustainable and more prosperous digital future, with the focus on digital skills, digital infrastructures, digitalisation of businesses and public services.

Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030: the Path to the Digital Decade sets the concrete plan to achieve Europe's digital transformation by 2030. It is guiding the Europe's digital transformation, encompassing also an annual cooperation mechanism involving the Commission and Member States

e-commerce Directive (Directive 2000/31/EC) and **Platform-to-Business Regulation** (Regulation 2019/1150)

The former is the key legal framework for online services in the EU. It is directed to remove obstacles to cross-border online services and was paramount in the development of online platforms in Europe, setting out, among other aspects, harmonised rules on the transparency and information requirements for online service providers and on electronic contracts and limitations of liability of intermediary service providers, besides enhancing the role of self-regulation.

The latter establishes rules in the area of business platforms for creating a fair, transparent and predictable business environment for smaller businesses and traders on online platforms. It is directed to ensure that the consumers receive the highest quality goods and services. Among other, it encompasses a list of fairness and transparency-oriented measures towards tempering the natural asymmetries characterizing the relationship between the platforms and their suppliers, in view of giving rise a fair and trustworthy innovation-driven ecosystem. It also contains the settlement of effective out-of-court redress mechanisms such as internal handling systems for business users and mediation procedures.

Directive on contracts for the supply of digital content and digital services (Directive 2019/770)

It i) ensures a high level of protection to consumers paying for or providing personal data in exchange of digital content and services and ii) imposes that digital contents or services fit to their expected purposes and have the qualities and performance features, which the consumer may reasonably expect. This might be relevant especially in the post-project phase, once the AI REDGIO 5.0 solutions will penetrate the market.

Human Rights Law: European Convention on Human Rights, adopted in 1950 and the **Charter of Fundamental Rights of the European Union**, 2016/C 202/02.

These sources, as well as the milestone document in the history of human rights (Universal Declaration of Human Rights, 1948), enshrine into EU law a wide array of fundamental rights enjoyed by EU citizens

and residents. They set a common European standard of achievements. The European Court of Human Rights' jurisprudence is a useful instrument for interpretation of human rights legislation. These sources are relevant in AI REDGIO 5.0, considering its human-centric approach and trustworthy framework: for instance, they will guide, together with the Ethics Guidelines for Trustworthy AI and the ALTAI Assessment List, the Human Rights Impact Assessments in WP2, and have already been take into account in relation to the WISE implications of the experiments and the Ethics and Data Protection Impact Assessment performed in WP1.

Table 1 AI REDGIO 5.0 legal and ethical framework

4.3. Ethical and legal requirements for AI REDGIO 5.0 Technology

This section contains the key legal and ethical requirements for the design, development and validation of AI REDGIO 5.0 system and technologies under development (as briefly outlined in Section 3) and, considering the overall AI REDGIO 5.0 environment and its relationship with AI REGIO Project, is partially based on its outcomes and findings[29] [16]. These requirements might be refined, updated and integrated in the next phase of the project, according, on the one hand, to the project's development and technical choices that will be taken, and, on the other hand, to the new developments or refinements of the evolving regulatory framework described in Section 4.2 of this document.

The legal and ethical requirements have been classified in:

- "Must be", which means binding requirements and refers to the cases when they directly derive from the applicable legislation, such as GDPR;
- "Should be", which are highly recommended, for instance because deriving from proposal of future regulations or from EC's communications;
- "Might have", which are preferable and advisable, for taking into account the ethical sources and the new regulatory developments under elaboration.

A certain degree of flexibility in the application of these requirement and in the evaluation of their fulfillment and of the adequateness of measures and technological solutions which will be developed to meet them, will be adopted, considering the research context and, for each requirement, a set of circumstances rotating around the severity of the risks and the reasonable efforts to face with them. This is reflected in the description of each of them "Priority").

The legal and ethical requirements pertain to the AI REDGIO 5.0 key technologies and assets and overall system , as described in Section 3.

[29] In particular, it refers AI REGIO D2.7 "Legal and Ethical Requirements and Guidelines v1" (2021) and D2.8 "Legal and Ethical Requirements and Guidelines v2" (2022).

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
1	**Ethics-by-Design**	The **Ethics-by-Design Approach** asks to make the research team think about and address potential ethics concerns, while they are developing a system in order to prevent at the maximum extent ethical issues from arising at a later stage. It is necessary that the development team proactively uses the ethical principles and adhere to the subsequent ethical and legal requirements, considering them as system requirements, together with the other technical, functional and non-functional requirements. More details on the Ethics-by-Design approach can be retrieved in D1.4 "Ethics Governance – M6", which defines the comprehensive Ethical Policy of the project on the basis of such approach. It relies on the guidance document provided by the European Commission"Ethics by Design and Ethics of Use Approaches for Artificial Intelligence"[30] [17]	ESL	Should be	ALL	R
2	**Privacy and Data Protection by Design and Privacy by Default**	The **Privacy and Data Protection by Design and Privacy by Default Approach** must be followed by AI REDGIO 5.0 Consortium, adopting since the beginning the adequate techniques and measures that, given the set of circumstances, "are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects"; "for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This applies to	PDPL, ESL	Must	ALL	R

[30] European Commission, "Ethics by Design and Ethics of Use Approaches for Artificial Intelligence", 2021.

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility" (art. 25 GDPR). As for the data storage, the Consortium must i) guarantee the protection of sensitive information, (ii) make hard for an adversary to learn the secret information required for any action (e.g., encryption, authentication, etc.), and (iii) credentials should be stored protected from eavesdropping / leakage. It is therefore necessary that the AI REDGIO 5.0 developers consider and gets aligned with the seven privacy principles defined by **Cavoukian**: "1. Proactive not reactive – preventative not remedial 2. Privacy as the default setting 3. Privacy embedded into design 4. Full functionality – positive-sum, not zero-sum 5. End-to-end security – full lifecycle protection 6. Visibility and transparency – keep it open 7. Respect for user privacy – keep it individual and user-centric". More details can be retrieved in D1.4 "Ethics Governance – M6", being this approach a pillar, as the Ethics-by-Design approach, of the project's Ethical Policy.				
3	**Fairness and avoidance of unfair biases**	It is key to adhere to the fairness principle in the design and deployment of AI REDGIO 5.0 technology. It encompasses equity, impartiality, egalitarianism, non-discrimination and justice. It consists in two main dimensions, where the substantive dimension regards an ideal of equal treatment between individuals or between groups of individuals, whilst the procedural perspective consists in the ability to seek and obtain relief when individual rights and freedoms are violated. The fairness requirement mainly relies on the Ethics Guidelines for Trustworthy AI. However, it is also encompassed by the GDPR (art. 5.1 a) and fairness obligations are also	HRs, ESL, P2BR, PDPL	Must	ALL	ALL

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		required by the P2BR for the intermediation services (platforms), though in the different meaning of settlement of effective out-of-court redress mechanisms such (as internal handling systems for business users) and mediation procedures. In relation to AI applications, the AI REDGIO 5.0 Consortium must prevent that the AI systems suffer from the inclusion of inadvertent historic bias and incompleteness, so to avoid the exacerbation of prejudice and marginalization against certain individuals and/or groups. In this way, biases, discrimination and harm against such individuals and/or groups can be avoided. Art. 21 European Charter of Fundamental Rights states that it is prohibited any kind of discrimination: therefore the efforts in the project should be directed to avoid that the overall solution and/or some of its components/tools facilitate any kind of discrimination (race, gender, age, religion, disabled) or social sorting, as well as to cause undue or unjustified harm to anyone, including wrongfully stigmatization The potential impact of the AI tools and their use on work and skills should be assessed as well: they may alter the work sphere and have an impact on the working environment, on workers, on the relationship between workers and employers, and on skills. As mentioned under the human empowerment requirement, the AI system should support humans in the working environment and aim for the creation of meaningful work (this is an assumption of AI REDGIO 5.0 and its CI paradigm). The Human Rights Impact Assessments that will be conducted in WP2, as well as all the ethics-related activities concerning the TERESA Experiments, the WISE				

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		Implications and the Ethics and Data Protection Impact Assessment represent useful tools in this direction.				
4	**Transparency and Interpretability**	This requirement is set by several regulatory sources. Under the **GDPR,** any personal data collection and processing must be inspired to full transparency in order to grant an adequate level of clarity of it, including all privacy-relevant properties and actions. The minimum list of mandatory information to be provided with the data subject are listed in GDPR (Art. 13). Under the **e-Commerce Directive** and the **DSA** information obligations are provided for the conclusion of a contract with a consumer and liabilities in relation to them (Sect. 4). Under the **P2BR,** transparency requirements are provided (see below under P2BR Obligations). Under the **AI Act**, transparency obligations are established not only in relation to the high-risk system, but also for the limited risk systems. Under the **Ethics Guidelines for Trustworthy AI** and related **ALTAI** the transparency, traceability and explainability are set as requirements, directed to ensure **interpretability**. The solutions should comprehensible, explainable or understandable from an external observer. The **explainability** requires that an AI system is intelligible to non-experts, in particular those directly and indirectly affected. This occurs if its functionality and operations can be explained non technically to a person not skilled in the art. The degree to which explainability is needed depends on the context and the severity of the consequences of erroneous/ inaccurate output to human life.	PDPL, ESL, P2BR, ECD, AIA, OAIL, SSPF	Must	ALL	ALL

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		Traceability means the ability to track and document the journey of a data input and related processes through all stages of the data lifecycle within the processes of the development of the AI system. The RPLD Proposal includes information obbligations in specific cases for alleviating the burden of proof for victims in complex cases. The **AILD proposal** sets the right of access to evidence subject to certain conditions, to a court (or, in limited circumstances, third parties) and to the victims, who have the right of access to evidence from companies and suppliers when high-risk AI is involved. It is also standards addressing transparency to be followed, such as the **IEEE Standard for Transparency of Autonomous Systems** (IEEE Std 7001TM-2021). More information on the transparency requirements under these sources are provided in Sect. 4.2				
5	**Human autonomy and empowerment**	The principle of respect for human autonomy when an AI system is involved is set the Ethics Guidelines for Trustworthy AI and other soft-law sources. In particular, it applies to those aimed at guiding, influencing or supporting humans in decision making processes: they should support human agency and human decision-making. Human oversight should be foreseen to ensure that AI artefacts do not undermine human autonomy: approaches and measures should be conceived and implemented, including the following approaches[31]: - human-in-the-loop(HITL), which is the capability for human intervention in every decision cycle of the system, which in many cases is neither possible nor desirable;	ESL, PDPL, DL, AIA	Should	ALL	ALL

[31] EC, "Ethics Guidelines for Trustworthy AI", 2019.

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		- human-on-the-loop (HOTL), which is the capability for human intervention during the design cycle of the system and monitoring the system's operation; - human-in-command (HIC), which is the capability to oversee the overall activity of the AI system (including its broader economic, societal, legal and ethical impact) and the ability to decide when and how to use the system in any particular situation. A step ahead should be moved, in order to allow human empowerment and flourishing: this is what AI REDGIO 5.0 is seeking to do, thanks to its Industry 5,0 solutions and CI approach. Besides this, the requirement also applied to the data subject's control over his/her personal data, as described under the GDPR Obligations requirements. More information are provided in Sect. 4.2.				
6	**Technical robustness, safety and security**	Both regarding data sharing and AI, the security, the safety and technical robustness of the system are paramount, in view of preventing harm to human beings. The integrity, confidentiality and availability of the data should be ensured, ensuring appropriate security of the data, especially personal data and protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. Appropriate technical and organizational measures should be taken, also to avoid cyber-security attacks. As for GDPR, this rule is laid down by Article 5, letter f). The trustworthiness of an AI system requires that it is able to deliver services that can justifiably be trusted (dependability), besides being robust when facing changes (resilience). A preventative approach to risks is recommeded during the development of an AI	ITSL, PDPL, DSL, ESL, SSPF, NRD	Must, apart from certification (which is might have)	ALL	R

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		system/tool, in order to achieve technical robustness, reliable behaviour and the minimization of unintentional and unexpected harm. Both for personal data processing (where relevant) and, in general, for AI design and development, appropriate technical and organizational measures should be implemented following, taking into account the level of security appropriate to the risk (Art. 32 GDPR). In order to enhance the trust in cross-border data processing, it is recommended a certification of security. Authorization and Access Control mechanisms should be ensured. It is necessary to ensure that the participating users act according to the security, privacy and data sharing policies. Access to AI REDGIO 5.0 technology and datasets should be possible only to authorized users.				
7	**Data Accuracy**	The AI REDGIO 5.0 Consortium must ensure that the data are of high quality, accurate, consistent, and contextualized, taking every reasonable step to ensure to prevent the use of inaccurate data, in order to avoid that the data or AI system leads to biased or erroneous outputs, untrustworthy results, lack of contextual relevance, and, ultimately, a loss of trust. This requirement is essential both for AI application and for data sharing services.	ESL, ITSL, PDPL, DL	Should	Industry 5.0 Data4AI Platform & Data Spaces Collaborative Intelligence platform	D, E
8	**Accessibility**	AI REDGIO 5.0 technology should be user-centric and designed in a way enabling all people to use it, regardless of their age, gender, abilities or other characteristics. It is also recommended that AI REDGIO 5.0 consortium develop user and data protection friendly User Interface (UI). Accessibility to AI for persons with disabilities should be considered as well, referring to the Universal Design principles to address the widest possible array of users. Relevant accessibility standards should be followed.	DL, HRs, ESL, SSPF, AIA	Should	ALL	R

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
	Accountability	This requirement is closely linked to the principle of fairness. First of all, under the GDPR accountability is foreseen as a principle requiring that organisations put in place appropriate technical and organisational measures and are able to demonstrate what they did and its effectiveness when requested (in other words, that they are compliant with the GDPR itself). Likewise, in relation to AI systems, mechanisms should be put in place to ensure responsibility and accountability for AI tools and their outcomes. It comprises i) the auditability, which entails the enablement of the assessment of algorithms, data and design processes; ii) the minimization and reporting of negative impacts; iii) Accessible redress mechanisms in place in case of unjust adverse impacts. The accountability is related to trustworthiness and operational correctness: in fact, it is necessary to be able to provide verifiable evidence on the correctness (i.e., correct configuration) of the current state of each component/system entities. Actions should be non-repudiable, as well as every system entity should be held accountable of its actions. This principle is also paramount both for the AILD Proposal and for the RPLD Proposal: as mentioned in Sect. 4.1, the liability relies on the attribution for AI-induced harms (and their mitigation), which is strongly interrelated with accountability. More details can be retrieved in Sect. 4.2.	PDPL, DL, ESL, SSPF, AIA	Must	Industry 5.0 Data4AI Platform & Data Spaces Collaborative Intelligence platform	ALL

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
9	**Risk-based approach**	This requirement is set both by the GDPR and by the the AI Act[32]. The GDPR requires to evaluate the ethics risks related to the data processing activities by assessing the particular likelihood and severity of each risk to data protection, taking into account "the nature, scope, context and purposes of the processing and the sources of the risk". The risk assessment must be conducted in an objective manner to determine whether there is a "risk" or a "high risk". Particular obligations are set in case of high risks and pursuant to Recital 75, 76, the risk level (in terms of likelihood and severity for freedoms and rights of individuals) determines what measures are appropriate in each case. The more severe and likely the risks are, the stronger measures will be required to counteract such risks. The AI Act classifies the AI system according to the risks posed by them and provides different obligations and requirements for the different types of systems. More information are in Sect. 4.2	PDPL, ESL, AIA	Should	Industry 5.0 Data4AI Platform & Data Spaces Collaborative Intelligence platform	D, E
10	**GDPR Obligations and other obligations regarding personal data**	The GDPR rules and obligations described in Section 4.2 must be accomplished. Here some additional details and guidelines are provided on some of them: - The **lawfulness principle:** the data processing has to be performed according to the data protection legislation and any other applicable law and regulation. According to the GDPR (art. 6) the legal bases on which the lawfulness of processing relies and which makes the processing lawful include, among others, the informed consent, which is "any freely given, specific, informed and unambiguous	PDPL, ESL, HRs	Must	Industry 5.0 Data4AI Platform & Data Spaces, Collaborative Intelligence platform	D, E

32 COM/2021/206 final, Proposal for a Regulation on Artificial Intelligence.

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (art. 4 GDPR). - **Purpose limitation and legitimate aim principle:** the data must be collected for specific, explicit and legitimate purpose served by the AI REDGIO 5.0 system/components, without further processing them in a way incompatible with it. Adequate safeguards against misuse must be taken. - **Data Minimization Principle:** the personal data collected and or handled by AI REDGIO 5.0 Consortium must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". The anonymization and pseudonymization techniques should be adopted to the maximum extent, including safeguards for mitigating the risks of re-identifying the individuals and for minimizing possible linkability and actual linkages; - **Storage Limitation Principle**: the personal data must either be erased or anonymized as soon as it is no longer necessary for the purpose (Art. 5 (1) (e) GDPR). Furthermore, the **data subjects** must be effectively entitled to **exercise their rights**, laid down in the Articles 12 –22 GDPR. They are described in Section 4.2. It is key to ensure the **individual control** of personal data by adopting concretely allow o the data subjects concerned to retain and exercise real control over their personal information, pursuant to both GDPR and the upcoming ePrivacy Regulation (ePR).				

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
11	**Data sovereignty**	It is key to ensure the **data sovereignty** in order to incentivize the data sharing and build/reinforce trust among participants, making considerably more data sources accessible. The IDS standard **DIN SPEC 27070**, where parts of the current version of the IDS reference architecture (version 3.0) has been incorporated for operating secure and trustworthy infrastructures for data exchange, should be considered in the perspective of guaranteeing data sovereignty.. Data sovereignty presupposes metadata attached to data, unambiguously defining data usage policies at each level of the data value chain. The technical infrastructure should be able to enforce data sovereignty, facilitating the execution of contractual provisions on the access and use of data, which, in turn, enforce the data policies in terms of processing, allow (or disallow) linkage or analysis of data-by-data users, or allow (or disallow) third parties access to data, and other use limitations, flow control, data transfer restrictions, etc. Data sovereignty should be ensured also within AI REDGIO 5.0 wide ecosystem, including third parties' digital infrastructures (e.g. clouds, software components, networks). The **Industry Agreements** related to the Data Spaces for Manufacturing should be used, being an important tool to guide the industry stakeholders' efforts in their data sharing practices according to the data sovereignty paradigm, through a taxonomy of key aspects to consider towards voluntary B2B data sharing schemes.	ESL, DL, HRs, SSPF	Should	Industry 5.0 Data4AI Platform & Data Spaces	ALL

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
12	**Data Portability**	Pursuant to the Regulation on the free flow of non-personal data (art. 6), it is key to ensure the data portability in AI REDGIO 5.0, being it increasingly relevant to enable or facilitate the switching of service providers and the porting of data between different IT systems, in a structured, commonly used and machine-readable format. The two self-regulatory codes of conduct, respectively on data portability and on Cloud switching, developed by the SWIPO Working Group - Switching from Provider and Porting non-personal data should be followed. It is also important under GDPR (art. 20). For more details, see Sect. 4.2	DL, ESL, SSPF	Should	Industry 5.0 Data4AI Platform & Data Spaces, Collaborative Intelligence platform	ALL
13	**AIA Obligations**	In case of **high-risk systems** to be developed in AI REDGIO 5.0 (which is expected not to occur or to be an exceptional case), the regulatory requirements set by the AI Act for these systems must be followed to ensure that these systems operate safely, ethically, and transparently. The requirements for the providers (developers) cover various stages (from design and implementation to post-market introduction) and comprise mandatory requirements, including also technical requirements, and an ex-ante conformity assessment. They are established by Art. 8–17 and include: i) establish a risk management system throughout the AI system's lifecycle; ii) conduct data governance, ensuring that training, validation and testing datasets are relevant, sufficiently representative and, to the best extent possible, free of errors and complete according to the intended purpose; iii) prepare and maintain detailed technical documentation to demonstrate compliance and provide authorities with the information to assess that compliance; iv) design the	AIA	Must	ALL	ALL

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		AI system for record-keeping in order to enable it to automatically record events. The system must generate logs while being in operation, thereby guaranteeing the traceability of the system's functioning; v) provide instructions for use to downstream deployers to enable the latter's compliance; vi) ensure transparency and clear information to users. The system must be designed and developed in a way to ensure that its operation is sufficiently transparent so as to enable users to interpret the system's output and use it in the proper manner; viii) design the AI system to allow deployers to implement human oversight when the system is in use. Among others, this includes providing a "stop" button or a similar procedure by way of which, the AI system can be safely stopped; ix) design the AI system to achieve appropriate levels of accuracy, robustness, and cybersecurity, upholding the relevant standards; x) establish a quality management system to ensure compliance; xi) conduct a Fundamental Rights Impact Assessment Beside the providers, other subjects have distinct obligations with regard to high-risk AI systems as well. In case the manufacturers of products covered by some of the EU pieces of legislation listed in Annex I to the AI Act place, under their own name, a product on the EU market in which a high-risk AI system is embedded, they are subject to the same obligations as the provider of the AI system. The users (deployers) have some obligations, though less than providers (developers): they must use the AI systems in accordance with the provided instructions of use, carefully select input data, monitor the operation of it, and keep logs.				

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		Most of the AI Systems in AI REDGIO 5.0 are expected to be **limited to minimal risks**. The transparency requirements for some systems interacting with individuals have to be followed: the individuals must be informed when they are interacting with AI (unless this is obvious from the circumstances and the context of use)to foster an environment of trust and accountability in AI deployment. The providers of AI systems that create synthetic audio, image, video or text content must ensure that the outputs are marked in a machine-readable format and detectable as artificially generated or manipulated (except in limited exceptions). The deployers of an emotion recognition system or a biometric categorisation system must inform the affected individuals of the operation of the system. The limited risk systems are not subjected to the same stringent compliance checks (such as conformity assessments or product safety reviews). Nevertheless, they are evaluated based on similar criteria to ensure they meet the necessary transparency and safety standards. As regards the **General Purpose AI Models** (AI models can be used for many different purposes) and Generative AI, they are regulated by the AI Act and they have to comply with specific transparency requirements, including: a declaration to users indicating that the content they are interacting with was generated by an AI system; measures to prevent the creation of illegal content must be incorporated in their design; summaries of copyrighted data used in the training of these AI models must be provided;				

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		The more advanced AI models which might have a significant impact, such as GPT-4, are subject to an extensive evaluations and, in case of serious incidents these must be reported to the EC.				
14	**Safety of the worker**	The health and safety of the operators, including the participants in the experiments (especially the Test-Before-Invest Experiments involving humans, above all the TERESA, and cobots operating in a shared workspace in collaborative settings), might imply some health and safety risks. Most of these risks might be related physical harm and comprise hazardous collisions, cybersecurity, lack of focus, loss of movement control, debris and pinch points. However, also cognitive risks and psychological/ethical risks might occur, including mental strain, lack of trust and complicated interaction mechanisms, as well as social impact and acceptance. The ALTAI indications and AI Act requirements must be followed to minimize the risk in the design and development of the system. Furthermore, in the experiments the relevant safety at work regulatory sources must be applied must be applied, health and safety procedures and protcolos establiehd at company level or set by dedicated standards, must be adopted and dedicated training organize to minimize the risks. Furthermore, the WISE implications and indicators must be monitored in each experiment.	HRs, ESL, AIA, SSPF, OAIL	Must	Collaborative Intelligence platform	ALL
15	**Environmantal - friendliness**	The efforts should be directed towards a more sustainable and environmentally friendly AI in manufacturing, such as by optimizing manufacturing processes to reduce emissions and reducing energy consumption. The solutions of the project should be based on choices aimed at contributing to a circular economy, minimizing the environmental damage caused	HRs, ESL, SSPF	Should	ALL	ALL

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		by industrial production, and, reduce the industrial carbon footprint. The sustainability and ecological responsibility of AI systems should be pursued The most environmentally friendly solutions should be selected in the system's development, deployment and use process, as well as its entire supply chain, examining the resource usage and energy consumption during training, opting for less harmful choices.				
16	**Responsible use of Generative AI**	As regards the potential use of Generativ AI solutiosn within AI REDGIO 5.0 technological development, the following apply, among others described in the EC's Living guidelines on the Responsible use of Generative AI in research: - The researcher are accountable for the integrity of the content generated by or with the support of generative AI and have to maintain a critical approach to using the output produced by generative AI, being of its limitations (such as potential bias, hallucinations and inaccuracies). - The use of generative AI must be transparent, including detail on which generative AI tools have been used; - It must be taken into account the stochastic (random) nature of generative AI tools, which might produce different output from the same input (to the detriment of reproducibility and robustness of the results and conclusions) - Attention must be paid to privacy, confidentiality and intellectual property rights when sharing sensitive or protected information with AI tools and no third parties' personal data can be uploaded to online generative AI systems without consent;	ESL	Should	ALL	D

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		- Since the generated or uploaded input (text, data, prompts, images, etc.) could be used for other purposes, such as the training of AI models, the unpublished or sensitive work must not be uploaded into an online AI system unless there are assurances that the data will not be re-used - The AI REDGIO research should constantly learn how to use generative AI tools properly to maximise their benefits and, since generative AI tools are evolving quickly, they should stay up to date on the best practices Additional requirements regarding the Generative AI stem from the AI Act and have been described in that part.				
17	**P2BR Obligations**	The set of obligations provided by the P2BR must be accomplished, in case of provision of online intermediation services. Thes include the transparency obligations are laid down for providers of intermediation services: in fact, under P2BR transparency obligations are laid down for providers of intermediation services to inform, through clear, unambiguous and readily available contractual terms and conditions, about the treatment, the criteria used to rank their products and the requirements to suspend or terminate their services. The EC published the Guidelines[33] , which address the main requirements for online platforms identified in P2BR.	P2BR	Must	Industry 5.0 Data4AI Platform & Data Spaces, Collaborative Intelligence platform	E
18	**e-Commerce (and DSA) Obligations**	Among others, the following requirements potentially relevant to AI REDGIO 5.0 apply in case of intermediary services, hosting services, online platforms: transparency reporting, measures against abusive	ECD, DL	Might be	Industry 5.0 Data4AI Platform & Data Spaces,	E

[33] Commission Notice "Guidance Guidelines on ranking transparency pursuant to Regulation 2019/1150

Req. Nr.	Req. Name	Req. Description and Guidelines	Regulatory Source	Priority	AI REDGIO 5.0 Technology	Phases
		notices and counter-notice, Vetting credentials of third-party suppliers ("KYBC"), risk management obligations and compliance officer, external risk auditing and public accountability.			Collaborative Intelligence platform	
19	**Appointment and involvement of the Ethics-related figures**	Need to set-up and involve: 1) the Ethics Board committee to i) monitor ethical and legal issues in the project and report to the EC; ii) work closely with the consortium in order to address the ethical and legal issues; 2) the Ethics Mentor, to guide and orchestrate the ethics and legal activities withing the project; 3) The Ethics Experiment Managers, to fine tune the project-level ethics protocols and forms and to timely and identify any potentially ethics issues, besides monitoring the advancement of the WISE Implications	ESL	Should	ALL	ALL

Table 2 AI REDGIO 5.0 Legal and Ethical Requirements

5. The ethical and legal framework and requirements for AI REDGIO 5.0 Experiments

The following sections contains, respectively for the AI REDGIO 5.0 SME-driven experiments and Test-Before-Invent Experiments, the legal and ethical pieces of regulation specifically applicable to them (in addition to the sources described in Section 4, as well as the legal and ethical requirements relevant for their operations.

5.1.1. AI REDGIO 5.0 SME-driven experiments

5.1.1.1. SME PILOT I SCAMM (LOMBARDY, ITALY): AI-BASED QUALITY CONTROL OF WHITE GOODS COMPONENTS

5.1.1.1.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
Directive 2006/42/EC - machinery directive	This Directive aims at the free market circulation of machinery and at the protection of workers and consumers.	it defines essential health and safety requirements of general application.	repeals Directive 98/37 EC as of 29th December 2009
EN ISO 13849-1:2015	provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software.	defines the main machine safety functions and the procedure for determining the Performance Level required for each safety function.	repeals EN ISO 13849-1:2008/AC:2009, EN ISO 13849-1:2008
The Ethics Guidelines for Trustworthy AI (2019)	7 key requirements: human agency and oversight; technical Robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; accountability.	The accuracy and reliability of the system should be validated in laboratories and relevant environments. Clear information should be provided concerning AI limitations, reasoning and the processed data. The user should remain in charge of supervise the results.	Further support documents: Definition of Artificial Intelligence used for the Guidelines; Assessment List for Trustworthy AI (ALTAI).
General Data Protection Regulation (GDPR) - (EU) Regulation 2016/679	Explicit and informed consent; declaration of data and finality; queried information limited to the declared needs; data can be retained only for the time needed for the intended action; data security.	The system will preliminarily ask for informed consent. The user must be informed on which data will be recorded and must be able to access these data and to remove the consent.	This regulation applies to any subject, be it a natural person or a legal person, that is exploiting personal data within the European economic area.

Table 2 Ethical and Legal Framework of SME Pilot I

5.1.1.1.2. Ethical and Legal Requirements

Req #	EL Req	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset	Business Process	Business Objectives
01	Technical Robustness and safety	Validate security, safety, accuracy and reliability. **The Ethics Guidelines for Trustworthy AI (2019)**	Critical	- Production process - Maintenance	Ethical	AI Pipeline Manager	- Quality control - Process optimization - Maintenance	- Reduce waste - Reduce energy - Maintenance efficiency
02	Human agency and oversight	Implement proper oversight mechanisms. **The Ethics Guidelines for Trustworthy AI (2019)**	Critical	- Production process - Maintenance	Ethical	AI Pipeline Manager	- Quality control - Process optimization - Maintenance	- Reduce waste - Reduce energy - Maintenance efficiency
03	Transparency	Declare limitations, reasoning and data used. **The Ethics Guidelines for Trustworthy AI (2019)**	Critical	- Production process - Maintenance	Ethical	AI Pipeline Manager	- Quality control - Process optimization - Maintenance	- Reduce waste - Reduce energy - Maintenance efficiency
04	Accountability	Identify, declare and minimize potential risks **The Ethics Guidelines for Trustworthy AI (2019)**	Critical	- Production process - Maintenance	Ethical	AI Pipeline Manager	- Quality control - Process optimization - Maintenance	- Reduce waste - Reduce energy - Maintenance efficiency
05	Privacy and data governance	The user must provide explicit and informed consent **GDPR - (EU) Regulation 2016/679**	Critical	- Production process - Maintenance	Legal	AI Pipeline Manager	- Quality control - Process optimization - Maintenance	- Reduce waste - Reduce energy - Maintenance efficiency
06	Protection of workers	Comply with health and safety requirements **- Directive 2006/42/EC - machinery directive - EN ISO 13849-1:2015**	Critical	- Production process - Maintenance	Legal	None	- Quality control - Process optimization - Maintenance	- Reduce waste - Reduce energy - Maintenance efficiency

Table 3 Ethical and Legal Requirements of SME Pilot I

5.1.1.2. SME PILOT II PERNOUD (RHÔNE ALPS, FRANCE): DECISION-MAKING TOOL FOR THE REALIZATION AND ORGANIZATION OF THE MANUFACTURING SEQUENCES IN A SHOP FLOOR

5.1.1.2.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
French Labour Code	L. 6321-1 : Every employer has a legal obligation to adapt its employee to changes in their employment, especially for evolution in technology or organization.	Our experiment includes numerical technologies not used today. Employees in direct contact with this system will have to be trained.	
Auvergne-Rhone-Alpes convention for high potential companies "PERL"	The company (PERNOUD) is committed to maintaining and creating jobs in the regional territory.	Using AI to replace employees should not be an objective, AI has to help or complete humans and not replace.	
ISO 9001, Quality Management System	It helps businesses and organizations be more efficient and improve customer satisfaction. The primary focus of the ISO 9001 standard is to meet customer requirements and strive to exceed customer expectations. The standard is based on seven Quality Management Principles, including a strong customer focus, the motivation and implication of top management, the process approach and continual improvement.	Improvement of the production process	

Table 4 Ethical and Legal Framework of SME Pilot II

5.1.1.2.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives

01	Employment adaptation	Obligation to support employee for adaptation with new technology introduced in the organization	Critical	Human resources	Legal	None	BP3	Skilfulness & Accuracy
02	Human in the loop	Human has to oversee the AI	Preferred	AI system	Ethical	Collaborative platform	BP1, 3	Accuracy
03	Quality management 1	Data used for model training has to be referenced	Preferred	AI system	Ethical	Local Open Hardware	BP1, 2	Service level & Production
04	Quality management 2	Rules integrated in the applied knowhow has to be referenced	Preferred	AI system	Ethical	Local Open Hardware	BP1, 2	Service level & Production
05	Quality management 3	Older AI model has to be archived	Preferred	AI system	Ethical	AI pipeline designer/ Local Open Hardware	BP1, 2	Service level & Production

Table 5 Ethical and Legal Requirements of SME Pilot II

5.1.1.3. SME PILOT III GPALMEC (TRENTINO, ITALY): AUTONOMOUS DRIVING FOR AGRICULTURAL VEHICLE

5.1.1.3.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other

Civil Law Rules on Robotics (from EU Parliament)	The resolution regulates both the robot liability and a possible code of conduct (Code of Ethical Conduct for Robotics Engineers and a Code for Research Ethics Committees).	The need to propose robotics solutions which are ethical according to the EC policies. Specific fields considered are: ● liability for damage caused by robots; ● the four ethical principles in robotics engineering: 1) beneficence (robots should act in the best interests of humans); 2) non-maleficence (robots should not harm humans); 3) autonomy (human interaction with robots should be voluntary); 4) justice (the benefits of robotics should be distributed fairly).	
Ethics guidelines for trustworthy AI (From EC)	To give general guidelines to regulate AI throughout its entire life cycle to be: 1) lawful: complying with all applicable laws and regulations; 2) ethical: ensuring adherence to ethical principles and values; 3) robust: both from a technical and social perspective.	The need to develop ethical and robust AI solutions and so to meet the seven requirements indicated by the EC, i.e.: 1) human agency and oversight; 2) technical robustness and safety; 3) privacy and data governance; 4) transparency; 5) diversity, non-discrimination and fairness; 6) environmental and societal well-being; 7) accountability.	Other possible reference are the Tools for trustworthy AI Identified by OECD
2006/42/EC machinery directive	This Directive aims at the free market circulation on machinery and at the protection of workers and consumers using such machinery. It defines essential health and safety requirements of general application, supplemented by a number of more specific requirements for certain categories of machinery.	Autonomous drive system deeply affects the machine functioning. Each vehicle on the market equipped with the autonomous drive system needs to be recertified according to the machinery directive. To do so, a new risks assessment needs to be carried out and all the resulting prescriptions must be observed by the autonomous drive system.	

Table 6 Ethical and Legal Framework of SME Pilot III

5.1.1.3.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	Ethics guidelines for trustworthy AI	To give general guidelines to regulate AI throughout its entire life cycle to be: 1) lawful: complying with all applicable laws and regulations; 2) ethical: ensuring adherence to ethical principles and values; 3) robust: both from a technical and social perspective.	Critical	R&D	Ethical & Legal	Edge AI Reference Models & Collaborative Intelligence platform for Edge AI in Manufacturing	Business process #1: Long time operations on fields dedicated to agriculture are the source of costs for the cultivation. The vehicles contributed in the last century to support humans to operate in an efficient and repeatable way on field lowering the costs of workforce. Introducing automation machines and AI supported driving features frees the operator from the duty of driving lowering even more the human time requirements.	Business objective #1: To reduce the human contribution to the field management with effects on the related costs implied and the efficiency of the agricultural processing. Business objective #2: To reduce the occurrence of severe and potentially life-threatening accidents during agricultural activities, lowering the risk for the personnel operating in the harsh environment and that are prone to human error or underestimation of risks

							Business process #2: Increase safety on extreme and critical field scenarios.	
02	Civil Law Rules on Robotics	The need to propose robotics solutions ethical according to the EC policies. Specific fields considered are: ● liability for damage caused by robots; ● the four ethical principles in robotics engineering: 1) beneficence (robots should act in the best interests of humans); 2) non-maleficence (robots should not harm humans); 3) autonomy (human interaction with robots should be voluntary);	Critical	R&D	Ethical & Legal	Edge AI Reference Models & Collaborative Intelligence Platform for Edge AI in Manufacturing	Business process #1: Long time operations on fields dedicated to agriculture are the source of costs for the cultivation. The vehicles contributed in the last century to support humans to operate in an efficient and repeatable way on field lowering the costs of workforce. Introducing automation machines and AI supported driving features frees the operator from the duty of driving lowering even more the human time requirements.	Business objective #1: To reduce the human contribution to the field management with effects on the related costs implied and the efficiency of the agricultural processing. Business objective #2: To reduce the occurrence of severe and potentially life-threatening accidents during agricultural activities, lowering the risk for the personnel operating in the harsh environment and that are prone to human error or underestimation of risks

		4) justice (the benefits of robotics should be distributed fairly).					Business process #2: Increase safety on extreme and critical field scenarios.	
03	2006/42/EC machinery directive	The directive aims at the free market circulation on machinery and at the protection of workers and consumers using such machinery. It defines essential health and safety requirements of general application, supplemented by a number of more specific requirements for certain categories of machinery	Critical	R&D	Legal	Edge AI Reference Models	Business process #1: Long time operations on fields dedicated to agriculture are the source of costs for the cultivation. The vehicles contributed in the last century to support humans to operate in an efficient and repeatable way on field lowering the costs of workforce. Introducing automation machines and AI supported driving features frees the operator from the duty of driving lowering even more the human time	Business objective #1: To reduce the human contribution to the field management with effects on the related costs implied and the efficiency of the agricultural processing. Business objective #2: To reduce the occurrence of severe and potentially life-threatening accidents during agricultural activities, lowering the risk for the personnel operating in the harsh environment and that are prone to human error or underestimation of risks

							requirements. Business process #2: Increase safety on extreme and critical field scenarios.	

Table 7 Ethical and Legal of SME Pilot III

5.1.1.4. SME PILOT IV POLYCOM (SLOVENIA): MAXIMIZATION OF AVAILABILITY, PRODUCTION QUALITY AND EFFICIENCY OF MOLDING MACHINES

5.1.1.4.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
Name, date, number, type, etc.	*Provide a summary/excerpt of the content/articles/rules of the regulatory source*	*Explain the relevancy of this regulatory source to your experiment*	*Any other relevant details*
ISO 9001: Quality management system	ISO 9001 is a globally recognized standard for quality management. It helps organizations of all sizes and sectors to improve their performance, meet customer expectations and demonstrate their commitment to quality. Its requirements define how to establish, implement, maintain, and continually improve a quality management system (QMS).	The standard helps identify and eliminate inefficiencies, reduce waste, streamline operations, and promote informed decision-making, resulting in cost savings and better outcomes. The developed tool will help in process improvement by providing additional process insight.	
IATF 16949: Quality management system for organizations in the automotive industry	IATF 16949:2016 is a technical specification aimed at the development of a quality management system which provides for continual improvement, emphasizing defect prevention and the reduction of variation and waste in the automotive industry supply chain and assembly process.	The developed tool will support: ● Process effectiveness and efficiency ● Problem Solving (root-cause analysis)	
ISO 14001: Satisfying requirements for an environmental management system	ISO 14001 is the internationally recognized standard for environmental management systems (EMS). It provides a framework for organizations to design and implement an EMS, and continually improve their environmental performance. By adhering to this standard, organizations can ensure they are taking proactive measures to minimize their environmental footprint, comply with relevant legal requirements, and achieve their environmental objectives.	The developed tool will support: ● controlling or influencing the way the organization's products are manufactured ● protecting the environment by preventing environmental impacts	

Table 8 Ethical and Legal of SME Pilot IV

5.1.1.4.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	**Explainability of AI**	Results of the AI solutions should provide means to explain why certain conclusions have been provided.	Preferred	R&D	Ethical	Production anomaly detection tool	Design and tracking of algorithms	Predictive maintenance
02	**Data safety and protection against unauthorized access**	Data interfaces should have means to protect against access from unauthorized agents and systems outside the facility	Critical	Production	Ethical	AI REDGIO 5.0 DATA SPACES	Data and model storage, sharing and reuse	Continuous research and development
03	**Storage of operator data**	Collecting of feedback from operators for tuning the sensitivity of algorithms should not be linked with specific operator.	Critical	Operator	Legal and Ethical	Collaborative Intelligence Platform for Edge AI in Manufacturing	Tuning and adjustment of the algorithms	Predictive maintenance
04	**Auditability of results**	The system should establish mechanisms that facilitate the auditability	Preferred	Accountability	Ethical	Production anomaly detection tool	Design and tracking of algorithms	Auditability of results

		of the AI systems						

Table 9 Ethical and Legal Requirements of SME Pilot IV

5.1.1.5. SME PILOT V QUESCREM (GALICIA, SPAIN): QUALITY IMPROVEMENT OF CHEESE PRODUCTS AND REDUCTION OF WASTES

5.1.1.5.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
EU AI Act	Title IV ('Transparency obligations for certain AI Systems')	Transparency obligations should be considered, especially when interacting with humans in order to provide explainability over the provided results from AI algorithms. Operators shall be able to know how the algorithms reached a certain conclusion.	
ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence	The document surveys topics related to trustworthiness in AI systems, including: — approaches to establish trust in AI systems through transparency, explainability, controllability, etc.; — engineering pitfalls and typical associated threats and risks to AI systems, along with possible mitigation techniques and methods; and — approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems.	Approaches to establish trust and assess the accuracy, safety, and security of the smart tools. Additionally, typical risks related to AI systems, and the possible mitigation techniques are documented.	

New industrial strategy for a green and digital Europe	Guidelines for innovation in Industrial environment	The new factsheet underlines the need for a guided introduction of new technologies in the industrial and productive ecosystem, underlining the need for education, re-skilling and training.	
Regulation (EC) No. 852/2004 of the European Parliament and of the Council of April 29, 2004	It is related to the hygiene of food products. This regulation obliges all food companies to have a HACCP (Hazard Analysis and Critical Control Point) system in place. Within the HACCP system, although it will be different for each industry, there are usually hazards to be measured during the production process and the shelf life of the product.	In critical process monitoring, there will be certain variables that must be measured and recorded to ensure food safety. In the case of the production process of the experiment, the monitoring of PCC1 (measurement and recording of incoming raw milk antibiotic tests), PCC2 (final pasteurization of the product, with the control and recording of the pasteurization temperature) and PCC3 (control of foreign bodies, with the recording of detectors, passing of witnesses and recording of possible positives) is carried out. In addition, there is also monitoring and recording of temperatures of cold chambers where ingredients and final product are stored. Of course, many more things are recorded during the process: cleaning, laboratory compositions, etc.	
QMS – Quality Management Systems **ISO 9001**	ISO 9001 is a set of standards, a certified quality management systems (QMS) that help manufacturing companies to ensure they meet customer and other stakeholder needs within statutory and regulatory requirements related to certain product.	The company is certified ISO 9001:2015 and IATF 16949:2016 (former ISO/TS 16949).	
Spanish Royal Decree 283/2001 of 16 March 2001 amending certain articles of the Corporate Income Tax Regulations on the deduction for investments in	Article 40 addresses environmental protection, amongst others to promote the reduction, recovery, or treatment of industrial waste.	This Royal Decree creates fiscal incentives for companies for investments contributing to environmental protection and can therefore promote eco-innovation.	

environmental protection.			
ISO 14001, Environmental Management System	It helps organizations improve their environmental performance through more efficient use of resources and reduction of waste, gaining a competitive advantage and the trust of stakeholders. This improvement can take many forms, such as improved communications and employee awareness, improved environmental performance, and improved emergency planning and response programs.	Lowering CO2 emission	

Table 10 Ethical and Legal Framework of SME PIlot V

5.1.1.5.2. Ethical and Legal Requirements

Req#	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset	Business Process	Business Objectives
01	**AI system's Accountability**	Potential risks should be identified, declared and minimized. Based on: The Ethics Guideline for Trustworthy AI (2019)	Critical	AI system's design and operational area	Ethical	The implementation of the AI system that is being designed and developed for the SustGAIN experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	Cream cheese production and quality monitoring, forecasting production KPIs and prescribing optimal production parameters	To improve the quality of the cream cheese and to increase the efficiency of the production process, by reducing the need of reprocessing the end product
02	**Privacy and data governance**	Proper data anonymization techniques and	Critical	AI system's operational area	Ethical	The implementation of the AI system	Cream cheese production	To improve the quality of the cream

		data management policy need to be assessed and implemented. Based on: General Data Protection Regulation (GDPR) (EU) Regulation 2016/679				that is being designed and developed for the SustGAIN experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	and quality monitoring, forecasting production KPIs and prescribing optimal production parameters	cheese and to increase the efficiency of the production process, by reducing the need of reprocessing the end product
03	**Sustainability**	Guidelines for innovation in Industrial environment and sustainability. Based on: New industrial strategy for a green and digital Europe (EC, 2020) [COM(2020) 102 final)]	Critical	AI system's operational area	Legal	The implementation of the AI system that is being designed and developed for the SustGAIN experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	Cream cheese production monitoring, forecasting production KPIs and prescribing optimal production parameters	Production process optimization by reducing the amount of waste generated
04	**Quality Management Systems**	ISO 9001 is a set of standards, a certified quality management system (QMS) that helps manufacturing companies ensure they meet customer and other stakeholder needs within statutory and regulatory	Critical	AI system's operational area	Legal	The implementation of the AI system that is being designed and developed for the SustGAIN experiment's use case is linked to this EL requirement. This implementation will integrate	Cream cheese production and quality monitoring, forecasting production KPIs and prescribing optimal production parameters	To improve the quality of the cream cheese and to increase the efficiency of the production process, by reducing the need of reprocessing

		requirements related to certain products. Based on: QMS – Quality Management Systems ISO 9001:2015 and IATF 16949:2016 (former ISO/TS 16949)				some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).		the end product
05	**Safety of the machines and system**	Machine Directive and other machine safety-related standards will be considered so the safety of the humans working in the pilot line environment, including researchers, is ensured.	Critical	Physical production system	Legal and ethical	This EL requirement refers to the physical production environment linked to the operation of the AI system that is being implemented for the SustGAIN pilot.	Cream cheese production and quality monitoring, forecasting production KPIs and prescribing optimal production parameters	To improve the quality of the cream cheese and to increase the efficiency of the production process, by reducing the need of reprocessing the end product
06	**Human agency and oversight**	AI systems can support the user in the decisional process, but proper oversight mechanisms should be implemented. Based on: The Ethics Guidelines for Trustworthy AI (2019) Nevertheless, no actions are expected to be automated based on the AI system's prescriptions in the scope of this experiment. The outputs of the AI system will only serve as valuable additional	Critical	AI system's operational area	Ethical	The implementation of the AI system that is being designed and developed for the SustGAIN experiment's use case is linked to this EL requirement. This implementation plans to integrate the AI REDGIO 5.0 Collaborative Intelligence Platform that is being developed in WP5.	Cream cheese production and quality monitoring, forecasting production KPIs and prescribing optimal production parameters	To improve the quality of the cream cheese and to increase the efficiency of the production process, by reducing the need of reprocessing the end product

		information for supporting the decision making of the human operators.						
07	**Technical robustness and safety**	A crucial component for achieving Trustworthy AI is technical robustness, which is closely linked to the principle of prevention of harm. Technical robustness requires that AI systems are developed with a preventative approach to risks and in a manner such that they reliably behave as intended, while minimising unintentional and unexpected harm and preventing unacceptable harm. This should also apply to potential changes in their operating environment or the presence of other agents (human and artificial) that may interact with the system in an adversarial manner. In addition, the physical and mental integrity of humans should be ensured. Based on The Ethics Guidelines for	Critical	AI system's design and implementation	Ethical	The implementation of the AI system that is being designed and developed for the SustGAIN experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	Cream cheese production and quality monitoring, forecasting production KPIs and prescribing optimal production parameters	To improve the quality of the cream cheese and to increase the efficiency of the production process, by reducing the need of reprocessing the end product

		Trustworthy AI (2019)						
08	**AI system's transparency**	Clear information has to be provided concerning the algorithm limitations, illustrating the reasoning and the data that led to the system prediction. Based on: The Ethics Guideline for Trustworthy AI (2019)	Critical	AI system's operational area	Ethical	The implementation of the AI system that is being designed and developed for the SustGAIN experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	Cream cheese production and quality monitoring, forecasting production KPIs and prescribing optimal production parameters	To improve the quality of the cream cheese and to increase the efficiency of the production process, by reducing the need of reprocessing the end product
09	**Risk assessment of the AI applications**	Before implementing the AI algorithms, a risk assessment must be performed in order to consider the possible implications that it could have on the installation from the security level. Based on: The Ethics Guideline for Trustworthy AI (2019) The machine room setpoints will not be automatically modified by AI algorithms. The AI algorithms will only provide recommendations to the human operators.	Critical	AI system's operational area	Ethical	The implementation of the AI system that is being designed and developed for the SustGAIN experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	Cream cheese production and quality monitoring, forecasting production KPIs and prescribing optimal production parameters	To improve the quality of the cream cheese and to increase the efficiency of the production process, by reducing the need of reprocessing the end product

10	**AI system's traceability**	The results of the algorithms must be tested regularly, ensuring that they fulfill the functions for which they were designed and that no variables appear over time that could cause anomalous operation. Based on: The Ethics Guideline for Trustworthy AI (2019) This will be achieved thanks to the nature of the AI algorithms implemented for this experiment, which are incremental/life-long learning models. Moreover, mechanisms will be provisioned to allow the tracking of the models' operation.	Preferred	AI system's operational area	Ethical	The implementation of the AI system that is being designed and developed for the SustGAIN experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	Cream cheese production and quality monitoring, forecasting production KPIs and prescribing optimal production parameters	To improve the quality of the cream cheese and to increase the efficiency of the production process, by reducing the need of reprocessing the end product
11	**Auditability of AI system's results**	The system should establish mechanisms that facilitate the auditability of the AI models, providing traceability of the training process. The system must provide means to ensure that third parties can audit the AI system, for instance. Based on: The Ethics Guideline	Preferred	AI system's operational area	Ethical	The implementation of the AI system that is being designed and developed for the SustGAIN experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in	Cream cheese production and quality monitoring, forecasting production KPIs and prescribing optimal production parameters	To improve the quality of the cream cheese and to increase the efficiency of the production process, by reducing the need of reprocessing the end product

		for Trustworthy AI (2019) Each of the datasets used for training each of the versions of the model will be registered, together with the corresponding evaluation metrics of each version.				the technical WPs (WP4/WP5).		

Table 11 Ethical and Legal Requirements of SME Pilot V

5.1.1.6. SME PILOT VI CAP (WALES, UK): INTELLIGENT CONTEXTUALISED VISUAL SYSTEM FOR ERROR REDUCTION

5.1.1.6.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
ISO 9001: Quality management system	ISO 9001 is a globally recognized standard for quality management. It helps organizations of all sizes and sectors to improve their performance, meet customer expectations and demonstrate their commitment to quality. Its requirements define how to establish, implement, maintain, and continually improve a quality management system (QMS).	The standard helps identify and eliminate inefficiencies, reduce waste, streamline operations, and promote informed decision-making, resulting in cost savings and better outcomes. The developed tool will help in process improvement by providing additional process insight	
EU AI Act	The AI Act is a proposed European regulation on artificial intelligence (AI) to assess the risk and potential harm of an AI system. The Act applies to all types of AI systems and is designed to ensure that risks to society are minimized.	Any new tools developed as prototypes under AI REDGIO 5 will be subject to the new AI act and therefore will need to be checked for compliance before market exploitation.	https://artificialintelligenceact.eu/

Table 12 Ethical and Legal Framework of SME Pilot VI

5.1.1.6.2. Ethical and Legal Requirements

Req#	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	Explainable AI	Ensuring that improvement decisions are explainable and appropriate	Preferred	Research and Prototyping	Ethical	Production anomaly detection tool	Design of self-healing production system	Quality and Auditability

02	Operator Safety	Ensuring that AI controlled production systems are safe for use with human operators	Critical	Production	Legal	Production control system and data integration layer	Process Control	Efficiency and Safety

Table 13 Ethical and Legal Requirements of SME Pilot VI

5.1.1.7. SME PILOT VII KATTY FASHION (ROMANIA): DEVELOPMENT OF A PRODUCT DEFECT DETECTION SYSTEM FOR CLOTHING ITEMS

5.1.1.7.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
Non Disclosure Agreements	KAF shall not disclose to any third party information related to the design or manufacturing information for the manufactured goods	Since the products used for analysis are covered by NDAs and represent confidential information, access to experiment data must be secured and limited to team members only	Since personal data or humans are not the subject of the experiment ethical aspects are not applicable
General Data Protection Regulation (GDPR)	appropriate technical and organizational measures	Legal Agreement with clients regarding the type of photos used and type of product used in the experiment	n/a
EU AI Act	Title IX ('Codes of Conduct')	AI activities proposed are minimal risk, at least a Code of Conduit is required.	

Table 14 Ethical and Legal of SME PIlot VII

5.1.1.7.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives

01	Technical Robustness and Safety	Validate security, safety, accuracy and reliability of solution using relevant guidelines.	Critical	QA Process Maintenance	Ethical	Key AI REDGIO 5.0 Technology Assets	Quality Control Process optimization Maintenance	Reduce waste Reduce time Decrease failure products
02	Human Agency and oversight	Implement proper oversight mechanisms	Critical	QA Process Maintenance	Ethical	Key AI REDGIO Technology Assets	Quality Control Process Optimization Maintenance	Reduce waste Reduce time Decrease failure products
03	Explainability of AI	Offering users the reasoning and/or description for QA issues detection should improve user trust and engagement	Optional	Data reasoning	Ethical	Key AI REDGIO Technology Assets	Quality Control Process Optimization Maintenance	User Wellbeing and engagement
04	Transparency	Declare limitations, reasoning snd data used	Critical	QA Process Maintenance	Ethical	Key AI REDGIO Technology Assets	Quality Control Process Optimization Maintenance	Quality Control Process Optimization Maintenance

05	Accountability	Identify, declare and minimize potential risks	Critical	QA Process Maintenance	Ethical	Key AI REDGIO Technology Assets	Quality Control Process Optimization Maintenance	Quality Control Process Optimization Maintenance
06	GDPR Compliance	Targeted users must provide explicit and informed consents	Critical	Data Management	Ethical & Legal	Key AI REDGIO Technology Assets	Quality Control Process Optimization Maintenance	Quality Control Process Optimization Maintenance
07	Data Security	Tested solution should comply with the highest standards of data security & quality	Medium	Data Management	Legal	Policies and strategies for data management and security which should guarantee protection against data breach/loss	Business	Data security and management

Table 15 Ethical and Legal Requirements of SME Pilot VII

5.1.2. DF experiments

5.1.2.1. DFI: POLIMI - I4.0LAB (LOMBARDY, ITALY): INDUSTRY4.0LAB

5.1.2.1.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
EU 348/2013	Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), in particular for what concerns the hexavalent chromium, which could be released in desoldering PCB summary or extract of the content/articles/rules	Environmental conditions of desoldering activities	

	of this regulatory source relevant to the experiment		
WEEE Directive 2012/19/EU	At the regulatory level, the WEEE Directive 2012/19/EU considers the producer responsibility "one of the means of encouraging design and production of EEE which take into full account and facilitate its repair, possible upgrading, re-use, disassembly and recycling".	Environmental conditions	
ISO/TS 15066-2016	ISO/TS 15066:2016 specifies safety requirements for collaborative industrial robot systems and the work environment, and supplements the requirements and guidance on collaborative industrial robot operation given in ISO 10218-1 and ISO 10218-2.	ISO/TS 15066:2016 applies to industrial robot systems as described in ISO 10218-1 and ISO 10218-2. It does not apply to non-industrial robots, although the safety principles presented can be useful to other areas of robotics.	
EN 50625-1:2014	Collection, logistics & Treatment requirements for WEEE - Part 1: General treatment requirements	This European Standard is applicable to the treatment of waste electrical and electronic equipment (WEEE). This standard will be supplemented, for example by standards covering specific equipment.	

Table 16 Ethical and Legal Framework of DF I

5.1.2.1.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	Safety Requirements for Industrial Robots	ISO 10218-1:2011 specifies requirements and guidelines for the inherent safe design, protective measures and information for use of industrial robots. It describes basic hazards associated with robots and provides requirements to eliminate, or adequately reduce, the	Critical	Industrial Robotics	Legal		Industrial Robotic Operation	Ensure Robotic Safety during Operation

		risks associated with these hazards						
02	Collaborative Robotics – Human-Robot Interaction	ISO/TS 15066:2016 specifies safety requirements for collaborative industrial robot systems and the work environment, and supplements the requirements and guidance on collaborative industrial robot operation given in ISO 10218-1 and ISO 10218-2. ISO/TS 15066:2016 applies to industrial robot systems as described in ISO 10218-1 and ISO 10218-2. It does not apply to non-industrial robots, although the safety principles presented can be useful to	Critical	Industrial Collaborative Robotics	Legal		Industrial Collaborative Robotics; Human-Robot Interaction	Ensure Robotic Safety during Operation; Promote Human-Robot Interaction and Collaboration

		other areas of robotics.						
03	Privacy and data governance	Proper data anonymization tecniques and and data management policy need to be in place. Based on: General Data Protection Regulation (GDPR) (EU) Regulation 2016/679	Critical	AI Infrastructure printed circuit board disassembly	Ethical		PCB dismantling	data management and privacy
04	Storage of operator data	At current point, we don't expect to collect personal data during the experimentation. However, if that should happen, we will follow GDPR	Preferred	Operator	Legal and Ethical		optimizing the onboarding of new employees in disassembling products	Lower entry barriers for less skilled and/or inexperienced personnel and/or High Complexity -Low volume production
05	Risk assessment of the AI applications	Before implementing the AI algorithms, a risk assessment must be performed in order to consider the	Critical	Operational area	Ethical	AI implementation	The machine room setpoints will be modified by AI algorithms directly or through recommendations.	Risk assessment of the AI applications.

		possible implications that it could have on the installation from the security level. Based on: The Ethics Guideline for Trustworthy AI (2019)						

Table 17 Ethical and Legal Requirements of DF I

5.1.2.2. DFII: UNIBO – ACTEMA (EMILA-ROMAGNA, ITALY): E^{2}MECH

5.1.2.2.1. Ethical and Legal Framework

Regulatory Source	Relevant content	Legal and/or ethical issues concerned	Other
Data Act	Data Privacy	Ownership of raw and elaborated data and their potential commercial use	Transfer learning might be considered
EU Artificial Intelligence Act	Codes of conduct	Our application to the collected data, i.e. for condition monitoring and predictive maintenance, does not fall into the high-risk category, and generative algorithms are not foreseen at the moment. However, legal sandboxes and guideline which will be given also at national level will be followed.	/
EU Regulation 2023/1230 on machinery	Codes of conduct	At the moment we do not expect to deal with safety critical conditions directly with our algorithms (a separate and certified safety system is assumed to be operational).	/

Table 18 Ethical and Legal of DF II

5.1.2.2.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset	Business Process	Business Objectives

01	Privacy and data governme nt	Issues concerning ownership of raw and elaborated data generated by the experiment should be considered. Particularly if data can potentially be used for commercializat ion, e.g. for transfer learning applications to similar systems	preferr ed	AI infrastructure	Legal		Anomaly detection, condition monitorin g, and predictive maintena nce	Automatiz e and improve maintena nce procedure for mechatro nic mechanis ms and automatic machines
02	Transpare ncy	Clear information must be provided concerning the algorithm limitations, illustrating the rationale and the data that led to the system prediction/res ults. Based on: The Ethics Guideline for Trustworthy AI (2019) .	preferr ed	Operational area	Ethic al	AI quality control	Anomaly detection, condition monitorin g, and predictive maintena nce	Automatiz e and improve maintena nce procedure for mechatro nic mechanis ms and automatic machines
03	EU Regulation 2023/123 0 on machinery	We do not expect to use AI for automatically trigger safety critical operations of the machines.	Preferr ed	Production/Operato r	Legal		Automatic detection with AI of safety critical conditions	Improve system's safety with AI

Table 19 Ethical and Legal Requirements of DF II

5.1.2.3. DFIII JSI - IJS SYSTEMS & CONTROL LAB (SLOVENIA) E2-LAB: SELF-EVOLVING MONITORING SYSTEMS FOR ASSEMBLY PRODUCTION LINES

5.1.2.3.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
New industrial strategy for a green and digital Europe (EC, 2020) [COM(2020) 102 final)]	Industrial strategy that would support the twin transition to a green and digital economy, make EU industry more competitive globally, and enhance Europe's open strategic autonomy.	Need for a guided introduction of new technologies in the industrial and productive ecosystem and the need for education, re-skilling and training of the workforce.	
ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence	The document surveys topics related to trustworthiness in AI systems, including: - approaches to establish trust in AI systems through transparency, explainability, controllability, etc.; - engineering pitfalls and typical associated threats and risks to AI systems, along with possible mitigation techniques and methods; and - approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems.	Topics relevant for the developed solution: data pre-processing and modelling, bias, unpredictability, model updates, software defects, HCI factors.	

Table 20 Ethical and Legal Framework of DF III

5.1.2.3.2. Ethical and Legal Requirements (Trial HandbookSect. 2.3)

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	**Explainability**	Results of the AI solutions should provide means to explain why certain conclusions have been provided.	Preferred	Operational	Ethical	Production anomaly detection tool	Design and tracking of algorithms	Predictive maintenance

02	**Privacy and data governance**	Proper data anonymization techniques and data management policy need to be in place for data to be shared in order to hide sensitive information.	Critical	R&D	Ethical	AI REDGIO 5.0 DATA SPACES.	Data sharing and reuse	Test and develop new algorithms
03	**Traceability and auditability**	The results of the algorithms must be tested regularly, ensuring that they fulfil the functions for which they were designed and that no variables appear over time that could cause anomalous or condition changes in a way that models are not valid any more.	Preferred	Operational	Ethical	Production anomaly detection tool	Monitoring preformance of the algorithms	Predictive maintenance

Table 21 Ethical and Legal Requirements of DF III

5.1.2.4. DFIV: BRAINPORT INDUSTRIES (THE NETHERLAND) - FLEXIBLE MANUFACTURING - VISION ENHANCEMENT THROUGH SYNTHETIC DATA

5.1.2.4.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
ISO/TS 15066-2016	ISO/TS 15066:2016 specifies safety requirements for collaborative industrial robot systems and the work environment, and supplements the requirements and guidance on collaborative industrial robot	ISO/TS 15066:2016 applies to industrial robot systems as described in ISO 10218-1 and ISO 10218-2. It does not apply to non-industrial robots, although the safety principles presented can be useful to other areas of robotics.	

	operation given in ISO 10218-1 and ISO 10218-2.		
WEEE Directive 2012/19/EU	At the regulatory level, the WEEE Directive 2012/19/EU considers the producer's responsibility "one of the means of encouraging design and production of EEE which take into full account and facilitate its repair, possible upgrading, re-use, disassembly and recycling".	Environmental conditions	
EN 50625-1:2014	Collection, logistics & Treatment requirements for WEEE - Part 1: General treatment requirements	This European Standard is applicable to the treatment of waste electrical and electronic equipment (WEEE). This standard will be supplemented, for example by standards covering specific equipment.	
Machine Directive, ISO 12100, ISO 13849, ISO 10218 1-2, TS 15066	The safety of the humans working in the laboratory and pilot line environment, including researchers, students and laboratory personnel, has to be ensured by following the Machine Directive as much as possible, and especially obeying the mentioned standards.	There are no legal or ethical issues raised by the experiment.	
ROS 1 and ROS2	ROS 1 and from very recently ROS 2 are the most popular robotic environments followed by the Open Source community in all hardware and/or software related developments in the domain of robotic operations.	Technology exploited so far in the development of the experiment's Open Scalable Production System, aggregating robotic manipulators and digital twins, uses ROS technology. Currently, these principles do not yet apply to the experiment but as AAS implications and applicability will be researched, these might become more relevant.	
IDS-RAM	Reference architectural model for data sovereignty. Standard to use when interchanges are desired to be carried out maintaining the property and governance of those items to be exchanged (data, models, etc.)	Data acquisition from AM-FLOW's machines and the usage of these data and the resultant prediction models. Currently, these principles do not yet apply to the experiment but as AAS implications and applicability will be researched, these might become more relevant.	
GDPR (General Data Protection Regulation)	Article 5: Principles relating to processing of personal data	The processing of personal data shall be lawful, fair, and transparent. Data shall be collected for specified, explicit, and legitimate purposes. Even though our experiment currently is not using, nor expecting to use personal data, we will make sure to abide by GDPR regulation (AVG in Dutch, is a direct translation).	
AI Act	Regulations on the use of autonomous systems in specific industries.	Specifies guidelines and requirements for artificial intelligence, particularly in safety-critical industries.	

Intellectual Property Laws	Patent, copyright, and trademark laws	Protection of intellectual property rights for developed technologies and innovations at SME-level.	

Table 22 Ethical and Legal Framework of DF IV

5.1.2.4.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	Safety Requirements for Industrial Robots	ISO 10218-1:2011 specifies requirements and guidelines for the inherent safe design, protective measures and information for use of industrial robots. It describes basic hazards associated with robots and provides requirements to eliminate, or adequately reduce, the risks associated with these hazards	Critical	Industrial Robotics	Legal	AM-Vision system, AAS	Industrial Robotic Operation	Ensure Robotic Safety during Operation.
02	Collaborative Robotics – Human-Robot Interaction	ISO/TS 15066:2016 specifies safety requirements for collaborative industrial robot systems and the work environment, and supplements the requirements	Critical	Industrial Collaborative Robotics	Legal	AM-Vision System, AAS	Industrial Collaborative Robotics; Human-Robot Interaction	Ensure Robotic Safety during Operation; Promote Human-Robot Interaction and Collaboration.

		and guidance on collaborative industrial robot operation given in ISO 10218-1 and ISO 10218-2. ISO/TS 15066:2016 applies to industrial robot systems as described in ISO 10218-1 and ISO 10218-2. It does not apply to non-industrial robots, although the safety principles presented can be useful to other areas of robotics.						
03	Privacy and data governance	Proper data anonymization techniques and data management policy need to be in place. Based on: General Data Protection Regulation (GDPR) (EU) Regulation 2016/679	Critical	AI Infrastructure printed circuit board disassembly	Ethical	AM-Vision system, Synthetic Training Data	Synthetic Data Collection	Data management and privacy.

04	Storage of operator data	At this point, we don't expect to collect personal data during the experimentation. However, if that should happen, we will follow GDPR	Preferred	Operator	Legal and Ethical	AM-Vision system	Optimizing the onboarding of (new) employees in product recognition.	Lower entry barriers for less skilled and/or inexperienced personnel and/or High Complexity -Low volume production.
05	Risk assessment of the AI applications	Before implementing the AI algorithms, a risk assessment must be performed in order to consider the possible implications that it could have on the installation from the security level. Based on: The Ethics Guideline for Trustworthy AI (2019)	Critical	Operational area	Ethical	AI implementation	The machine output and the operator's work will change by AI algorithms directly or through recommendations.	Risk assessment of the AI applications.

Table 23 Ethical and Legal Requirements of DF IV

5.1.2.5. DFV: UNITWENTE – AMC (THE NETHERLAND): IIOT SMART BOX

5.1.2.5.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
Name, date, number, type, etc.	*Provide a summary/excerpt of the content/articles/rules of the regulatory source*	*Explain the relevancy of this regulatory source to your experiment*	*Any other relevant details*

EU AI Act	The AI Act is a European regulation pertaining to the field of artificial intelligence (AI).The EU AI Act applies to AI systems in the EU under general circumstances. Some parts of the content are relevant to this experiment such Chapter I: General Provisions, Chapter V: General Purpose AI Models.	For the processing of various machine data in experiments, the specifications for AI model application need to be checked and the compliance with the EU AI act.	
EU Data Act	The EU Data Act aims to enhance the EU data economy by making data more accessible and usable, encouraging data-driven innovation and improving data availability. Some parts of this Data Act are relevant to this experiment, such as Chapter II on business-to-business and business-to-consumer data sharing in the context of IoT, Chapter VI on switching between data processing services, Chapter VIII on interoperability.	In the experiment, this system collects, transmits and stores machine data safely under the concept of industrial IoT. and concerns about data reliability and some norms for sharing data.	

Table 24 Ethical and Legal Framework of DF V

5.1.2.5.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	Data Security	The experimental system should ensure safe and reliable transmission and storage of machine data. Data sharing is carried out under a	Critical	Data management	Legal	Open platform	Performance	Data Security

		reliable authorization mechanism.						
02	Explainable AI	The AI algorithm in the experiment provides explainable reasons, and the results given can be explained through expert knowledge,	Preferred	AI system	Legal	Edge AI Reference Models	optimization	Supports productivity improvement, etc.
03	Transparency	The data collected by the system during the experiment and the AI algorithm will remain traceable and transparent.	Critical	Data management and AI system	Legal	Open hardware and platform	optimization	Supports productivity improvement, etc.

Table 25 Ethical and Legal Requirements of DF V

5.1.2.6. DFVI: FBK - 4.0ILAB (TRENTINO, ITALY): 4.0ILAB

5.1.2.6.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
Name, date, number, type, etc.	*Provide a summary/excerpt of the content/articles/rules of the regulatory source*	*Explain the relevancy of this regulatory source to your experiment*	*Any other relevant details*
Ethics guidelines for trustworthy AI (From EC) Europe's Internet o Things Policy (From EC) A European Strategy for data (from EC)	To give general guidelines to regulate AI throughout its entire life cycle to be lawful, ethical, and robust. Collection of actions and programs of the European Commission to plan and support the future of IoT. The strategy for data focuses on proposing policy and legal solutions concerning	The need to develop ethical and robust AI solutions and so to meet the seven requirements indicated by the EC. The need to securely identify devices to be plugged into IoT networks. The need to offer fair access to and use of the data collected during the experiment.	

	the free flow of data across national borders within the EU		

Table 26 Ethical and Legal Framework of DF VI

5.1.2.6.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	Data collection and storage	Metrics should be collected and stored for monitoring and evaluation	Critical	Research	Legal			Application monitoring and benchmarking

Table 27 Ethical and Legal Requirements of DF VI

5.1.2.7. DFVII MAKE - PM50 (FLANDERS, BELGIUM): PREDICTIVE MAINTENANCE 5.0

5.1.2.7.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
New industrial strategy for a green and digital Europe (EC, 2020) [COM(2020) 102 final)]	Industrial strategy that would support the twin transition to a green and digital economy, make EU industry more competitive globally, and enhance Europe's open strategic autonomy.	Need for a guided introduction of new technologies in the industrial and productive ecosystem and the need for education, re-skilling and training of the workforce.	
OPC Foundation	OPC Unified Architecture standard	Standardised data models, communication patterns and security models for industry	
Cyber Resilience Act (CRA)	Regulation on cybersecurity requirements for products with digital elements	Involves Security by Design that has to be taken into account by all companies by 2027	
ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence	The document surveys topics related to trustworthiness in AI systems, including: - approaches to establish trust in AI systems through transparency, explainability, controllability, etc.; - engineering pitfalls and typical associated threats and risks to AI systems,	Topics relevant for the developed solution: data pre-processing and modelling, bias, unpredictability, model updates, software defects, HCI factors.	

	along with possible mitigation techniques and methods; and - approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems.		

Table 28 Ethical and Legal Framework of DF VII

5.1.2.7.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	**Explainability**	Results of the AI solutions should provide means to explain why certain conclusions have been provided.	Preferred	Operational	Ethical	Predictive Maintenance 5.0	Design and tracking of algorithms	Predictive maintenance
02	**Traceability and auditability**	The results of the algorithms must be tested regularly, ensuring that they fulfil the functions for which they were designed and that no variables appear over time that could cause anomalous or condition changes in a way that models are not valid any more.	Preferred	Operational	Ethical	Predictive Maintenance 5.0	Monitoring preformance of the algorithms	Predictive maintenance

03	**Accountability**	Potential risks should be identified, declared and minimized. Based on: The Ethics Guideline for Trustworthy AI (2019)	Critical	Operational area	Ethical	AI Quality Control	Quality control score; Fault detection	Reduce maintenance time
04	**Storage of operator data**	At this point, we don't expect to collect personal data during the experimentation. However, if that should happen, it will be compliant with GDPR.	Preferred	Operator	Legal and Ethical	AM-Vision system	Optimizing the onboarding of (new) employees in product recognition.	Lower entry barriers for less skilled and/or inexperienced personnel and/or High Complexity-Low volume production.
05	**Risk assessment of the AI applications**	Before implementing the AI algorithms, a risk assessment must be performed in order to consider the possible implications that it could have on the installation from the security level. Based on: The Ethics Guideline for Trustworthy AI (2019)	Critical	Operational area	Ethical	AI implementation	The machine output and the operator's work will change by AI algorithms directly or through recommendations.	Risk assessment of the AI applications.

Table 29 Ethical and Legal Requirements of DF VII

5.1.2.8. DFVIII DMWI - DIGITAL INNOVATION MANUFACTURING INNOVATION HUB (WALES, UK): INDUSTREWEB OPERATOR KNOWLEDGEBASE (IWOK)

5.1.2.8.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other

ISO 23247 Digital Twin Standards	Automation systems and integration — Digital twin framework for manufacturing	A digital twin assists with detecting anomalies in manufacturing processes to achieve functional objectives such as real-time control, predictive maintenance, in-process adaptation, Big Data analytics, and machine learning. A digital twin monitors its observable manufacturing element by constantly updating relevant operational and environmental data. The visibility into process and execution enabled by a digital twin enhances manufacturing operation and business cooperation.	

Table 30 Ethical and Legal Framework of DF VIII

5.1.2.8.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	Explainable AI	Ensuring decision-making process is explainable	Preferred	IWOK (Decision Tree)	Ethical	Industreweb Operator Knowledge Base (IWOK) Edge application	Performance optimisation	Process Improvement
02	Operator Safety	Ensuring safety of human operators whilst using IWOK	Critical	Production System Control	Legal	Industreweb Operator Knowledge Base (IWOK) Edge application	Performance optimisation	Compliance and Continual Improvement

Table 31 Ethical and Legal Requirements of DF VIII

5.1.2.9. DFIX: MADE (LOMBARDY, ITALY): BEHAI – ADAPTING QUALITY INSPECTION SYSTEM TO HUMAN BEHAVIOR AND HUMAN STATES

5.1.2.9.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
ISO/TS 15066:2016 Robots and robotic devices	ISO/TS 15066:2016 specifies safety requirements for collaborative industrial robot systems and the work environment, and supplements the requirements and guidance on collaborative industrial robot operation given in ISO 10218-1 and ISO 10218-2. ISO/TS 15066:2016 applies to industrial robot systems as described in ISO 10218-1 and ISO 10218-2. It does not apply to non-industrial	ISO/TS 15066 provides guidelines for the design and implementation of a collaborative workspace that reduces risks to people. It specifies: Important characteristics of safety control systems Factors to be considered in the design of collaborative robot systems	

	robots, although the safety principles presented can be useful to other areas of robotics.	Built-in safety-related systems and their effective use Guidance on implementing the following collaborative techniques: **safety-rated monitored stop**; **hand guiding**; **speed and separation monitoring**; **power and force limiting**.	
ISO/IEC 24745 - Information security, cybersecurity and privacy protection — Biometric information protection	ISO/IEC 24745 covers the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. It also provides requirements and recommendations for the secure and privacy-compliant management and processing of biometric information. This document does not include general management issues related to physical security, environmental security and key management for cryptographic techniques.	ISO/IEC 24745 provide the guidelines to be followed while handling biometrics data, in particular specifies: Analysis of the threats to and countermeasures inherent to biometrics and biometric system application models; Security requirements for securely binding between a biometric reference (BR) and an identity reference (IR); Biometric system application models with different scenarios for the storage and comparison of BRs; Guidance on the protection of an individual's privacy during the processing of biometric information.	
European Commission Ethics Guidelines for Trustworthy Artificial Intelligence	On 8 April 2019, the High-Level Expert Group on AI presented tasked by EC released a set of Guidelines that set out a framework for achieving Trustworthy AI.	The Guidelines put forward a set of 7 key requirements that AI systems should meet in order to be deemed trustworthy. A specific assessment list aims to help verify the application of each of the key requirements: - Human agency and oversight - Technical Robustness and safety - Privacy and data governance: - Transparency - Diversity, non-discrimination and fairness - Societal and environmental well-being - Accountability	Human agency and oversight, Non-discrimination and fairness, Societal and environmental well-being, Privacy and data governance checklist are particularly significant for this use case
General Data Protection Regulation (GDPR) Regulation (EU) 2016/679	The General Data Protection Regulation (GDPR) is a comprehensive data privacy law that establishes a framework for the collection, processing, storage, and transfer of personal data.	To process data it is necessary to do so according to seven protection and accountability principles outlined in Article 5.1-2: Lawfulness, fairness and transparency — Processing must	

		be lawful, fair, and transparent to the data subject. Purpose limitation — Process data for the legitimate purposes specified explicitly to the data subject collected. Data minimization — Collect and process only as much data as absolutely necessary for the purposes specified. Accuracy — Keep personal data accurate and up to date. Storage limitation — Store only personally identifying data for as long as necessary for the specified purpose. Integrity and confidentiality — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption). Accountability — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.	
QMS – Quality Management Systems ISO 9001	ISO 9001 is a globally recognized standard for quality management. It helps organizations of all sizes and sectors to improve their performance, meet customer expectations and demonstrate their commitment to quality. Its requirements define how to establish, implement, maintain, and continually improve a quality management system (QMS):	ISO 9001 in particular the chapter 7.1 address the provision and the maintenance of the environment necessary for the operation of its processes and to achieve conformity of products and services.	

5.1.2.9.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	**Safety of Machinery**	ISO 13855:2010 establishes the positioning of safeguards with respect to the approach speeds of parts of the human	Critical	Industrial Robotics; Machinery	*legal*		Robotics Operation; Human Safety in Industrial environments	Ensure Robotic Safety during Operation

		body. It specifies parameters based on values for approach speeds of parts of the human body and provides a methodology to determine the minimum distances to a hazard zone from the detection zone or from actuating devices of safeguards. The values for approach speeds (walking speed and upper limb movement) in ISO 13855:2010 are time tested and proven in practical experience. ISO 13855:2010 gives guidance for typical approaches. Other types of approach, for example running, jumping or falling, are not considered in ISO 13855:2010.						

02	**Collaborative Robotics – Human-Robot Interaction**.	ISO/TS 15066:2016 specifies safety requirements for collaborative industrial robot systems and the work environment, and supplements the requirements and guidance on collaborative industrial robot operation given in ISO 10218-1 and ISO 10218-2. ISO/TS 15066:2016 applies to industrial robot systems as described in ISO 10218-1 and ISO 10218-2. It does not apply to non-industrial robots, although the safety principles presented can be useful to other areas of robotics.	*Critical*	Industrial Collaborative Robotics	*Legal*		Industrial Collaborative Robotics; Human-Robot Interaction	Ensure Robotic Safety during Operation; Promote Human-Robot Interaction and Collaboration

Table 32 Ethical and Legal Requirements of DF X

5.1.2.10. DFX: TUIASI I4.0 (ROMANIA): IMPLEMENTATION OF QAD-AI@E SOLUTION IN THE REAL CLOTHING MANUFACTURING ENVIRONMENT

5.1.2.10.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
Directive 2006/42/EC	Directive 2006/42/EC, known as the Machinery Directive, is a European Union directive that aims to ensure the safety and health of workers and	The directive applies to machinery, interchangeable equipment, safety components, lifting accessories, chains, ropes and webbing,	

	consumers by regulating the design and manufacture of machinery.	removable mechanical transmission devices, and partly completed machinery.	
Ethics guidelines for trustworthy AI/2019	The "Ethics Guidelines for Trustworthy AI," issued by the High-Level Expert Group on Artificial Intelligence (AI HLEG) appointed by the European Commission, outline the key principles and requirements for developing and deploying AI systems in a manner that is ethical and trustworthy. These guidelines focus on ensuring that AI systems are aligned with fundamental rights, societal values, and user needs	Requirements for Trustworthy AI **1. Human Agency and Oversight:** a) AI systems should support human decision-making processes and empower users. b) There should be mechanisms for human oversight, such as the ability to intervene or oversee the AI system. **2. Technical Robustness and Safety:** a) AI systems should be reliable and function as intended under normal and unexpected conditions. b) They should include security measures to prevent malicious use and ensure data integrity. **3. Privacy and Data Governance:** a) AI systems should respect privacy and data protection laws. b) They should ensure data quality, integrity, and security while providing users with control over their data.	

Table 33 Ethical and Legal Framework of DF XI

5.1.2.10.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	**Safety of Machinery**	QAD-AI@E has moving parts that are controlled by AI algorithms but proper	Critical	Machinery	Legal	Collaborative Intelligence Platform for Edge AI in Manufacturing	Human Safety in Industrial environments	Ensure Machinery Safety during Operation

		oversight mechanisms should be implemented.						
02	**Human agency and oversight**	QAD-AI@E support the user in the decisional process	- Optional]	Quality prediction	- Ethical	Technological Asset: IDSS for predictive quality assurance	Quality Control	Improve and automate quality control

Table 34 Ethical and Legal Requirements of DF XI

5.1.2.11. DFXI CTU RICAIP (CZECH REPUBLIC): AI-DRIVEN MONITORING OF ROBOTIC ASSEMBLY PROCESS

5.1.2.11.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
Name, date, number, type, etc.	*Provide a summary/excerpt of the content/articles/rules of the regulatory source*	*Explain the relevancy of this regulatory source to your experiment*	*Any other relevant details*
National Artificial Intelligence Strategy of the Czech Republic, 2019,	Its priority areas include (section 6.3.2 and 6.3.3) upgrading the legal framework of the Czech Republic to address consumer protection and safety; intellectual property protection; cybersecurity; and data protection and management.	It focuses on esponsible and trusted AI ecosystem, digitalisation of enterprises, in particular SMEs, equitable opportunities and benefits in AI to boost the economic development of society.	https://vlada.gov.cz/assets/evropske-zalezitosti/umela-inteligence/NAIS_kveten_2019.pdf
Information technology Artificial intelligence Management system ISO/IEC 42001, 2023	addresses the unique challenges posed by AI, including ethical considerations, transparency, and the necessity of continual learning.	ethical considerations, transparency and continual learning	

Table 35 Ethical and Legal Framework of DF XI

5.1.2.11.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	Compliance with to internal company regulations.	Although the experiment is realized in a digital factory, it should demonstrate what internal regulations could be an issue for its real deployment in factory..	Preferred	Production	Legal	Examples of regulatory sources and their relevant legal issues collected in AI REDGIO 5.0.	AI driven assembly process monitoring	Better quality of the assembled products
02	Keep the human in the loop.	Human can start to over rely on the AI system and provide poor feedback. To avoid this, It is needed to keep his attention and keep him in the quality control loop.	Critical	Quality control	Ethical	Edge AI Reference Models	Continual learning and AI system monitoring	More effective quality control

Table 36 Ethical and Legal Requirements of DF XI

5.1.2.12. DFXII AAU SMART LAB (DENMARK): AAU ADVANCED IOT

5.1.2.12.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
ISO/IEC 29182-1:2013	The standard provides a general overview of the characteristics of a sensor network and the organization of the entities that comprise such a network. It also describes the general requirements that are identified for sensor networks.	The experiment focuses on collecting and processing the sensor data of the production line.	
ISO/IEC TR 30166:2020 (E)	The standard provides guidance and overview of the application of IoT technologies in industrial environments. It addresses the specific requirements, challenges, and	The experiment targets the SMEs which require industrial focused IoT solution.	

	considerations for implementing IoT solutions in industrial setting.		

Table 37 Ethical and Legal Framework of DF XII

5.1.2.12.2. Ethical and Legal Requirements (Trial HandbookSect. 2.3)

Req#	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	Data access and storage	Sensor data should be collected and stored for production monitoring and training AI model	Critical	Production	Legal	Local Open Hardware	BP1	Enable real-time multi-sensor monitoring
02	Quality management	The AI model should be able to assist the quality control.	preferred	R&D	Legal	Edge AI Reference Models	BP2	Enable production failures detection

Table 38 Ethical and Legal Requirements DF XII

5.1.2.13. DFXIII PBN amLAB (HUNGARY): SUNSYNC: AI SOLUTION FOR OPTIMIZING RECYCLING IN INDUSTRY AT THE LEVEL OF AM-LAB'S DF

5.1.2.13.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
QMS – Quality Management Systems ISO 9001	ISO 9001 is a set of standards, a certified quality management systems (QMS) that help manufacturing companies ensuring they meet customer and other stakeholder needs within statutory and regulatory requirements related to certain product	The Quality Management System of PBN according to the MSZ EN ISO 9001:2015 standard, covers the following areas: Unique plastic component production, use of 3D printing technologies • Education • Project management • R&D activity	

EU AI Act	The AI Act is a European regulation pertaining to the field of artificial intelligence (AI).The EU AI Act applies to AI systems in the EU under general circumstances. For our experiment the following sessions should be considered: Chapter I: General Provisions, Chapter IV 'Transparency obligations for certain AI Systems' Chapter V: General Purpose AI Models.	For the processing of various machine data in experiments, the specifications for AI model application need to be checked and the compliance with the EU AI act. Transparency obligations should be considered, especially when interacting with humans, in order to provide explainability over the provided results from AI algorithms. Operators shall be able to know how the algorithms reached a certain conclusion.	
New industrial strategy for a green and digital Europe	Guidelines for innovation in Industrial environment	The new factsheet underlines the need for a guided introduction of new technologies in the industrial and productive ecosystem, underlining the need for education, re-skilling and training.	

Table 39 Ethical and Legal Framework DF XIII

5.1.2.13.2. Ethical and Legal Requirements

Req #	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset /other tool	Business Process	Business Objectives
01	Quality Management Systems	ISO 9001 is a set of standards, a certified quality management systems (QMS) that help manufacturing companies ensuring they meet customer and other stakeholder needs within statutory and regulatory requirements related to	Critical	The Quality Management System of the Pannon Economic Network Association was created in accordance with the MSZ EN ISO 9001:2015 standard and its requirements; The Quality Management System of PBN	Legal	The entire experiment is following the MSZ EN ISO 9001:2015 standard and requirement. The dataset created within the experiment is also in line with ISO requirements.	Quality control	Improve quality control

		certain product		according to the MSZ EN ISO 9001:2015 standard, covers the following areas: •Unique plastic component production, use of 3D printing technologies • Education •Project management • R&D activity				
02	**Safety of the machines and system**	Machine Directive and other machine safety-related standards will be considered so the safety of the humans working in the pilot line environment, including researchers, is ensured.	Critical	Physical production system	Legal and ethical	This EL requirement refers to the physical manufacturing cell linked to the operation of the AI system that is being implemented for the am-LAB Didactic Factory experiment.	Provision and dissemination of a site for testing, showcasing and training on the use and potential of Edge&AI technologies in a realistic industrial environment.	To maximize reach to manufacturing companies in near environment. To maximize reach to students and learning organizations in near environment.
03	**Transparency**	The data collected by the system during the experiment and the AI algorithm	Critical	Data management and AI system	Legal	Open hardware and platform	optimization	Supports productivity improvement, etc.

		will remain traceable and transparent.						

Table 40 Ethical and Legal Requirements DF XIII

5.1.2.14. DFXIV: GRADIANT - GALICIA INDUSTRIAL LOGISTICS LAB (SPAIN): GALICIA DF

5.1.2.14.1. Ethical and Legal Framework

Regulatory source	Relevant content	Legal and/or ethical issues concerned	Other
EU AI Act	Title IV ('Transparency obligations for certain AI Systems')	Transparency obligations should be considered, especially when interacting with humans, in order to provide explainability over the provided results from AI algorithms. Operators shall be able to know how the algorithms reached a certain conclusion.	
ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence	The document surveys topics related to trustworthiness in AI systems, including: — approaches to establish trust in AI systems through transparency, explainability, controllability, etc.; — engineering pitfalls and typical associated threats and risks to AI systems, along with possible mitigation techniques and methods; and — approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems.	Approaches to establish trust and assess the accuracy, safety, and security of the smart tools. Additionally, typical risks related to AI systems, and the possible mitigation techniques are documented.	

Machine Directive, ISO 12100, ISO 13849, ISO 10218 1-2, TS 15066	The safety of the humans working in the laboratory and pilot line environment, including researchers, students and laboratory personnel, has to be ensured by following the Machine Directive as much as possible, and especially obeying the mentioned standards.	There are no specific legal or ethical issues raised by the experiment.	
New industrial strategy for a green and digital Europe	Guidelines for innovation in Industrial environment	The new factsheet underlines the need for a guided introduction of new technologies in the industrial and productive ecosystem, underlining the need for education, re-skilling and training.	
QMS – Quality Management Systems ***ISO 9001***	ISO 9001 is a set of standards, a certified quality management systems (QMS) that help manufacturing companies ensuring they meet customer and other stakeholder needs within statutory and regulatory requirements related to certain product.	The company is certified ISO 9001:2015 and IATF 16949:2016 (former ISO/TS 16949).	

Table 41 Ethical and Legal Framework DF XIV

5.1.2.14.2. Ethical and Legal Requirements

Req#	EL Requirements	Description	Priority	Application Area	Nature	AI REDGIO 5.0 Technology Asset	Business Process	Business Objectives
01	**Data protection**	To comply with GDPR regulation. Some volunteers are expected to visit the Didactic Factory with the purpose of validating the execution of the experiment, in terms of serving as a valuable learning opportunity for gaining hands-on experience with AI&Edge	Critical	DF's services dissemination and validation	Legal	This EL requirement is linked to the fact that some visits are expected to the Didactic Factory facilities from manufacturing companies and students organizations by the end of the second experiment iteration, for trying out the	Provision and dissemination of a site for testing, showcasing and training on the use and potential of Edge&AI technologies in a realistic industrial environment.	To maximize reach to manufacturing companies in near environment. To maximize reach to students and learning organizations in near environment.

		technologies. The visit will only consist in showcasing the potential of these technologies in a realistic industrial manufacturing environment, in order to promote learning and adoption. Therefore, no personal data will be collected for the actual execution of the experiment (defect detection during a metal additive manufacturing process). The personal data that will be collected (not processed in any way) is the information that the volunteers provide in the Informed consent form. In addition, images and videos from the participation in the workshops and/or interviews might be collected and responses given in the questionnaires, interviews, workshop and focus group might be recorded. The best practices on the informed consent procedures compliant with				DF's technologies and learning about them.		

		GDPR will be followed and all the volunteers will be informed and given the opportunity to provide their consent.						
02	**AI system's Accountability**	Potential risks should be identified, declared and minimized. Based on: The Ethics Guideline for Trustworthy AI (2019)	Critical	AI system's design and operational area	Ethical	The implementation of the AI system that is being designed and developed for the Galicia Didactic Factory experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	Metal additive manufacturing process and quality monitoring, providing defect detection mechanisms during the production	Provision of real-time analysis of additive manufacturing process data through AI-at-the-Edge models, aiming at showcasing these technologies so companies and students can learn their use for their purposes
03	**Quality Management Systems**	ISO 9001 is a set of standards, a certified quality management system (QMS) that helps manufacturing companies ensure they meet customer and other stakeholder needs within statutory and regulatory requirements related to certain products. Based on: QMS – Quality Management Systems	Critical	AI system's operational area	Legal	The implementation of the AI system that is being designed and developed for the Galicia Didactic Factory experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical	Metal additive manufacturing process and quality monitoring, providing defect detection mechanisms during the production	Provision of real-time analysis of additive manufacturing process data through AI-at-the-Edge models, aiming at showcasing these technologies so companies and students can learn their use for their purposes

		ISO 9001:2015 and IATF 16949:2016 (former ISO/TS 16949)				WPs (WP4/WP5).		
04	**Safety of the machines and system**	Machine Directive and other machine safety-related standards will be considered so the safety of the humans working in the pilot line environment, including researchers, is ensured.	Critical	Physical production system	Legal and ethical	This EL requirement refers to the physical manufacturing cell linked to the operation of the AI system that is being implemented for the Galicia Didactic Factory experiment.	Provision and dissemination of a site for testing, showcasing and training on the use and potential of Edge&AI technologies in a realistic industrial environment.	To maximize reach to manufacturing companies in near environment. To maximize reach to students and learning organizations in near environment.
05	**Human agency and oversight**	AI systems can support the user in the decisional process, but proper oversight mechanisms should be implemented. Based on: The Ethics Guidelines for Trustworthy AI (2019) Nevertheless, no actions are expected to be automated based on the AI system's prescriptions in the scope of this experiment. The outputs of the AI system will only serve as valuable additional information for supporting the decision making of the human operators.	Critical	AI system's operational area	Ethical	The implementation of the AI system that is being designed and developed for the Galicia Didactic Factory experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	Metal additive manufacturing process and quality monitoring, providing defect detection mechanisms during the production	Provision of real-time analysis of additive manufacturing process data through AI-at-the-Edge models, aiming at showcasing these technologies so companies and students can learn their use for their purposes

06	**Technical robustness and safety**	A crucial component for achieving Trustworthy AI is technical robustness, which is closely linked to the principle of prevention of harm. Technical robustness requires that AI systems are developed with a preventative approach to risks and in a manner such that they reliably behave as intended, while minimising unintentional and unexpected harm and preventing unacceptable harm. This should also apply to potential changes in their operating environment or the presence of other agents (human and artificial) that may interact with the system in an adversarial manner. In addition, the physical and mental integrity of humans should be ensured. Based on The Ethics Guidelines for Trustworthy AI (2019)	Critical	AI system's design and implementation	Ethical	The implementation of the AI system that is being designed and developed for the Galicia Didactic Factory experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	Metal additive manufacturing process and quality monitoring, providing defect detection mechanisms during the production	Provision of real-time analysis of additive manufacturing process data through AI-at-the-Edge models, aiming at showcasing these technologies so companies and students can learn their use for their purposes
07	**AI system's transparency**	Clear information has to be provided	Critical	AI system's operational area	Ethical	The implementation of the AI	Metal additive manufacturing process and	Provision of real-time analysis of

		concerning the algorithm limitations, illustrating the reasoning and the data that led to the system prediction. Based on: The Ethics Guideline for Trustworthy AI (2019)				system that is being designed and developed for the Galicia Didactic Factory experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	quality monitoring, providing defect detection mechanisms during the production	additive manufacturing process data through AI-at-the-Edge models, aiming at showcasing these technologies so companies and students can learn their use for their purposes
08	**Risk assessment of the AI applications**	Before implementing the AI algorithms, a risk assessment must be performed in order to consider the possible implications that it could have on the installation from the security level. Based on: The Ethics Guideline for Trustworthy AI (2019) The machine room setpoints will not be automatically modified by AI algorithms. The AI algorithms will only provide recommendations to the human operators.	Critical	AI system's operational area	Ethical	The implementation of the AI system that is being designed and developed for the Galicia Didactic Factory experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	Metal additive manufacturing process and quality monitoring, providing defect detection mechanisms during the production	Provision of real-time analysis of additive manufacturing process data through AI-at-the-Edge models, aiming at showcasing these technologies so companies and students can learn their use for their purposes
09	**AI system's traceability**	The results of the algorithms must be tested regularly, ensuring that	Preferred	AI system's operational area	Ethical	The implementation of the AI system that is being designed	Metal additive manufacturing process and quality monitoring,	Provision of real-time analysis of additive manufacturing process data

		they fulfill the functions for which they were designed and that no variables appear over time that could cause anomalous operation. Based on: The Ethics Guideline for Trustworthy AI (2019) This will be achieved thanks to the nature of the AI algorithms implemented for this experiment, which are incremental/life-long learning models. Moreover, mechanisms will be provisioned to allow the tracking of the models' operation.				and developed for the Galicia Didactic Factory experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	providing defect detection mechanisms during the production	through AI-at-the-Edge models, aiming at showcasing these technologies so companies and students can learn their use for their purposes
10	**Auditability of AI system's results**	The system should establish mechanisms that facilitate the auditability of the AI models, providing traceability of the training process. The system must provide means to ensure that third parties can audit the AI system, for instance. Based on: The Ethics Guideline for Trustworthy AI (2019) Each of the datasets used for	Preferred	AI system's operational area	Ethical	The implementation of the AI system that is being designed and developed for the Galicia Didactic Factory experiment's use case is linked to this EL requirement. This implementation will integrate some of the AI REDGIO 5.0 tools that are currently being developed in the technical WPs (WP4/WP5).	Metal additive manufacturing process and quality monitoring, providing defect detection mechanisms during the production	Provision of real-time analysis of additive manufacturing process data through AI-at-the-Edge models, aiming at showcasing these technologies so companies and students can learn their use for their purposes

		training each of the versions of the model will be registered, together with the corresponding evaluation metrics of each version.						

Table 42 Ethical and Legal Requirements DF XIV

6. Conclusions and future outlook

This document investigates the main legal and ethical challenges relevant for AI REDGIO 5.0, such as the liability and safety issues, the data ownership and data sovereignty, the concerns related to the privacy and data protection, the risk of algorithmic biases, the psychological issues of human-machine interaction and the uncertainties related to the possible use of Generative AI solutions. It also provides, on the one hand, a comprehensive legal review, including both THE pieces of legislation relevant to AI REDGIO 5.0 breakthroughs and those specifically applicable to each of its SME-driven and DF experiments, and, on the other hand, the elicitation of the set of legal and ethical requirements and related guidelines, functional to ensure the legal compliance and ethical soundness of the AI REDGIO 5.0 technologies and validation activities. Their fulfillment is directed to ensure that they are respectful of the applicable regulatory framework, as well as value-driven and aligned with the highest ethical standards.

The future work of T7.1 « Legal, Regulatory and Ethical Issues» and T2.4 “Legal and ethical requirements for AI Collaborative Intelligence Scenarios” will encompass the update, refinement and enrichment of the requirements described in this deliverable, relying on the monitoring of the regulatory developments underway and on the project’s progress, as well as the elaboration of guidelines for the legally compliant, responsible and trustworthy adoption and use of AI REDGIO 5.0 solutions, taking into account the lessons learnt during the project’s lifetime and the running of its 21 experiments, especially its TEchnology and REgulatory SAnd boxes under T6.4 « TERESA Experiments in TEF Network», as well as the activities and findings of the Human Rights Impact Assessments (HRIAs), to be conducted in T2.4, the final release of the Ethics and Data Protection Impact Assessments, performed and potentially updated in T1.4 “Ethics Management”.

7. References

[1] AI REGIO D7.1 "AI REGIO Human-AI Interaction Framework – M12", AI REGIO D7.2 “AI REGIO Human-AI Interaction Framework – M24.

[2] A. Brintrupa, G. Baryannisb, A. Tiwaric, S. Ratchevd, G. Mart´ınez-Arellanod, J. Singhe, “Trustworthy, responsible, ethical AI in manufacturing and supply chains: synthesis and emerging research questions”, 2023.

[3] J. Newman, “A taxonomy of trustworthiness of Artificial Intelligence. Technical report”, 2023.

[4] European Commission, «COM (2020) 65 final “White Paper on Artificial Intelligence – A European Approach to Excellence and Trust,» 2020.

[5] European Commission, «COM(2020) 64 final. “Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics”,» 2020.

[6] European Parliament, «Resolution on a civil liability regime for artificial intelligence, (2020/2014 (INL),» 2020 and European Parliament, "Resolution on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/20.

[7] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)).

[8] Martina Barbero, Diana Cocoru, Hans Graux and other, “Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability. Study prepared for the European Commission DG Communications Networks, Content & Technolo.

[9] IDSA, «DIN SPEC 27070,» 2021.

[10] AI REGIO D5.1 “Collaborative Intelligence and Industry 5.0”, 2021.

[11] Gordon Briggs, Matthias Scheutz, “How Robots Can Affect Human Behavior: Investigating the Effects of Robotic Displays of Protest and Distress”, 2019.

[12] Yordanka Ivanova,”Generative AI and the AI Act”, 2023.

[13] European Commission, Living guidelines on the responsible use of Generative AI in research, 2024.

[14] European Commission, COM(2019) 250 final, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union.

[15] IDSA Rule Book, Version 1.0, November 2020 and the draft IDSA Rule Book, version 2.0, 2023 (retrieved at https://docs.internationaldataspaces.org/idsa-rulebook-v2/front-matter/frontmatter).

[16] AI REGIO D2.7 “Legal and Ethical Requirements and Guidelines v1” (2021) and D2.8 “Legal and Ethical Requirements and Guidelines v2” (2022).

[17] European Commission, "Ethics by Design and Ethics of Use Approaches for Artificial Intelligence”, 2021.

[18] AI Act, Regulation (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 201.

[19] AI Liability Directive (AILD) Proposal, COM (2022) 496 final “Proposal for a Directive of the European Parliament and of the Council on adapting non- contractual civil liability rules to artificial intelligence.