

D7.3

Ethics Recommendations and Regulatory Framework

June 2022

OPTIMAI



This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 958264

The material presented and views expressed here are the responsibility of the author(s) only.
The EU Commission takes no responsibility for any use made of the information set out.

DOCUMENT SUMMARY INFORMATION

Grant Agreement No	958264	Acronym	OPTIMAI
Full Title	Optimizing Manufacturing Processes through Artificial Intelligence and Virtualization		
Start Date	01/01/2021	Duration	36 months
Deliverable	D7.3 Ethics Recommendations and Regulatory Framework		
Work Package	WP7		
Deliverable type	R	Dissemination Level	PU
Lead Beneficiary	TRI		
Authors	Paul Hayes (TRI) Agata Gurzawska (TRI) Andrea Guillén (UAB) Emma Teodoro (UAB)		
Co-authors			
Reviewers	Louis de Koker (La Trobe University) (External Member of the Ethics Board) Lilian Mitrou (University of the Aegean) (External Member of the Ethics Board) Ugo Pagallo (University of Turin) (External Member of the Ethics Board) Marta Poblet Balcells (RMIT University) (External Member of the Ethics Board) Cinzia Rubattino (ENG) Dimos Ioannidis (CERTH) Stavroula Ntoa (FORTH) Linda Henriksson (CARR) Theofilos Mastos (KLEE)		

DISCLAIMER

The OPTIMAI Project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 958264. The sole responsibility for the content of this document lies with the authors. It does not necessarily reflect the opinion of the European Union. The European Commission is not responsible for any use that may be made of the information contained herein.

DOCUMENT HISTORY

Version	Date	Changes	Contributor(s)
V0.1	01/04/2022	Table of contents	TRI UAB
V0.2	26/04/2022	Section 1 added Section 2 added Section 4 added	Paul Hayes (TRI)
V0.3	27/04/2022	Section 5 added Section 7 added	Paul Hayes (TRI)
V0.4	12/05/2022	Section 6 added	Emma Teodoro (UAB) Andrea Guillén (UAB)
V.05	17/05/2022	Executive Summary drafted Conclusion drafted	Paul Hayes (TRI)
V.06	19/05/2022	Section 3 added Appendix A, B and C added	Emma Teodoro (UAB) Andrea Guillén (UAB) Paul Hayes (TRI)
V.07	24/05/2022	Conclusion updated Internal Review version finalised	Emma Teodoro (UAB) Andrea Guillén (UAB) Paul Hayes (TRI) Agata Gurzawska (TRI)
V.08	29/05/2022	All sections revised following review from CARR, KLEE, EB members	Agata Gurzawska (TRI) Emma Teodoro (UAB) Andrea Guillén (UAB) Pinelopi Troullinou (TRI)

PROJECT PARTNERS

Logo	Partner	Country	Short name
 CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	Greece	CERTH
 FINT Future Intelligence TELECOM ENGINEERING COMPANY	FINT FUTURE INTELLIGENCE LIMITED	Cyprus	FINT
 FORTH ΕΡΕΥΝΑ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΕΡΕΥΝΑ	IDRYMA TECHNOLOGIAS KAI EREVNAS	Greece	FORTH
 EVT	EVT EYE VISION TECHNOLOGY GMBH	Germany	EVT
 VISUAL COMPONENTS	VISUAL COMPONENTS OY	Finland	VIS
 YUBIQUO	YUBIQUO SRL	Italy	YBQ
 ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ χρόνια δημιουργίας	PANEPISTIMIO THESSALIAS	Greece	UTH
 ENGINEERING	ENGINEERING – INGEGNERIA INFORMATICA SPA	Italy	ENG
 innovalia METROLOGY INNOVATION AND ACCURACY	UNIMETRIK SA	Spain	UNIMET
 UNIVERSITAT POLITECNICA DE VALÈNCIA	UNIVERSITAT POLITECNICA DE VALENCIA	Spain	UPV
 CARR COMMUNICATIONS	Carr Communications Limited	Ireland	CARR
 UAB Universitat Autònoma de Barcelona	UNIVERSIDAD AUTONOMA DE BARCELONA	Spain	UAB
 TRILATERAL RESEARCH	TRILATERAL RESEARCH LIMITED	Ireland	TRI
 KLEEMANN	KLEEMANN HELLAS –INDUSTRIAL COMMERCIAL SOCIETE ANONYME FOR MECHANICAL CONSTRUCTION SA	GREECE	KLEE
 Televes	TELEVES SA	Spain	TVES
 MICROCHIP	MICROCHIP TECHNOLOGY CALDICOT LIMITED	United Kingdom	MTCL

LIST OF ABBREVIATIONS

Abbreviation	Definition
AEPD	Agencia Española de Protección de Datos
AI	Artificial Intelligence
ALLEA	European Federation of Academies of Sciences and Humanities
AR	Augmented Reality
DoA	Description of Action
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DT	Digital Twin
DX.X	Deliverable X.X
EB	Ethics Board
EC	European Commission
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ELS	Ethical, Legal, and Societal
ENISA	European Union Agency For Network and Information Security
ERA	Employment Rights Act
EU	European Union
FA	Factories Act
GDPR	General Data Protection Regulation
HDPa	Hellenic Data Protection Authority
HSWA	Health and Safety at Work etc. Act
ICO	Information Commissioner's Office
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of things
IP	Internet Protocol
ISO	International Standards Organisation
IT	Information Technology

LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
MAC	Media Access Control
OECD	Organisation for Economic Co-operation and Development
OS	Operating System
PPE	Personal Protective Equipment
QR	Quick Response
RRI	Responsible Research and Innovation
UK	United Kingdom
UPS	Uninterruptible Power Supply
WP	Work Package

Executive Summary

D7.3 Ethics Recommendations and Regulatory Framework provides the OPTIMAI Consortium with an informational resource to support pilot activities that respect the moral and legal rights of human research participants in the industrial/industry 4.0 employment context.

This deliverable builds upon previous deliverables dealing with ethics and legal issues including *D9.1 Report on the OPTIMAI Ethical and Legal Framework*, and *D9.2 Report on the OPTIMAI Ethical, Legal, and Societal Risks – 1st Version*. This deliverable builds upon and refines both ethics and legal requirements presented in those deliverables, utilising ethics and legal partners UAB and TRI's most up-to-date understanding of the tools to be deployed and the environments in which they will be deployed. Additional guidance on ethical procedures to be observed and executed in managing ethical human research participation is also provided, bearing in mind the relevant circumstances of the pilot sites.

In building upon and refining the work undertaken in previous deliverables, UAB and TRI have notably taken a country-specific approach to examining end-user and technical partners' legal obligations. A general section dealing with GDPR requirements notwithstanding, this deliverable provides a country-by-country breakdown of highlights of relevant national law in the United Kingdom, Spain, and Greece, where OPTIMAI pilot activities will take place. The particular areas of law detailed include data protection law, employment law, equality law, and health and safety law. A non-exhaustive list of legal requirements are presented to aid all partners, but particularly end-user partners, in making decisions in the design and implementation of OPTIMAI solution research activities in the industrial context that respect the rights of human research participants and comply with the laws of the countries where these activities will take place. Furthermore, the insights of the deliverable can be beneficial in similar contexts after the end of the project raising end-users' awareness regarding ethical and legal issues in future.

Table of Contents

Executive Summary	8
Table of Contents	9
1 Introduction	16
1.1 Background	16
1.2 Purpose and Scope	17
1.3 Intended Readership	17
1.4 Document Outline	18
1.5 Limits of this Deliverable	19
2 Methodology	20
2.2 Introduction	20
2.3 Desktop Research	20
2.4 Touchpoint Table™	22
2.5 Dialogue Sessions and Questionnaires	24
2.5.1 Work Undertaken in 2021	24
2.5.2 Work Undertaken in 2022	26
3 Ethical Procedures and Guidelines for Pilot Activities	28
3.1 Ethical Framework Applicable to OPTIMAI Piloting Activities	28
3.2 Ethical Requirements Identified for OPTIMAI Piloting Activities	30
3.3 Ethical Procedures: Monitoring Strategy	35
4 The General Data Protection Regulation and Basic Data Protection Recommendations for OPTIMAI Pilot Activities	39
4.1 Introduction	39
4.2 Data Processing and Personal Data	39
4.2.1 Data Protection Principles	41
4.2.2 Legal Bases for Data Processing and Conditions for Consent	42
4.2.3 Processing of Special Categories of Data	44
4.2.4 Controller and Processor	46
4.2.5 Rights of the Data Subject	47
4.2.6 Derogations for Research and Employment Purposes	53
4.2.7 Transfers of Personal Data to Third Countries or International Organisations	54
4.2.8 Technical Security Measures	55

4.3	Basic Data Protection (BDP) Requirements for OPTIMAI Pilot Activities.....	59
5	Regulatory Framework to Support Lawful Conduct of Pilot Activities in the United Kingdom	63
5.1	Introduction.....	63
5.2	Pilot description MTCL.....	63
5.3	Data Protection Law	64
5.3.1	Data Protection in the Employment Context and other ICO Guidance	65
5.3.2	Exemptions	67
5.4	Employment Law	70
5.4.1	Protected Disclosures	71
5.4.2	Health and Safety	71
5.4.3	Unfair Dismissals	72
5.5	Equality Law.....	72
5.5.1	Protected Characteristics.....	73
5.5.2	Discrimination, Harassment, and Victimisation in Relation to Employment.....	73
5.5.3	Adjustments for Persons with Disabilities.....	74
5.6	Health and Safety Law.....	75
5.6.1	General Duties of Employers as Specified in Health and Safety at Work etc. Act 1974	75
5.6.2	General Health and Safety Requirements with Regards to Working Environment and Equipment.....	76
5.6.3	General Provisions on Worker Welfare	78
5.6.4	Risk Assessment and Management Requirements	78
5.6.5	Employee Duties, Capabilities and Training.....	79
5.6.6	Duty of Consultation	80
5.7	UK Data protection, Employment and Equality, and Health and Safety Law Requirements.....	82
5.7.1	United Kingdom (UK) – Data Protection Law Requirements.....	82
5.7.2	UK – Employment Law Requirements	87
5.7.3	UK – Equality Law Requirements.....	88
5.7.4	UK – Health and Safety Law Requirements.....	88
6	Regulatory Framework to Support Lawful Conduct of Pilot Activities in Spain	94
6.1	Introduction.....	94
6.2	Pilot Descriptions TVES.....	94

6.3	Data protection in the Employment Context	96
6.3.1	AEPD Guidance on Data Protection in the Employment Context	96
6.4	Employment Law	100
6.4.1	Health and Safety	101
6.4.2	Unfair Dismissals	102
6.5	Equality Law.....	102
6.5.1	Adjustments for Persons with Disabilities.....	104
6.6	Health and Safety Law	105
6.6.1	General health and Safety Requirements with Regards to Equipment and Means of Protection	106
6.6.2	Risk Assessment and Management Requirements	107
6.6.3	Employee Duties, Capabilities, and Training	108
6.6.4	Duty of Consultation	108
6.7	Spain Data Protection, Employment and Equality, Health and Safety Law Requirements	109
6.7.1	Spain (SP) – Data Protection Requirements	109
6.7.2	Spain – Employment Law Requirements.....	115
6.7.3	Spain – Equality Law Requirements	116
6.7.4	Spain – Health and Safety Law Requirements	117
7	Regulatory Framework to Support Lawful Conduct of Pilot Activities in Greece.....	122
7.1	Introduction.....	122
7.2	Pilot Description KLEE.....	122
7.3	Data Protection Law	123
7.3.1	Processing of Special Categories of Personal Data	124
7.3.2	Processing of Personal Data in the Context of Employment.....	125
7.3.3	Processing and Freedom of Expression and Information; for Archiving Purposes in the Public Interest; and Scientific or Historical Research Purposes or for the Collection and Maintenance of Statistical Information	126
7.3.4	Rights to information, access, and erasure	126
7.4	Employment Law	128
7.5	Equality Law.....	129
7.5.1	Protected Characteristics	129
7.5.2	Discrimination and harassment prohibitions as understood by Law 4443/2016.....	129
7.5.3	Reasonable Accommodations	130

7.6	Health and Safety Law	130
7.6.1	The Roles of Safety Technician and Occupational Physician	131
7.6.2	Duties linked to Directive 89/391/EEC	133
7.7	Greece Data Protection, Employment and Equality, and Health and Safety Law Requirements.....	134
7.7.1	Greece (GR) – Data Protection Law Requirements	134
7.7.2	Greece – Employment Law Requirements	139
7.7.3	Greece – Equality Law Requirements	139
7.7.4	Greece – Health and Safety Law Requirements.....	140
8	Conclusion	144
9	References	145
10	Appendix A: OPTIMAI Pilot National Legal Framework	149
11	Appendix B: OPTIMAI Human Research Participant Information Sheet and Consent Form 151	
12	Appendix C: OPTIMAI Pilot Research Ethics Application for CERTH.....	155

LIST OF FIGURES

Figure 1: OPTIMAI Touchpoint Table.....	23
Figure 2: OPTIMAI Artificial Intelligence Risk Table.....	23

LIST OF TABLES

Table 1 Sources influencing ethics requirements.....	20
Table 2 Sources influencing initial legal requirements.....	21
Table 3 OPTIMAI Dialogue Sessions 2021	24
Table 4 OPTIMAI WP7 Information and Feedback Webinars.....	26
Table 5 AI: Ethical Requirements.....	31
Table 6 Digital Twins and Virtualisation: Ethical Requirements	32
Table 7 IoT & Sensors: Ethical Requirements.....	33
Table 8 Wearables & AR: Ethical Requirements.....	34
Table 9 Blockchain: Ethical Requirements.....	35
Table 10 Lawful Basis Requirements	59
Table 11 Special Categories of Data Requirements.....	59
Table 12 Data Controller and Processor Requirements.....	60
Table 13 Data Subject Rights Requirements	61
Table 14 International Data Transfer Requirements.....	62
Table 15 UK Lawful Basis Requirements	82
Table 16 UK Special Categories of Data Requirements.....	83
Table 17 UK Data Controller and Processor Requirements.....	84
Table 18 UK Data Subject Rights Requirements	85
Table 19 UK International Data Transfer Requirements.....	87
Table 20 UK Employment Law Requirements.....	87
Table 21 UK Equality Law Requirements.....	88
Table 22 General Duties of Employers Requirements	88
Table 23 UK Work Environment and Equipment Requirements	89
Table 24 UK Worker Welfare Requirements	90
Table 25 UK Risk Assessment and Management Requirements.....	91
Table 26 UK Employee Duties, Capabilities, and Training Requirements.....	92
Table 27 UK Employee Consultation Requirements.....	92
Table 28 Spain Lawful Basis Requirements.....	109
Table 29 Spain Data Subject Rights Requirements.....	110
Table 30 Spain Confidentiality and Security Requirements.....	111
Table 31 Spain Right to Privacy Requirements	112
Table 32 Spain Right to Digital Disconnection Requirements	112

Table 33 Spain Employee Monitoring Requirements	113
Table 34 Spain Use of Video Monitoring Systems Requirements	113
Table 35 Spain Use of Sound Recording Systems Requirements.....	114
Table 36 Spain Use of Geolocation Systems Requirements	114
Table 37 Spain Employment Law Requirements	115
Table 38 Spain Employees' Obligations Requirements	115
Table 39 Spain Equality Law Requirements	116
Table 40 Spain General Duties of Employers Requirements.....	117
Table 41 Spain Duties of Employers with Regards to Equipment and Means of Protection Requirements	118
Table 42 Spain Risk Assessment and Management Requirements	118
Table 43 Spain Employee Duties, Capabilities, and Training Requirements	119
Table 44 Spain Duty of Consultation Requirements.....	120
Table 45 Greece Lawful Basis Requirements	134
Table 46 Greece Special Categories of Data Requirements.....	135
Table 47 Greece Data Controller and Processor Requirements.....	136
Table 48 Greece Data Subject Rights Requirements	137
Table 49 Greece International Data Transfer Requirements.....	138
Table 50 Greece Employment Law Requirements.....	139
Table 51 Greece Equality Law Requirements.....	139
Table 52 Greece Safety Technician and Occupational Physician Requirements.....	140
Table 53 Greece Risk Assessment and Management Requirements.....	141
Table 54 Greece Employee Duties, Capabilities, and Training Requirements.....	142
Table 55 Greece Other Duties Requirements	142
Table 56 OPTIMAI Pilot National Legal Framework	149

1 Introduction

1.1 Background

The OPTIMAI project is undertaken by 16 partners from academia and industry from across eight different countries. The project seeks to build on the promises of Industry 4.0 by advancing the state-of-the-art in smart technologies and innovating industrial manufacturing processes through a secure and interconnected framework of multisensorial technology, blockchain, defect detection and prediction, and machine reconfiguration support through artificial intelligence (AI) solutions, digital twins (DT) and virtualization, and wearables and augmented reality (AR).

More specifically, it is the objective of the OPTIMAI project to:

- develop a secure and adaptive multi-sensorial network and fog computing framework for continuous production monitoring and quality inspection
- create a blockchain-enabled ecosystem for securing data exchange and ensuring in real-time the validity and traceability of the collected data and communication transactions
- develop AI methodologies for defect detection and prediction, integrated in a decision support framework for zero-defect manufacturing
- virtualize manufacturing processes via digital twins of sensors and production equipment allowing the rapid line qualification and exploration of alternative production scenarios
- enable the on-the-fly reconfiguration of production equipment based on quality control feedback and operator's interaction in an AR environment.

The cutting edge innovation work undertaken by researchers in Work Packages (WP) 2-7 takes place within the context of a comprehensive ethical and legal framework (WP9 and WP7), encouraging responsible research and innovation and supporting “value sensitive design” [1], “by-design” and “through-design” [2] efforts to promote the development of technical tools that respect moral and societal values, fundamental and human rights, and international legal norms.

Starting in 2022, pilot studies will take place in the manufacturing sites of the three OPTIMAI end-user partners, Kleemann (KLEE), Televés (TVES), and Microchip Technology Caldicot Ltd (MTCL). Three use cases will be tested in each pilot site, each one deploying a number of OPTIMAI software and hardware solutions including AI tools, augmented reality (AR) and wearables, digital twins, blockchain, and sensor devices. The use cases include zero defect quality inspection, production line setup-calibration, and production planning. These pilot studies represent a crucial aspect of OPTIMAI's empirical work and are undertaken to concretely demonstrate how manufacturing processes can be optimized through OPTIMAI's novel ecosystem of data driven hardware and software tools [3]. In what follows, and as will be outlined, we focus our efforts on providing an updated set of ethics recommendations and an outline of the legal framework that end-users and contributing partners need to be aware of and

take necessary action on in order to support their compliance with ethical principles and international and national law.

1.2 Purpose and Scope

With pilot site use case scenarios having begun and with the involvement of human research participants, as represented by pilot site employees, beginning in earnest imminently, this deliverable sets out to achieve two objectives, namely:

1. to build on work previously undertaken in deliverables *9.1 Report on the OPTIMAI Ethical and Legal Framework* and *9.2 Report on OPTIMAI ethical, legal and societal risks – 1st Version*, by providing and refining, where applicable, previously presented ethics requirements and procedures and ensuring their applicability and specificity to pilot site activities, and;
2. to provide an overview of the national legal frameworks relevant to the carrying out of pilot site activities in the United Kingdom (UK), Spain, and Greece, as well as develop legal requirements cognisant of the particularities of these cases.

As human participants have significant involvement in pilot activities by utilising new tools and being present in environments with significant data capturing capabilities and new physical features, it is of urgent and intrinsic importance to set about investigating how their rights can satisfactorily be upheld, both in terms of their moral rights to be treated with dignity and have their agency respected, and their nationally and internationally enshrined legal rights including data protection rights, employment rights, equality rights, and rights pertaining to health and safety protection in the workplace.

Based on previously undertaken work (such as requirements identified in D2.2), further research and consultation into the circumstances of pilot activities, and research concerning national legal frameworks, this deliverable presents—on the basis of the aforementioned objectives—guidance and requirements that point to key areas that responsible partners will need to be aware of and action as appropriate in their efforts to comply with the law and respect the rights and welfare of their employees and potentially pilot site visitors who may be exposed to the same conditions and environments as those employees.

Fundamentally, the guidance provided in this document is intended to help end-user partners and other contributing partners take further measures to ensure that pilot activities are carried out in an ethical and lawful manner, and further mainstream mitigation and monitoring efforts into their research design and implementation.

1.3 Intended Readership

The primary intended readership of this deliverable is end-user partners, MTCL, KLEE and TVES, as they operate the pilot sites and have the ultimate responsibility for ensuring the ethical and lawful conduct of research activities on their premises and ensuring that no harm or disadvantage comes to their employees, particularly as a result of their involvement in OPTIMAI research and pilot activities. Nevertheless, technical partners have a role to play in ensuring ethical and legal outcomes as they are responsible for designing and developing the tools that

will be deployed in the pilot sites as well as processing different types of research data. To that end, it is also firmly recommended that technical partners read and respond to, in their work, the requirements and guidance provided here, which applies to them insofar as they supply equipment which should be safe and accessible, and that they are data controllers or are responsible for provision of tools utilised by data controllers that should in any case support General Data Protection Regulation (GDPR) compliance.

A tertiary intended audience of this deliverable is members of other EU projects with similar goals, circumstances and within the same relevant geographical boundaries (the United Kingdom, Spain, and Greece). The work presented here may represent a useful point of reference and guidance for future industrial demonstrations and pilot activities of a similar nature.

1.4 Document Outline

This document is structured as follows. **Section 2 Methodology** presents the methodology of this deliverable, including details on the desktop research and legal analysis as well as end-user engagement and feedback. This section will also take the opportunity to present methods utilised in *D9.2* that informed results in **Section 3 Ethical Procedures and Guidelines for Pilot Activities**.

Section 3 Ethical Procedures and Guidelines for Pilot Activities provides details on the ethics work undertaken in support of pilot activities that comply with ethical principles and respect the dignity and autonomy of pilot site workers, including details on procedures undertaken and to be undertaken in support of ethics approvals, monitoring, and compliance. Section 3 will also present ethics requirements as detailed in *D9.2*, updated based on new information and for an appropriate fit here in order to avoid any duplication with new legal requirements.

Section 4 The General Data Protection Regulation and Basic Data Protection Recommendations for OPTIMAI Pilot Activities provides an overview of provisions of the GDPR which will be relevant to all end-user partners and data controllers, including data controller duties and data subject rights. Baseline data protection requirements are presented on the basis of this overview.

Section 5 Regulatory Framework to Support Lawful Conduct of Pilot Activities in the United Kingdom provides an overview of the legal framework for pilot site activities for MTCL and contributing partners in the UK, including of specific national data protection considerations, employment law, equality law, and health and safety law. Non-exhaustive legal requirements are then presented on the basis of this.

Section 6 Regulatory Framework to Support Lawful Conduct of Pilot Activities in Spain provides an overview of the legal framework for pilot site activities for KLEE and contributing partners in Greece, including of specific national data protection considerations, employment law, equality law, and health and safety law. Non-exhaustive legal requirements are then presented on the basis of this.

Section 7 Regulatory Framework to Support Lawful Conduct of Pilot Activities in Greece

provides an overview of the legal framework for pilot site activities for TVES and contributing partners in Spain, including of specific national data protection considerations, employment law, equality law, and health and safety law. Non-exhaustive legal requirements are then presented on the basis of this.

Section 8 Conclusion concludes this deliverable.

1.5 Limits of this Deliverable

The requirements outlined in law and regulation are of a very specific character and relate to matters of extreme importance for the health and safety of end-user employees or site visitors, and other legal obligations. This deliverable provides useful guidance and indicative, but not exhaustive, ethics recommendations and legal requirements to help support responsible decision-making and action. Laying out all possible requirements arising from international and national law and regulation, in full detail, is beyond the scope of this deliverable which largely serves informational purposes.

The substantial work on this deliverable was undertaken by researchers from diverse academic and professional backgrounds with varying expertise located across different European countries. No independent national experts in specific areas of national legal practice (including employment law, data protection law, equality law, and health and safety law) contributed directly to respective sections of this deliverable.

OPTIMAI Partners are responsible for ensuring their compliance with the law. The purpose of the following is to help highlight useful areas of action, and therefore this deliverable should not be considered a checklist or a policy document guaranteeing full legal compliance.

2 Methodology

2.2 Introduction

This section will detail the methods used to collect and analyse research data in our efforts to identify appropriate ethics and legal recommendations for OPTIMAI pilot activities. The methods used were qualitative, including desktop research methods with a particular focus on identifying and reviewing relevant legislation and supporting documentation in terms of legal opinions, guidance and summaries.

This deliverable and work leading to it do not exist in a vacuum of other efforts. Qualitative research methods utilized over the course of WP9 tasks, including those resulting in *D9.2*, *D9.5* and *D9.6*, were undertaken with a view to informing end-user ethics and legal requirements that were directly called for by this deliverable. With this being the case, and as the dissemination level of this is Public and not Confidential (thereby meaning a new audience without access to previous deliverables can access this one), these methods—including the Touchpoint Table™ and dialogue sessions—will be revisited to properly contextualise this work, especially as presented in **Section 3 Ethical Procedures and Guidelines for Pilot Activities** here. The OPTIMAI Consortium member reader then is warned of duplication in this section, however the new external reader will find this information useful in understanding how our ethical requirements were devised.

2.3 Desktop Research

Desktop research was undertaken in order to identify and review relevant literature, and national legislation and legal opinions, guidance and summaries of legislation that would be necessary to adhere to for the ethical and lawful conduct of OPTIMAI pilot activities in three distinct countries.

Much of the ethics research leading to this deliverable, in terms of data collection, analysis and literature review was undertaken in 2021 for the purposes of *D9.1* and *D9.2*. Internet searches (open access resources) were utilised to acquire advanced and extensive information on the state-of-the-art of ethics and novel technologies, including AI, in the general and industrial context. Information was acquired from internet searches, and the sources identified that were translated into *D9.1* requirements—which subsequently influenced those found in *D9.2*—and which were updated here in **Section 3 Ethical Procedures and Guidelines for Pilot Activities**, include those listed in Error! Reference source not found..

Table 1 Sources influencing ethics requirements

ETHICS	
ALLEA, The European Code of Conduct for Research Integrity	European Commission, EU Ethical Responsible Research and Innovation Framework
European Commission, Ethics and Data Protection, 2018	High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI

European Commission, Ethics for Researchers, 2013	High-Level Expert Group on Artificial Intelligence, Assessment List for Trustworthy AI
European Commission, Horizon 2020 Programme: Guidance How to Complete your Ethics Self-Assessment, 2019	IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, "Ethically Aligned Design"
Asilomar AI Principles	OECD AI Principles

Initial legal research with a primary focus on international law was also undertaken in 2021 with a view to translating these into legal requirements for all partners, at the time, without specific regard for the countries in which the research activities were taking place. The sources identified and consulted through internet searches are tabulated in Error! Reference source not found..

Table 2 Sources influencing initial legal requirements

HARD LAW	
INTERNATIONAL LEGAL INSTRUMENTS	
Universal Declaration on Human Rights	Convention on the Rights of Persons with Disabilities
International Covenant on Civil and Political Rights	European Convention on Human Rights
International Covenant on Economic, Social and Cultural Rights	Freedom of Association and Protection of the Right to Organise Convention, 1948 (No. 87)
International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families	Right to Organise and Collective Bargaining Convention, 1949 (No. 98)
International Convention on the Elimination of All Forms of Racial Discrimination	Discrimination (Employment and Occupation) Convention, 1958 (No. 111)
Convention on the Elimination of All Forms of Discrimination against Women	Employment Policy Convention, 1964 (No. 122)
EU LAW	
Treaty of the European Union	<u>Directives:</u>
Treaty on the Functioning of the European Union	Directive 89/391/EEC (<i>Framework Directive</i>)
Charter of Fundamental Rights of the European Union	Directive 89/654/EEC (<i>Workplace requirements</i>)
<u>Regulations:</u>	Directive 89/656/EEC (<i>Personal Protective Equipment</i>)
Regulation (EU) 2016/679 (<i>General Data Protection Regulation</i>)	Directive 2009/104/EC (<i>Work equipment</i>)
Regulation (EU) 2018/1807 (<i>Framework for the free flow of non-personal data</i>)	Directive 2014/95/EU (<i>Non-Financial Reporting Directive</i>)
	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (<i>NIS Directive</i>)

In order to provide end-user and technical partners with more advanced insight into national legal requirements, with the knowledge that a completely generic one-size-fits-all legal framework for differing circumstances across geographically and culturally distinct countries

would not be appropriate, we set about identifying core national legal texts for review and analysis.

Key areas of law relevant to our partners' needs were identified as data protection law, employment law, equality law, and health and safety law. These areas of law directly regulate interactions between employers and their employees, outlining their respective rights and duties, and knowledge of them is necessary to ensure pilot activities involving human research participants in the employment context respect the rights of those employees.

Internet searches were used to identify the relevant legislation under each of these categories in each pilot country. Similarly, national guidance documents, reports, and summaries were identified to supplement the legal analysis (and can be found in the **References** section).

The sources of law informing our analysis and national legal requirements are listed in Error! Reference source not found. Table in [Appendix A](#).

2.4 Touchpoint Table™

The Touchpoint risk assessment table™ is a tool designed by Trilateral Research with the purpose of simplifying the process of the ethical, legal and societal risk and impact assessment in research projects [4]. The Touchpoint "...provides a systematic, structured, comprehensive approach to the identification, assessment and disposition of risks or impacts that might arise during or because of a project" [4].

In its most basic form the Touchpoint table is essentially a spreadsheet consisting of four columns. The first column is often used to list the individual task or task description which can, for instance, be linked to the task descriptions in a project description of action (this deliverable itself falls under Task 7.2: Ethics Recommendations and Regulatory Framework). The second column is used to enumerate the various ethical, legal and societal risks identified. The third column enumerates methods agreed with task leaders for addressing the identified issues. Finally, the fourth column lists the comments of the external advisory board in relation to the risks and the agreed mitigation methods.

The Touchpoint table is not monolithic and is highly adaptable to the needs of a project and can be tailored for more depth or efficiency. Below, **Figure 1** is a screenshot which depicts the configuration of the Touchpoint table utilised for the OPTIMAI project. Here, we use six columns. The first column contains the technology clusters which grouped together complimentary OPTIMAI tasks and tools. The second column lists the ethical, legal, and societal risks. In this case, the third column links these risks to particular requirements decided in *D9.1*. The fourth column links these risks to specific societal standards, in our case for the purposes of OPTIMAI, the Sustainable Development Goals. The fifth column is for assessment of the likelihood and severity of the identified risks. The sixth column lists to methods identified for mitigating the probability and/or severity of the risks.

The OPTIMAI Touchpoint table's primary file-type is an excel spreadsheet, containing multiple sheets documenting both internal and external project risks.

The column recording ethics board feedback was omitted in this case, as instead this was sought upon completion of the risk tables (discussed below) by partners and presented directly in D9.2.

Trilateral TouchPoint Table™					
Technology	Ethical, Legal, Societal Risks	Applicable D9.1 Requirements	Relevant SDG	Assessment of Risk: Low: Minimal likelihood that the risk will materialise. Medium: Some likelihood that the risk will materialise. Appropriate actions (counter-measures) should dispense with the risk. High: The likelihood of the risk materialising is high, but the risk can be avoided or minimised or shared with appropriate countermeasures	Mitigation Measures

Figure 1: OPTIMAI Touchpoint Table

From the earliest phase of the project the Touchpoint table was populated with potential risks based on reviewing relevant literature and the project's Description of Action (DoA).¹ These risks informed the questions presented to partners during dialogue sessions held in 2021 (see **Subsection 2.4.1 Work Undertaken in 2021**) and were put to partners in the form of risk tables.

The Touchpoint table contains five categories or clusters of technologies (AI, digital twins & virtualization, internet of things (IoT) & sensorial network, wearables & AR, and blockchain).

When organising dialogue sessions with partners, these sessions were split along these clusters. In order to present partners with our findings, the Touchpoint table was divided into smaller risk tables tailored to the dialogue session. **Figure 2** below is a screenshot which depicts the columns of the AI risk table. These tables were distributed to relevant task leaders following explanation, and partners were invited to self-assess the likelihood and severity of pre-identified risks (both internal and external), and, following discussions held during the dialogue session, use their expert knowledge to identify additional risks that may have been overlooked by the legal and ethics team. Most importantly, this was used as a method for the direct collection of ideas on mitigating the ethical, legal and societal risks from partners.

Artificial Intelligence							
	Ethical/Legal/Societal Risk	Likelihood Internal	Severity Internal	Likelihood External	Severity External	Mitigation Measures	Notes

Figure 2: OPTIMAI Artificial Intelligence Risk Table

¹ An extensive enumeration of potential ethical and legal issues and relevant sources of norms drawn from literature review is presented in both D9.1 and D2.3.

Ultimately, the Touchpoint table informed the direction of dialogue sessions and presented partners with issues to consider and motivate them to think further on ethical, legal and societal issues. Partners' feedback was collected in the form of the risk tables, the results of which will be collated in future iterations of the Touchpoint in order to support monitoring of ethical, legal, and societal issues and how the project seeks to deal with them or has dealt with them.

2.5 Dialogue Sessions and Questionnaires

2.5.1 Work Undertaken in 2021

In order to elicit relevant information about the spectrum of OPTIMAI artefacts, methodologies and their contextual applications (or indeed, in order to understand the OPTIMAI socio-technical system), dialogue sessions were arranged with project partners. The sessions were held between October 27th and November 12th 2021, and were conducted virtually via Zoom. There were six sessions in total, based largely on the cluster topics (and in the order) of artificial intelligence, internet of things and sensors, wearables and augmented reality, digital twins and virtualization, blockchain, and culminating into an open session with end-users.

The composition of the dialogue sessions was agreed with the coordinator, CERTH, who indicated the most essential partner organisations to engage based on each technology. The date, time, and composition of each session is presented in Error! Reference source not found. below. Note that both ethics and legal partners, TRI and UAB, led and attended each dialogue session.

Table 3 OPTIMAI Dialogue Sessions 2021

OPTIMAI WP9 Dialogue Sessions 2021			
Session Topic	Date and Time	Participating Partner	Note
Artificial Intelligence	October 27th, 13:00-15:00 CET	UTH, CERTH, FORTH, ENG, UNIMET, FINT	
Internet of Things & Sensorial Network	October 29th, 11:00-13:00 CET	EVT, UNIMET, UPV, CERTH	FINT were invited but unable to attend. Follow up was conducted via email exchange
Wearables & Augmented Reality	November 2nd, 14:00-16:00 CET	YBQ, FORTH, CERTH	
Digital Twins & Virtualization	November 5th, 09:00-11:00 CET	ENG, VIS, FINT	
Blockchain	November 11th, 11:00-13:00 CET	CERTH, FINT	ENG were invited but unable to attend. Follow up was conducted via email exchange

End-Users	November 12th, 11:00-13:00 CET	MTCL, KLEE, TVES	This session was open to all partners and was additionally attended by FINT, CARR, ENG, YBQ
-----------	-----------------------------------	------------------	---

The clusters and their composition were chosen on the basis of the level of interdependence or distinctiveness of the tools and methods entailed and the interconnectivity of related WP tasks. This is a qualitative study, and as partners were chosen selectively based on their involvement in the project, sampling was purposive [5]**Error! Reference source not found..** At least one representative of required partner organisations made it to dialogue sessions where possible. The dialogue sessions represent a hybrid variation of the focus group and semi-structured interview. A semi-structured approach was chosen in order to control the pace of the interview and seek clarifications, and ask unplanned questions based on new or unexpected information arising. The group-based approach was added to this in order to help socialise each partner with the ethical, legal and societal (ELS) intricacies and in order to generate information from multiple perspectives on similar, and related issues, in a manner that enabled rapid cross-consultation.

We took precautions to ensure information was encoded clearly and understandably in order to be accurately decoded by our partners, and in a manner that would support them in accurately encoding their own answers [6]. Partners were clearly informed of the goals and purposes of our research activities in relation to ethics and legal research and monitoring at several junctures. Partners were extensively briefed on expected dialogue sessions during an introductory webinar in the first half of 2021, and an ethics and legal webinar organised in October, and were familiarised with their goals and purpose, and the kinds of information that would be sought. Partners were further briefed on the sessions via email in the weeks ahead of the sessions and were finally briefed once again at the beginning of each dialogue session. Following good interview and qualitative research practice [6], questions were designed to be clear and understandable to our partners using language appropriate to their expertise, efforts were made to avoid leading or double-questions, and questions were categorised by topic in order to ensure partners always knew the context under which answers were being sought.

Zoom calls were recorded with the consent of participants and notes were taken during the dialogue session. These notes were distributed to partners after the sessions so that they had the opportunity to provide additional information or clarify any misunderstandings.

The purpose of the dialogue sessions was firstly for the ethics and legal team to gain an understanding of the features of the technology under development and partners' contributions to their development. Secondly, the dialogue sessions were held in order to conduct live risk assessments in a dynamic way that supported multi-lateral communication. Thirdly, and as mentioned above, the dialogue sessions were held in an effort to support partners' sensitisation to ELS issues in their research and to elicit initial risk mitigation measures. This approach is in line with the OPTIMAI approach to responsible research and innovation (RRI) through continuous involvement of partners in the process the ethical, legal and societal risk and impact assessment to indirectly cultivate ethical and legal compliance attitude.

The precise structure of the dialogue sessions followed the following format:

1. An introduction to the goals and purposes of the session as well as an invitation for partners to provide details on their contributions to the research and development of the cluster's technology and any pertinent application examples
2. Questions and discussion related to **privacy and data protection**
3. Questions and discussion related to **equality, fairness and non-discrimination**
4. Questions and discussion related to **human agency and oversight, accountability, transparency and accuracy**
5. Questions and discussion related to **meaningful work and impact on work and skills**
6. Questions and discussion related to **security, health and safety**
7. Questions and discussion related to the **environment and the wider society**
8. An introduction to the risk assessment tables and how partners could coordinate to complete them

2.5.2 Work Undertaken in 2022

From mid-April 2022, OPTIMAI ethics and legal partners TRI and UAB began organising discrete webinars for OPTIMAI's three end-user partners. These sessions were classified as "information and feedback session" webinars. The purpose of these sessions was to provide end-user partners with updated requirements supporting the ethical and lawful conduct of research and pilot activities. The webinars were held in an interactive and semi-structured format, allowing dialogue between ethics and legal experts and end-users. The webinars were held remotely on Microsoft Teams. Only end-users were invited due to their being primary duty holders of ensuring responsible and lawful research on their pilot site premises, and due to their expert knowledge of the particularities of how research will be executed at the pilot sites.

End-user partners were fully informed by email of the purpose of the webinars ahead of scheduling and were provided with draft sections of this deliverable that corresponds to their pilot site. This allowed them to preview the work and consider any weaknesses or oversights that they could provide feedback on during the session itself.

End-users were presented with the updated requirements applicable to their pilot sites without planned follow-up questions, although the floor was opened formally for end-user questions at the end of each webinar, and end-users were invited to ask questions or for clarifications throughout the presentation. End-users provided feedback which was noted by the leading ethics and legal expert(s). The webinars for the UK and Greek pilots were led by TRI, whereas UAB led the Spanish webinar with TVES.

The schedule for these webinars is presented in Error! Reference source not found. below.

Table 4 OPTIMAI WP7 Information and Feedback Webinars

OPTIMAI WP7 Information and Feedback Webinars Q2 2022		
Topic	Date and Time	Participating Partner

D7.3 Webinar United Kingdom Requirements	May 3rd, 16:00-17:30 CET	MTCL - TRI
D7.3 Webinar Greece Requirements	May 4th, 14:30-16:00 CET	KLEE - TRI
D7.3 Webinar Spain Requirements	May 13th 12:00-13:30	TVES - UAB

Furthermore, OPTIMAI partner ENG circulated a survey to OPTIMAI partners requesting information about the OPTIMAI Use Cases, including the objectives, algorithms and tools to be implemented over the course of the pilot activities at end-users' pilot sites. The ethics and legal team utilised this updated information to help inform the content of this deliverable and its ethics and legal requirements.

3 Ethical Procedures and Guidelines for Pilot Activities

3.1 Ethical Framework Applicable to OPTIMAI Piloting Activities

OPTIMAI pilot activities are subject to be conducted in strict compliance with the ethics research framework identified as applicable for the OPTIMAI Project in *D9.1 Report on the OPTIMAI ethical and legal framework* (See **Section 2 Methodology**). It comprises the highest ethical standards, principles, and good practices of research ethics laid down in: i) the European Code of Conduct for Research Integrity;² ii) the EU Ethical Responsible Research and Innovation Framework (RRI);³ iii) Responsible Research Innovation in Industry; and iv) Ethical principles and guidelines for trustworthy Artificial Intelligence (AI).⁴

Accordingly, OPTIMAI piloting activities have been designed and will be conducted with respect to the general principle of integrity complemented by the ethical principles of reliability, honesty, respect, and accountability. In practical terms, the adherence to the applicable set of ethical principles of research integrity entails the implementation of the following actions in terms of designing and conducting OPTIMAI pilot activities:

- to address the potential ethical risks that OPTIMAI piloting activities may raise, by implementing adequate measures to minimise such risks and harmful results or consequences
- to ensure the quality of their design, methodology, analysis of results, and the use of resources
- to develop, undertake, review, report and communicate the piloting activities in a transparent, fair, full and unbiased manner
- to respect pilot site employees (research participants) and research colleagues
- to be accountable for publication, management, organisation, training activities, and supervision of such activities.

Pursuant to the RRI Framework, the following principles must be observed when conducting the piloting activities: diversity and inclusion; anticipation and reflection; openness and transparency; and responsiveness and adaptative change. The purpose of the piloting activities is two-fold: i) to anticipate and assess how OPTIMAI solutions may impact on society and the environment; and, ii) to ensure that such technological solutions respond to and align with individual and societal values, needs and expectations. To this end, OPTIMAI piloting activities have been designed and will be conducted as follows:

² <https://allea.org/code-of-conduct/>

³ <https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-researchinnovation>
<https://rri-tools.eu/en/about-rri>

⁴ <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai>

- being sensitive to research biases, avoiding discrimination and stigmatisation and striving for representativeness and diversity
- assessing their purpose, benefits, risks, outcomes, potential unintended consequences, and impacts on piloting site employees participating in such activities in order to address them
- being open to society in a meaningful and honest way
- adapting the piloting activities to changing societal values, needs and expectations, emerging knowledge and new insights particularly with regards to work environments and meaningful work

Ethical principles governing Responsible Research Innovation in Industry cover human rights, corporate and social responsibility, labour practices, conditions at work and social protection, health and safety at work, human development and training in the workplace, societal dialogue, community involvement and development, fair operating practices and environment. Thus, OPTIMAI piloting activities have been designed and will be conducted operationalising such ethical principles as follows:

- observing due diligence, respect for human rights, discrimination of vulnerable groups (e.g., workers with disabilities), and rights at work
- integrating societal and environmental concerns in companies' business operations
- implementing social, health and safety conditions at work, human development and training in the workplace
- encouraging employment creation and skills developments of workers, technology development and access
- promoting social responsibility to ensure that the technology developed and deployed within the industry context is responsible, sustainable, socially desirable and ethically acceptable
- when possible, considering sustainable resource use, climate change mitigation, and protection of the environment (e.g. prevent pollution, reduce emissions of pollutants into the air, water and soil as much as possible; use sustainable, renewable resources whenever possible; practice life-cycle approach to reduce waste, reuse products or components and re-cycle materials, among others).

Lastly, OPTIMAI pilot activities have been technically designed and will be carried out in strict compliance with the principles of trustworthy and ethical AI identified as applicable to OPTIMAI following primarily those found in the Artificial Intelligence High-Level Expert Working Group's *Ethics Guidelines for Trustworthy AI* [7]. These AI ethical principles are: Human autonomy, prevention of harms, fairness and explicability. These AI ethical principles are turned into the following requirements: Human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination, and fairness, environmental and societal well-being, accountability, awareness of misuse, and competence. Actioning AI ethical principles in the context of the OPTIMAI piloting activities require:

- OPTIMAI solutions should support human autonomy and decision-making, as prescribed by the principle of respect for human autonomy. This requires that OPTIMAI solutions should act as enablers to a democratic, flourishing and equitable society by supporting the user's agency, fostering fundamental rights, and allowing for human oversight, [7]
- technical robustness requires that OPTIMAI solutions be developed with a preventative approach to risks and in a manner such that these solutions 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 [7]
- the right to privacy requires adequate data governance that covers the quality and integrity of the data used, its relevance in light of the domain in which the OPTIMAI solutions will be deployed, its access protocols and the capability to process data in a manner that protects privacy [7]
- transparency is closely linked with the principle of explicability and encompasses transparency of elements relevant to the OPTIMAI solutions: the data, the systems, and the business models [7]
- in order to achieve Trustworthy AI, we must enable inclusion and diversity throughout the entire AI system's life cycle. Besides the consideration and involvement of all affected stakeholders throughout the process, this also entails ensuring equal access through inclusive design processes as well as equal treatment. This requirement is closely linked with the principle of fairness [7]
- the broader society and the environment should be also considered as stakeholders throughout the solutions' life cycle. Sustainability and ecological responsibility of OPTIMAI solutions should be encouraged, and research should be fostered into AI solutions addressing areas of global concern, such as, for instance the Sustainable Development Goals (SDGs). Ideally, OPTIMAI solutions should be used to benefit all human beings, including future generations [7]
- the requirement of accountability complements the above requirements and is closely linked to the principle of fairness. It necessitates that mechanisms be put in place to ensure responsibility and accountability for OPTIMAI solutions and their outcomes, both before and after their development, deployment and use [7]
- technical developers shall guard against reasonably foreseeable misuses and risks of the OPTIMAI solutions (e.g., hacking, misuse of personal data, system manipulation, or exploitation of vulnerable users) [7]
- technical developers shall specify and operators shall adhere to the knowledge and skill required for safe and effective operation [7].

3.2 Ethical Requirements Identified for OPTIMAI Piloting Activities

General ethical and legal requirements applicable to all OPTIMAI research activities have been provided in *D9.1, D2.1 (User and ethics and legal requirements - 1st version)* and *D2.2 (User and ethics and legal requirements - 2nd version)*.

A set of initial legal and ethical requirements for pilot sites was identified in *D9.2*. The following tables present these requirements, which must be observed before the start of the piloting activities. These requirements focus on the technologies used to develop the OPTIMAI solutions. Each requirement has been coded considering: (i) the activity in which these requirements must be observed, in this case the piloting activities (PA); and, (ii) the technology, i.e. Artificial Intelligence (AI), Digital Twins & Virtualisation (DT), IoT & Sensors (IoT), Wearables & AR (AR), Blockchain (B); and, iii) the number of the requirement (R1, R2, R3,...).

Table 5 AI: Ethical Requirements

Artificial Intelligence
Privacy and Data Protection
PAi-AI-R1: Personal data collected for training and testing algorithms should be limited to a strict minimum.
PAi-AI-R2: Before starting the pilot activities, human operators and persons at risk of data capture must be notified about: the pilot activities; the types of data being collected on site, who the data controller is, the purpose of data collection and their right to withdraw if applicable.
PAi-AI-R3: All personal data should be anonymised or pseudonymised, stored securely and transmitted and made accessible only to those researchers who are authorised to access the data for achieving the OPTIMAI objectives.
Equality, Fairness, and Non-Discrimination
PAi-AI-R4: Where applicable, operators participating in training OPTIMAI AI tools should be diverse and inclusive of different genders, ethnicities, body types and disabilities.
PAi-AI-R5: The recording of machine and equipment data should be prioritised over human movements and human activity.
PAi-AI-R6: Synthetic data that is representative should be utilised where it is reasonable to do so.
PAi-AI-R7: Controlled laboratory conditions should be established to generate data compensating for lack of diversity or certain disabilities.
Human Agency and Oversight, Accountability, Transparency and Accuracy
PAi-AI-R8: Wearable AR glasses should display a notification to the operator to inform them that they are interacting with AI tools.
PAi-AI-R9: To maintain satisfactory human control over autonomous processes guided by AI, human operators should be able to initiate or terminate these processes themselves through gesture recognition or other means.
PAi-AI-R10: Human operators must be trained in the correct use of the AI, as well as informed of its capabilities and limitations.
PAi-AI-R11: Training and training materials should provide operators with at least a high-level explanation about how AI tools come to a decision.
PAi-AI-R12: OPTIMAI AI tools should ensure that at least high-level explanations are available to human operators for AI output.

PAi-AI-R13: The project should follow the Human-Centred Artificial Intelligence approach, thus ensuring, to the greatest extent possible, the reliability, safety, transparency, and trustworthiness of the developed AI technologies.
Meaningful Work and Impact on Work and Skills
PAi-AI-R14: Voluntary participation and withdrawal from testing OPTIMAI AI tools at pilot sites must be ensured.
PAi-AI-R15: Feedback of operators after they have tested the technology in order to understand how they perceive it has affected their experience of meaning and value at work, should be collected.
PAi-AI-R16: Training to operators should be delivered in accessible and multi-lingual formats.
Security, Health and Safety
PAi-AI-R17: End-users should conduct health and safety impact assessments before initiating testing activity of OPTIMAI tools involving human operators
PAi-AI-R18: End-users should secure their operations with physical and logical firewalls, and any other security measure as necessary.
Environment
PAi-AI-R19: In the event of sub-optimal performance of the AI leading to manufacturing waste, related processes should be terminated and tools refined.

Table 6 Digital Twins and Virtualisation: Ethical Requirements

Digital Twins & Virtualisation
Privacy and Data Protection
PAi-DT-R1: Virtualised human agents should not be designed or perform in a way that may refer to identifiable workers in a specific context.
Equality, Fairness, and Non-Discrimination
PAi-DT-R2: Human agents represented in the virtual environment should be diverse and inclusive to the greatest extent possible without infringing on the privacy of any current employees/operators, even if this does not represent the workforce of the site where the tool is deployed.
PAi-DT-R3: Simulations should account for the capabilities of workers with disabilities.
Human Agency and Oversight, Accountability, Transparency and Accuracy
PAi-DT-R4: Operators should be able to understand the logic underlying simulations. At least high-level explanations should be provided to operators.
PAi-DT-R5: Multi-lingual and appropriately accessible training and materials should be made available to users of the system.
PAi-DT-R6: Users of the systems should always be in control of processes related to the tool, and should always possess the ultimate authority when making decisions and initiating or terminating production processes.
PAi-DT-R7: Feedback of users after they have tested the technology in order to understand how they perceive it has affected their experience of meaning and value at work, should be collected.
PAi-DT-R8: Logs of the tools' operations should be kept.
Meaningful Work and Impact on Work and Skills

PAi-DT-R9: DT and Virtualisation tools should be a complement to operators' work and should not excessively reduce opportunities for creativity and problem-solving.
PAi-DT-R10: Feedback of operators after they have tested the technology in order to understand how they perceive it has affected their experience of meaning and value at work, should be collected.
Security, Health and Safety
PAi-DT-R11: Accurate virtual replicas of the manufacturing environment should be ensured.
PAi-DT-R12: Access to the tool should be restricted only to qualified and authorised users in the pilot sites and research staff working on the project.

Table 7 IoT & Sensors: Ethical Requirements

IoT & Sensors
Privacy and Data Protection
PAi-IoT-R1: Data minimisation must be ensured. Any unnecessary personal data or identifiers that may be collected during the operations should be anonymised or deleted.
PAi-IoT-R2: Operators and employees in the manufacturing environment must be notified about data collection.
PAi-IoT-R3: Technical partners should guide end-users through the appropriate placement and use of sensor devices.
Equality, Fairness, and Non-Discrimination
PAi-IoT-R4: Devices must be accessible to operators, considering any disabilities they may have that could challenge setting them up, modifying them or interacting with them in legitimate ways.
Human Agency and Oversight, Accountability, Transparency and Accuracy
PAi-IoT-R5: Sensors should support or compliment human workers rather than outright replace them.
PAi-IoT-R6: Detailed logs of sensor data flow should be maintained and their accuracy and performance regularly monitored.
PAi-IoT-R7: Technical partners should endeavour to support explainability, transparency and auditability of algorithms utilised in the security middlebox.
Meaningful Work and Impact on Work and Skills
PAi-IoT-R8: Acceptance of sensors and IoT devices should be fostered by providing meaningful information about their purpose and the types of data they process.
PAi-IoT-R9: Devices should be used as intended, i.e., support production optimisation. Under no circumstances should devices be used to monitor worker performance or non-production related activities.
PAi-IoT-R10: IoT and sensor devices should complement rather than replace human operators' skills.
PAi-IoT-R11: Feedback from operators and employees regarding the impact on the nature of work should be obtained.
Security, Health and Safety
PAi-IoT-R12: End users should provide safety information relating to the correct and safe use of sensors that can cause harm or injury from misuse.

PAi-IoT-R13: Health and safety risk assessment should be performed by qualified staff at pilot sites.
PAi-IoT-R14: IoT devices should follow best practice security standards. Examples of mitigation measures preserving security include: consensus about data to be communicated, data logging, cryptographic hash to prevent unwanted data from being communicated, and encrypted communication. Furthermore, sensors should be secured with different root passwords per sensor, communication should be via secure channels, frequent vulnerability assessments should be conducted, patching should be regular, installation of sensors should be in a protected space.
Environment
PAi-IoT-R15: Sensor and IoT performance should be consistently monitored and any devices contributing to sub-optimal production should be appropriately addressed.

Table 8 Wearables & AR: Ethical Requirements

Wearables & AR
Privacy and Data Protection
PAi-AR-R1: Operators, users and other employees who may be in their field of view, must be informed of the personal data collection and processing capabilities (and reasons for data collection) of the wearable glasses.
PAi-AR-R2: Informed consent procedures must be in place.
PAi-AR-R3: Only necessary data should be collected and unnecessary personal data anonymised, pseudonymised or destroyed as soon as possible.
PAi-AR-R4: Two-factor authentication for access to wearables should be prioritised over biometric authentication unless biometric methods demonstrably provide more security in this instance, and that such a level of enhanced security is necessary.
Equality, Fairness, and Non-Discrimination
PAi-AR-R5: Testing and design should be inclusive and involve as diverse a workforce as possible, with reasonable accommodations made for different physiological attributes (weight, height, head-shape) levels of ability (eye-sight etc.), and religious attire, especially such that current members of the workforce are not excluded from using OPTIMAI tools.
PAi-AR-R6: Extra measures should be taken towards inclusive design where the workforce of the pilot sites is particularly unrepresentative of the wider population.
PAi-AR-R7: The feedback of women and under-represented groups should be proactively sought.
Human Agency and Oversight, Accountability, Transparency and Accuracy
PAi-AR-R8: Requirements outlined in relation to IoT and AI should be observed.
Meaningful Work and Impact on Work and Skills
PAi-AR-R9: Multilingual and accessible training should be provided to operators.
PAi-AR-R10: Feedback should be collected directly from operators and others directly or indirectly affected by wearables and AR in the pilot sites on how the use of these tools has changed the nature of their work.
Security, Health and Safety

PAi-AR-R11: The AR user interface should be designed in order to be minimally intrusive both from a field of view perspective and in terms of the amount of information that is being presented to operators.
PAi-AR-R12: Health and safety risk assessments should be conducted in order to ensure the health and safety of operators in the manufacturing environment.
PAi-AR-R13: Best practice methods for securing the devices from attack or modification should be adopted.

Table 9 Blockchain: Ethical Requirements

Blockchain
Privacy and Data Protection
PAi-B-R1: Personal information should be kept off the blockchain.
PAi-B-R2: Persons who could potentially be re-identified from the recording of time-stamps should be notified and off-chain employee scheduling information should be deleted by end users when it has outlived its use.
PAi-B-R3: Private permissioned blockchain should be used.
Meaningful Work and Impact on Work and Skills
PAi-B-R4: Multilingual and access training or training materials should be made available for end users.
Security, Health and Safety
PAi-B-R5: Appropriate measures should be taken to safeguard the blockchain key from theft or loss, particularly from malicious actors.
Environment
PAi-B-R6: Only environmentally low impact blockchain platforms should be utilised for OPTIMAI.

3.3 Ethical Procedures: Monitoring Strategy

Strong monitoring structures and procedures have been established from an internal and external perspective to ensure that all OPTIMAI research activities are ethically and legally compliant, including the piloting activities.

The internal monitoring bodies of the project include Consortium partners with expertise in AI ethics and data protection, namely, UAB as Ethics Advisor and TRI as Data Protection Advisor. A hybrid monitoring body of OPTIMAI is the Ethics Board (EB), in charge of the ethical monitoring of OPTIMAI research activities, which is composed of internal members of the Consortium as well as external independent experts.

A key activity included in the monitoring and enforcement strategy is the assessment of the impact that OPTIMAI pilot activities may entail. To this end, an integrated risk assessment including ethical, legal and societal risk assessments, was conducted and can be found in *D9.2 Report on the OPTIMAI ethical, legal and societal risks – 1st version*. In order to obtain detailed information that could enable such close ethical and legal monitoring of the project, and, in particular the pilot activities, two different types of events were held with OPTIMAI Partners. First, a webinar aimed at raising awareness among Consortium Partners on legal, ethical and societal

issues that OPTIMAI research activities and OPTIMAI solutions could raise. Second, six dialogue sessions were arranged with technical partners and end-users to elicit information about the OPTIMAI solutions and their envisaged application in the shopfloor in the piloting activities (as described in **Subsection 2.4.1 Work Undertaken in 2021**).

This integrated risk assessment was conducted by the OPTIMAI internal monitoring bodies and reviewed by the Ethics Board. As a result of the risk assessment, which allowed the identification and analysis of legal, ethical and societal risks, mitigation measures to be adopted before the start of the pilot activities were made available and a set of initial legal and ethical requirements for the pilot activities was provided. These legal and ethical requirements for the pilot activities aim at ensuring the ethical design, development, and deployment of OPTIMAI solutions during pilot activities, and can be found in **Section 3.2 Ethical Requirements Identified for OPTIMAI Piloting Activities**.

Lastly, to reinforce the OPTIMAI ethics monitoring strategy, the Consortium has sought the ethics approval from CERTH Research Ethics Panel for conducting the piloting activities, given that CERTH is the Coordinator of the Project. The aim of this procedure is to add another layer of ethics monitoring to the piloting activities. To this end, an application for Ethical Approval has been filled by CERTH with the assistance of the UAB as ethics lead partner. The application contains a detailed description of the project and the three use cases in each pilot site, information on the legal and ethical monitoring activities regarding the piloting activities and the deliverables in which such information is further elaborated, and the Information sheet and consent form to be provided to all pilot site employees by the end-users (see **Appendix B: OPTIMAI Human Research Participant Information Sheet and Consent Form** and **Appendix C: OPTIMAI Pilot Research Ethics Application for CERTH**). Pilot activities will not start until the Ethical Approval has been granted. At the time of writing, the application has been submitted and the decision of CERTH Research Ethics Panel is pending.

OPTIMAI Ethics Board Recommendations for the Ethical Conduct of OPTIMAI Piloting Activities
This subsection presents the recommendations provided by the OPTIMAI EB as a result of the monitoring activities related to the legal and ethical framework identified for OPTIMAI piloting activities.

1. The EB shall check that partners will document measures taken to abide by the ethical and legal requirements of the project. To this end, a list of the measures to be documented is encouraged to track compliance with the ethical and legal requirements.
2. The EB points out that Acceptance of AI is important, in particular, in the second use case, namely “production line setup-calibration”: In this use case the operator will use the AI-based Decision Support System to be notified about automations executed by the system; and receive recommendations to execute manual control actions. The EB stresses the importance of ensuring that operators accept the automations executed by the system as well as trust the provided recommendations and execute on time the manual actions that the system suggests.

3. Regarding PAi-AR-R1, internal members of the EB highlight that the wearable glasses to be used in OPTIMAI piloting activities will not record nor gather personal data or images. However, this does not preclude informing operators that no recording will take place.
4. In the case of acquiring images from pilot sites, the issue of confidentiality and IPR of the pertinent factory should be clarified. That is, besides people who are depicted in a photo, machinery and equipment may also be depicted, which would require permission of the corresponding pilot site partner.
5. The EB requires clarifications on whether operators' consent will be sought. In this regard, research participation consent and data processing consent should be clarified.
6. The EB requires clarifications on how data subjects rights will be exercised in the context of the piloting activities.

Lastly, the EB acknowledges that the involvement of ethical and legal partners in the project cultivates an ethical and legal compliance attitude in the Cosortium partners. Additionally, the EB recognizes that this framework can be useful for similar contexts outside OPTIMAI as it can enable end-users to identify the need for ethical and legal advice in future manufacturing solutions.

The recommendations provided by the OPTIMAI EB are being addressed. To this end, the following actions are planned to be taken:

1. A compliance tracker document is being currently developed to monitor compliance with the ethical and legal requirements. In that document the requirements will be presented and end-users and technical partners will be asked to read the requirements and to specify the technical and organizational measures that have been taken or will be taken to secure compliance with these requirements.
2. The risks related to the acceptance of AI and IoT have been identified in D9.2 'Report on OPTIMAI ethical, legal and societal risks – 1st version', and will be also considered in the next iteration of this Deliverable, D9.3 'Report on OPTIMAI ethical, legal and societal risks – 2nd version'.
3. The risk related to personal data and images in the context of the wearable glasses has been identified in D9.2. As indicated, the risk arising from this personal data use should be considered low in light of informed consent procedures. The severity of this data being transferred to inappropriate contexts could be severe, however such data is intended to be used solely to access the wearable hardware and will be secured using best practice methods according to the requirements concerning security of sensitive data. Alternative methods for accessing the wearable hardware, including two-factor authentication, are being considered. This issue will be reminded in Deliverable D9.3.
4. This issue will be included in Deliverable D9.3, and will be evaluated together with the partners in charge of IPR (WP8).

5. This issue was discussed with pilot site partners at each Dialogue Session. Clarifications have been included in section *1.14.2 Legal Bases for Data Processing and Conditions for Consent* of this Deliverable. Likewise, this distinction will be made clear in the training that will be delivered as part of D7.1, e.g. clarification regarding consent in the context of power imbalance and a list of activities that employees could reasonably expect.
6. Procedures on how data subjects rights will be exercised in the context of the piloting activities, will be designed together with the pilot site partners. Consultation with their DPOs and legal department is also planned.

4 The General Data Protection Regulation and Basic Data Protection Recommendations for OPTIMAI Pilot Activities

4.1 Introduction

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation passed on 25th May 2018 that enshrines the privacy rights of data subjects in Europe and confers duties upon data controllers and processors to protect these rights. The content and applicability of the GDPR to OPTIMAI project data processing activities has been discussed in deliverables *D1.2 Data Management Plan* as well as *D9.1 Report on the OPTIMAI Ethical and Legal Framework*. This section will reiterate some of this work, whilst also focusing more closely on its applicability to OPTIMAI pilot activities.

Each participant in the OPTIMAI project is responsible for adhering to the principles and requirements of the GDPR, at least as laid out in the national law that implements them. This section will provide a general overview of overarching GDPR principles, requirements, and other important concepts, whilst the sections that follow will supplement this with information regarding national implementation relevant to the local context of pilot sites, including national best practice or guidelines where possible.

4.2 Data Processing and Personal Data

The GDPR governs the processing of personal data by data controllers and processors. In order to support OPTIMAI project partners in identifying and appropriately managing their personal data processing activities, this subsection will provide some definitions and examples of these terms. Data processing activities and personal data may not always be obvious, or may be taken for granted (for example, mundane activities such as the collection of email addresses of named individuals can be considered the processing of personal information), however partners should be aware that both data processing and personal data can be widely construed and appropriate safeguards should be in place for the handling of all personal data.

According to Article 4(1) of the GDPR:

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

The European Commission (EC) provides further helpful examples of personal data, including [8]:

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone);
- an Internet Protocol (IP) address;
- a cookie ID;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Personal data is not in reference merely to data in written form, but is also applicable to video, images and audio that contains identifiers of individuals [9]. Personal data can be based on both identified (e.g., a named data subject) or identifiable persons (a person who can be identified with additional information) [9].

Article 9(1) prohibits (with some exceptions) processing of special categories of personal data. These data relate to:

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

Article 4(13)-(15) further clarifies these special categories of data. In the context of OPTIMAI, health and biometric data are relevant to the data capturing capabilities of deployed technologies, as well as types of sensitive data expected to be processed in the occupational context. For that reason, these will be elaborated here.

Biometric data, according to Article 4(14):

....means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

Examples of biometric data include fingerprints, facial information, iris scans, or gait recognition [10, 11].

Health data, according to Article 4(15):

...means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status...

Finally, when we refer to the processing of personal data, we refer to, as described in Article 4(2):

...any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction...

Thus, processing operations are widely construed and refer to many instances of utilisation of personal data [9]. For this reason, when partners process all of the many different types of personal data, they are subject to the principles and requirements of the GDPR and should respond accordingly to uphold data subject rights.

4.2.1 Data Protection Principles

The GDPR is designed around seven key principles for governing data processing activities and protecting data subject rights. These principles are set out in Article 5 of the GDPR and are [9]:

- *Lawfulness, fairness, and transparency*

Data processing should be lawful, fair and transparent to the data subject. Data should be processed on an appropriate legal basis and processing should be made known to data subjects [12]. Transparency entails that information and communications pertaining to the processing should be accessible, understandable and in clear and plain language [12].

- *Purpose Limitation*

Data should be processed for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Article 89(1) permits further processing for purposes in the public interest, scientific or historical research purposes or statistical purposes.

- *Data Minimisation*

Data should be adequate, relevant, and limited to the purposes for which they are processed.

- *Accuracy*

Data should be accurate and up to date and reasonable steps should be taken to erase or rectify inaccurate data.

- *Storage Limitation*

Data should not be stored that allows the identification of data subjects for longer than is necessary for the purposes for which the data is processed, subject to Article 89(1) exceptions and the implementation of appropriate technical and organisational measures safeguarding the rights and freedoms of data subjects.

- *Integrity and Confidentiality*

Data should be processed in a manner that ensures security and protection against unauthorised or unlawful access and against accidental loss, damage or destruction using appropriate technical and organisational means.

- *Accountability*

This principle sets out the responsibility of the Data Controller for complying with the preceding principles as well as being able to demonstrate compliance.

4.2.2 Legal Bases for Data Processing and Conditions for Consent

Article 6(1) sets out the legal bases for processing personal data, that is, legal justifications for using personal data in particular ways. These bases, laid out in Article 6(1)(a)-(f) are:

- consent
- necessary for the performance of a contract
- compliance with a legal obligation
- protecting the interests of a data subject or another natural person
- performance of a task in the public interest or the exercise of official authority
- legitimate interest.

For each data processing activity, OPTIMAI data controllers will need to carefully consider the legal basis for each data processing operation, as different processing operations may rely on different legal bases

Consent is a common legal basis that justifies the processing of personal data and the conditions for consent are set out in Article 7. Consent must be freely given (for example, not under coercion or threat or risk of adverse consequences) and data subjects must have the ability to easily withdraw their consent at any time. Consent must be unambiguous and given by a clear affirmative act, as well as specific and informed with the identity of the data controller and purposes of processing communicated to the data subject [13].

In the case of OPTIMAI, data subjects and controllers may have employee and employer relations characterised by power asymmetries. OPTIMAI pilot site employees will be expected to utilise cutting-edge digital technologies with audio and visual data processing capabilities and operate within the same environment as these technologies. As these employees will not be able to demonstrably freely consent to data processing operations entailed by the use of these technologies,⁵ consent cannot be relied upon as a lawful basis for data processing [14, 15].

Thus, alternative legal bases will need to be relied upon in cases where employees are data subjects without a demonstrably meaningful choice in participating or being a data subject for the purposes of OPTIMAI research data processing activities. In the absence of consent, legitimate interest or performance of contract should be considered as the legal basis for data processing operations involving employees' personal data. OPTIMAI partners should identify the legitimate interest for data processing operations, which may include commercial, academic or scientific interests and societal benefits [13]. A relevant legitimate interest to specific instances of data processing may exist between end-users and employees, for example, based on a "relevant and appropriate relationship" and where data subjects can "reasonably expect" the data processing operations at the time and in their context of taking place [13]. Nevertheless, the

⁵ In the context of OPTIMAI as a research project, the situation may raise the ethical tensions inherent in the differentiations between research participation consent and data processing consent.

processing operation should be transparent, and pilot site employees should be clearly and fully-informed about them including the purposes of the data processing [15].

Legitimate interest must be able to pass necessity and balancing tests [13]. Data controllers should be able to demonstrate that the data processing operations are “a reasonable and proportionate way of achieving their purpose” and that other, less intrusive methods are not available for achieving these purposes. A balancing test requires that the data controller determine whether data subjects can reasonably expect the kind of data processing operation in question and whether they are vulnerable to unjustified harm that could override the legitimate interest [13]. It is important that “clear and proportionate justification for the impact” on data subjects is provided, that the data subject’s rights and freedoms are taken into account, that adequate data protection considerations (safeguards, data minimisation etc.) are taken into account, that an appropriate record of the assessment is made and that the assessment is updated if necessary based on changing circumstances [13].

A legitimate interest assessment template has been made available to OPTIMAI partners, and data controllers are urged to utilise it where legitimate interest is expected to be a legal basis for data processing, in line with supporting compliance with the foregoing requirements.

In cases where the employee-employer relationship might not be as relevant and thus restrictive, consent may still be a preferred legal basis for data processing. For example, in the case of the publication of images of a data subject at work, the data subject might more freely provide and revoke consent to the action as the risks in incurring any detriment to themselves as employee seem limited. Special attention should also be given to the process of potential personal data other than the data subject’s image, i.e. other people being in the picture, as well as as other emerging issues such as confidentiality and IPR of the pertinent factory. However, whether or not refusal or retraction may hold detriment would depend on the circumstances of each case.

4.2.2.1 Consent: Ethical versus Data Protection Obligations

The reader may note an apparent contradiction in requirements regarding the ethical obligation to receive informed consent from research participants and the invalidity of consent in certain circumstances as a lawful basis for data processing. In the context of processing health/medical data, and still applicable here, the European Data Protection Board (EDPB) has addressed this contradiction [16]. Fundamentally, a line must be drawn between the ethical principle of informed consent in research project participation—something which protects persons from involvement in such research without their knowledge or against their will—and consent as a lawful basis for specific data processing operations, and not involvement in a research project per se [16]. Both of these types of consent are considered distinct but not incompatible concepts. The EDPB (specifically in the health/medical data context but again applicable here) still requires that ethical consent requirements for participation are met even where individuals cannot consent to specific data processing operations that might constitute that involvement [16]. Therefore, a situation may arise in the project where, for example, an employee in a pilot site is required to consent to participate in the research activity, but this consent does not provide a suitable legal basis for corresponding data processing operations, and therefore another *legal*

basis will have to be used in conjunction with the separate *ethical* requirement for informed consent.

4.2.3 Processing of Special Categories of Data

The processing of special categories of data (identified above) is generally prohibited under Article 9(1) of the GDPR. Nevertheless, data controllers may identify purposes for the processing of this data over the course of OPTIMAL research activities including possibly data relating to race and ethnicity for equal opportunity monitoring or, as identified in D9.2, biometrics for secure access to wearable devices.

Exceptions to this prohibition are outlined in Article 9(2)(a)-(j). The exceptions bearing potential relevance to the OPTIMAL project include where:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1⁶ may not be lifted by the data subject
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
- processing relates to personal data which are manifestly made public by the data subject
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a

⁶ Article 9(1):

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

health professional and subject to the conditions and safeguards referred to in paragraph 3⁷

- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)⁸ based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Note that the “*explicit*” consent condition is of a higher threshold than consent as referred to without the explicit condition specified. The European Data Protection Supervisor (EDPS) has stated the following [17]:

Explicit consent, described by the EDPB as ‘an express statement of consent’ which can be demonstrated in the event of doubt, is required thus in situations where there may be particular risk to the rights of the data subject.

The consent condition again should not be relied upon in many cases involving an employer-employee relationship. Generally, processing special categories of data should be avoided unless partners can demonstrate compelling justification, that it is necessary to achieve particular purposes compatible with Article 9(a)-(j) and the data subject’s rights and freedoms are effectively protected. Processing such data could be considered risky, especially if it is done on a large scale or entails other factors including monitoring, automated decision-making, or evaluating or scoring [18]. Conducting a data protection impact assessment (DPIA) in relation to processing special categories of personal data is good practice [18]. A threshold analysis has been provided to partners in order to support the decision about whether a DPIA is necessary.

Of note is that the Article 29 Data Protection Working Party warns against the processing of health data obtained from wearables in the employment context for the purposes of health monitoring, including the transfer of such data to device/service providers, given that explicit consent cannot be given by employees and because of the unreliability of anonymisation techniques [15]. This militates against live monitoring of employee health data, even if efforts are made to anonymise this data. Nevertheless, processing of health data is not absolutely

⁷ Article 9(3):

Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

⁸ Article 89(1):

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

prohibited as it may be necessary for different, limited and justifiable, instances of health surveillance or medical examinations/health assessments.

4.2.4 Controller and Processor

In the OPTIMAI project, entities responsible for personal data will be data controllers or processors who utilise in some cases personal data for the purposes of achieving research or communication, exploitation and dissemination objectives.

For clarity, a Data Controller, according to Article 4(7):

...means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

A Data Processor, according to Article 4(8):

...means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

A controller then decides how and why personal data is collected and processed, and in OPTIMAI could for example be a task leader or participant that is responsible for making these decisions. A joint controllership arises whereby multiple partners determine the means and purposes of data processing. A processor may be a partner who processes personal data under instruction of the data controller.

The data controller is obliged under Article 24(1)-(3) to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR, as well as implement appropriate data protection policies. Joint controllers must transparently determine their respective responsibilities and should designate a contact point.

Whereby it is determined that a partner is acting as a data processor for a data controller, Article 28(3) requires that the relationship be governed by a contract "...that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller".

Article 30(1) requires that controllers maintain records of their processing activities including names and contact details of controllers (including the Data Protection Officer (DPO)); purposes of data processing; description of categories of data categories and subjects as well as recipients; details (including safeguards) of third country data transfers; time limits for data erasure; and a description of technical and organisational security measures. Article 30(2) requires data processors to maintain shorter records, including names and contact details of processors and controllers and their data protection officers; categories of processing; details (including safeguards) of third country data transfers; time limits for data erasure; and a description of technical and organisational security measures.

Article 32(1)(a)-(d) explicates the security and organisational measures to be implemented by controller and processor:

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

Furthermore, Article 25(1)-(3) establishes duties of data protection by design and default which further emphasise the need for data minimisation, pseudonymisation and effective safeguards.

Article 35(1) lays out the requirement of a DPIA by the controller where it is established that processing may result in a high risk of harm for data subjects. A DPIA threshold analysis has been provided to OPTIMAI Consortium partners outlining the criteria used to establish risk of data processing operations and the necessity of a DPIA. Each partner should utilise this threshold analysis document before proceeding with data processing operations. Where a DPIA indicates a high risk to data subjects in the absence of mitigation measures, Article 36(1) requires consultation with the supervisory authority before data processing.

Where a data breach occurs, Articles 33 and 34 require that the supervisory authority and data subjects be notified without undue delay (or no later than 72 hours after the breach for data controllers).

Of special note is Article 35(9). This provision encourages data controllers to solicit the views of data subjects regarding the intended data processing operations.

4.2.5 Rights of the Data Subject

The GDPR enshrines the rights and freedoms of data subjects in relation to their personal data. Data subjects may represent a range of different persons during the overall course of the project including individual human research participants, external experts, media contacts, mailing-list subscribers and more. With regards specifically to the planned pilot activities, data subjects may include human research participants such as employees of the end-users' partners. Data processed about such data subjects could potentially include names and contact details, image and audio data or other data yet to be identified. The following lays out their rights as enshrined in the GDPR.

4.2.5.1 The Right to Information

Article 12(1) lays out transparency requirements for the communication of information to data subjects. The data controller is to communicate information to the subject in "concise, transparent, intelligible and easily accessible form".

Article 13(1) lists the information to be communicated to data subjects ("at the time when personal data are obtained"), including:

- the identity and the contact details of the controller and, where applicable, of the controller's representative
- the contact details of the data protection officer, where applicable
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- where the processing is based on point (f)⁹ of Article 6(1), the legitimate interests pursued by the controller or by a third party
- the recipients or categories of recipients of the personal data, if any
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46¹⁰ or 47,¹¹ or the second subparagraph of Article 49(1),¹² reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Additional information requirements stemming from Article 13(2) include:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- where the processing is based on point (a) of Article 6(1)¹³ or point (a) of Article 9(2),¹⁴ the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal

⁹ Article 6(1)(f):

...processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

¹⁰ Relating to transfers subject to appropriate safeguards.

¹¹ Relating to binding corporate rules.

¹² Which is:

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.³The controller shall inform the supervisory authority of the transfer.⁴The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

¹³ Consent.

¹⁴ Explicit consent.

- the right to lodge a complaint with a supervisory authority
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- the existence of automated decision-making, including profiling, referred to in Article 22(1)¹⁵ and (4)¹⁶ and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Article 13(3) requires that the data subject be notified about further processing beyond that for which the data was originally collected.

Article 14(1)-(2) governs information rights and controller duties whereby the data was not collected from the data subject. In this case, the controller must provide:

- the identity and the contact details of the controller and, where applicable, of the controller's representative
- the contact details of the data protection officer, where applicable
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- the categories of personal data concerned
- the recipients or categories of recipients of the personal data, if any
- where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability

¹⁵ Article 22(1):

The data subject shall have the 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.

¹⁶Article 22(4):

Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

- where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- the right to lodge a complaint with a supervisory authority
- from which source the personal data originate, and if applicable, whether it came from publicly accessible sources
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Article 14(4) requires that the data subject be notified about further processing beyond that for which the data was originally collected. Exceptions to these duties exist, as outlined in Article 14(5), which may preclude disclosure, for example, where the data subject already has the information; there are confidentiality requirements; or disclosure would require disproportionate effort.

It is noted that various devices with audio and visual data capturing capabilities will be utilised over the course of OPTIMAI pilot and research activities. The European Data Protection Board has published specific guidance relating to transparency and information obligations relating to the use of video surveillance [19]. The EDPB suggests a layered approach to informing data subjects about video surveillance. The layered approach is described in the following.

4.2.5.1.1 First Layer

As first layer information concerning the video surveillance operation the EDPB recommends a warning sign, as a possible example. The warning sign should convey to the data subject in “easily visible, intelligible and clearly readable manner, a meaningful overview of the intended processing”, in a format adapted to the location [19]. The warning sign should be placed (at eye level) in a manner that the data subject understands the circumstances of the surveillance before entering the monitored area, and can estimate the area being surveyed in order to avoid it or adapt their behaviour accordingly [19]. The warning sign should convey information including the purpose of the processing; the data controller’s identity and Data Processing Officer contact details; the existence of the data subject’s rights and the impacts of the data processing operation; and *refer to more detailed second layer information* (e.g., by QR (quick response) code or website address) [19].

The EDPB suggests informing the data subject of any unexpected details at this layer, including third-party transmission and storage periods [19].

4.2.5.1.2 Second Layer

The EDPB suggests that second layer information be made available at an easily accessible place and in an easily accessible format such as an information sheet available at a centralised location [19]. This information should be accessible in non-surveyed areas [19]. Second layer information should convey all relevant points as obliged by Article 13 [19]. The EDPB recommends the following methods for information provision [19]:

Geolocating cameras and including information in mapping apps or websites so that individuals can easily, on the one hand, identify and specify the video sources related to the exercise of their rights, and on the other hand, obtain more detailed information on the processing operation.

4.2.5.2 The Right to Access

Article 15(1) of the GDPR enshrines the right of the data subject to obtain confirmation on whether data about them is being processed, as well as the following information:

- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- the right to lodge a complaint with a supervisory authority
- where the personal data are not collected from the data subject, any available information as to their source
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Additionally, the data subject is entitled to information about appropriate safeguards where data is transferred to a third country.

Notably, it is important that the data controller implements measures to confirm the identity of the presumed data subject before disclosing personal data.

4.2.5.3 The Right to Rectification

Article 16 grants the data subject the right to have inaccurate information about them corrected, as well as, with regards to the purpose of the data processing, the right to complete incomplete information including by way of a supplementary statement.

4.2.5.4 The Right to Erasure

Article 17(1) grants the data subject the right to have data held about them erased on the following grounds:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing

- the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2)
- the personal data have been unlawfully processed
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject
- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).¹⁷

Where the controller has made any such data public, it should take steps to communicate the erasure request to other data controllers.

Article 17(3) lists exceptions to this right, which include, where the processing is:

- for exercising the right of freedom of expression and information
- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3)
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

4.2.5.5 The Right to Restriction of Processing

Article 18(1) grants the data subject the right to have data processing restricted on the following grounds:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead

¹⁷ Article 8(1):

Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where international transfers are concerned, the data subject also has a right to information pertaining to safeguards.

4.2.5.6 The Right to Data Portability

Article 20(1) gives the data subject the right to receive their personal data “in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided”, where the processing is based on consent or is carried out by automated means.

4.2.5.7 The Right to Object

Article 21(1) grants the data subject the right to object to processing of their personal data and the “controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims”.

4.2.5.8 The Right to Avoid Automated Decision-Making

Article 22(1) grants the data subject the right not to be subject to automated decision-making including profiling with legal (or similar) effects. Exceptions arise based on performance of contract, authorisation by law, and where *explicit* consent is obtained from the data subject.

4.2.6 Derogations for Research and Employment Purposes

As OPTIMAI is a scientific/academic research project which engages employees at work, it is important for partners, especially end-user partners, to be aware of permissible derogations that arise as a result of this set of circumstances, which may limit or affect particular data protection subject rights and data controller responsibilities in particular ways.

Article 89(2) provides for national legislation derogating from provisions of Article 15 (right of access by data subject), Article 16 (right to rectification), Article 18 (right to restriction of processing), and Article 21 (right to object), where the processing is done for the purposes of scientific or historical research purposes or statistical purposes subject to particular conditions and safeguards outlined in Article 89(1)¹⁸ and “in so far as such rights are likely to render

¹⁸ Article 89(1):

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner.

impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes”.

Article 89(2) provides for national legislation derogating from provisions of Article 15 (right of access by the data subject), Article 16 (right to rectification), Article 18 (right to restriction of processing), Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing), Article 20 (right to data portability), and Article 21 (right to object), where processing is done for the purposes of archiving in the public interest subject to particular conditions and safeguards outlined in Article 89(1) and again “in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes”.

Article 88(1) allows for member states to provide for specific measures relating to data processing in the employment context. Specifically, it states:

Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer’s or customer’s property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

Where any such measures are articulated, they will be provided in **Section 5 Regulatory Framework to Support Lawful Conduct of Pilot Activities in the United Kingdom**, **Section 6 Regulatory Framework to Support Lawful Conduct of Pilot Activities in Spain**, and **Section 7 Regulatory Framework to Support Lawful Conduct of Pilot Activities in Greece**.

4.2.7 Transfers of Personal Data to Third Countries or International Organisations

Articles 44 to 50 govern data processing involving transfers to third countries and international organisations. Transfer may only take place where an adequate level of protection can be ensured (as decided by the European Commission (EC) on the basis of an adequacy decision).

Data controllers and processors may only transfer personal data to third countries or international organisations where they have “provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available”.

Such appropriate safeguards include:

- a legally binding and enforceable instrument between public authorities or bodies
- binding corporate rules in accordance with Article 47

Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

- standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2)
- standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2)
- an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights
- contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
- provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Article 49 lays out derogations for specific situations absent adequacy decisions or appropriate safeguards, which include situations where:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
- the transfer is necessary for important reasons of public interest
- the transfer is necessary for the establishment, exercise or defence of legal claims
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

OPTIMAI involves a partner in the UK (MTCL), and a partner with shared infrastructure and resources with the UK (TRI Ireland), however the UK has benefited from an adequacy decision by the EC.

4.2.8 Technical Security Measures

As the GDPR stipulates the necessity of secure processing of personal data, including through the appropriate implementation of technical and organisational measures, it is worth elaborating more concretely what such requirements mean for OPTIMAI Consortium partners

from the perspective of technical measures (the preceding text has already extensively addressed matters of a more organisational nature). The European Union Agency For Network and Information Security (ENISA) provides helpful guidance on the security of data processing operations, learnings from which will be outlined in the this subsection. Suggestions on the adoption and implementation of technical measures via ENISA are based on ISO 27001: 2013. ENISA's risk evaluation indicator is defined as threat occurrence probability x impact to individuals whose data is being processed. ENISA guidance is provided at three tiers, low risk, medium risk, and high risk [20].

4.2.8.1 Access Control

For low-risk situations, ENISA suggests access control and authentication to prevent unauthorised access to IT systems [20]. ENISA recommends that an access control system be implemented for users of IT systems, facilitating the creation, review and deletion of user accounts, and that use of common user accounts be minimised or restricted to users with the same roles and responsibilities [20]. Authentication mechanisms for accessing IT systems should be in place minimally utilising username/password combinations where passwords respect a configurable complexity [20].

For medium-risk situations, ENISA suggests implementing specific password policies and the storage of passwords in hashed form [20].

For high-risk situations ENISA suggests two-factor authentication and device authentication to ensure that personal data is processed only through specific network resources [20].

4.2.8.2 Logging and Monitoring

For low-risk situations, ENISA suggests the adoption of log files for each system or application processing personal data including types of access to the data and that these logs are time-stamped, tamper-proof, protected against unauthorised access and "synchronised to a single reference time source" [20].

For medium-risk situations, ENISA suggests logging administrator actions, as well as restricting the possibility for modifying logs, and access should be monitored for unusual activity [20]. A system should be in place to produce reports and alerts based on the logs [20].

4.2.8.3 Server/Database Security

For low-risk situations, ENISA recommends that databases and applications servers be configured to run a separate account with minimum operating system (OS) privileges [20]. Such databases should only process personal data necessary to achieve the purpose of the data processing operation [20].

For medium-risk situations, encryption should be considered through hardware or software implementations on specific files or records including storage drives [20]. Pseudonymisation should be used to unlink personal identifiers [20].

For high-risk situations, it suggests other privacy preserving techniques should be considered e.g., “such as authorized queries, privacy preserving data base querying, searchable encryption....” [20].

4.2.8.4 Workstation Security

For low-risk situations, ENISA suggests that users should not be able to deactivate or bypass security settings nor install unauthorised software; that antivirus applications and detection signatures are configured weekly; systems should have time-out protocols for inactive/idle users; and that critical OS updates are regularly installed [20].

For medium-risk situations, it is suggested that anti-viruses and detection signatures be configured daily.

For high-risk situations, it is suggested that personal data should not be moved to external storage; that workstations used for personal data processing be kept disconnected from the internet unless adequate security measures are in place to prevent unauthorised processing; and full disk encryption should be utilised on workstations operating system drives [20].

4.2.8.5 Network/Communication Security

For low-risk situations, ENISA suggests that when access is performed through the internet, communications should be encrypted using cryptographic protocols including TLS/SSL [20].

For medium-risk situations, it is suggested that wireless access to information technology (IT) systems is restricted to specific users and processes and protected by encryption [20]. Remote access should generally be avoided and subject to monitoring through pre-defined devices where it is necessary [20]. Traffic to the system should be monitored and governed through firewalls and intrusion detection systems [20]. The network of an information technology (IT) system should be segregated from other data controller networks [20]. Access to IT system should be granted only to authorised devices and terminals using, e.g., Media Access Control (MAC) filtering or Network Access Control.

4.2.8.6 Back-ups

For low-risk situations, ENISA recommends the definition of data back-up and restore procedures that are documented and clearly linked to roles and responsibilities [20]. Back-ups should have appropriate physical and environmental protection “...consistent with the standards applied on the originating data” [20]. The execution of back-ups should be regularly monitored to ensure their completeness and full back-ups should be regularly carried out [20].

For medium-risk situations, back-up media should be tested regularly to ensure reliability [20]. It is advised that incremental back-ups be carried out daily [20]. Copies should be stored securely in different locations [20]. If third party services are utilised for back-up storage, the data should be encrypted prior to being sent [20].

For high-risk situations, it is recommended that back-up copies are encrypted and stored securely offline [20].

4.2.8.7 Mobile/Portable Devices

For low-risk situations, ENISA suggests that portable device management procedures be defined and documented [20]. Devices accessing the network should be pre-registered and pre-authorised [20]. Access control procedures should mirror those of other terminal equipment [20].

For medium-risk situations, specific roles and responsibilities should be assigned in relation to portable device management [20]. The data controller/processor should be capable of remote deletion of personal data on devices that have been compromised [20]. Software containers should facilitate the separation of business and personal uses of devices [20]. The portable devices should be physically protected from theft when they are not in use [20].

For high-risk situations, the devices should be secured with two-factor authentication [20]. Personal data stored on the device should be encrypted [20].

4.2.8.8 Application Lifecycle Security

For low-risk situations, ENISA recommends following best practices, state-of-the-art and recognised secure development practices including standards and frameworks during the development cycle of data processing systems or applications [20]. It is recommended to define and implement specific security requirements at the beginning of this lifecycle, which should be tested and validated [20]. Privacy enhancing technologies should be adopted in this process [20]. ENISA recommends the adoption of secure coding standards and practices [20].

For medium-risk, vulnerability assessments should be conducted including application and infrastructure penetration tests by third parties, with penetration testing being periodic [20]. Vulnerability information about the information systems should be acquired [20]. Software patches should be tested and evaluated before installation in the operating environment [20].

4.2.8.9 Data Deletion/Disposal

In low-risk situations, ENISA suggests software-based overwriting of storage media before its disposal or their complete destruction where this is not possible [20]. Paper and portable media should be shredded or otherwise destroyed [20].

In medium-risk situations, ENISA suggests multiple passes of the software overwriting solution on the storage media and the use of a service agreement where third parties or engaged for disposal of media [20].

In high-risk situations, ENISA suggests degaussing or physical destruction following software erasure and that the data controller consider engaging third parties to destroy media on its (the data controller's) own premises [20].

4.2.8.10 Physical Security

For low-risk situations, ENISA has suggested that the physical perimeter of IT system infrastructure be inaccessible to unauthorised persons [20].

For medium-risk situations, ENISA has suggested that clear identification for all personnel and visitors on the premises be used [20]. Secure zones protected by appropriate means (including physical barriers) supported by regularly monitored logging and audit trails should be implemented [20]. Intruder detection methods should be deployed in secure zones [20]. Vacant

secure areas should be “physically locked and periodically reviewed” [20]. Furthermore, it is suggested that “[a]n automatic fire suppression system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) should be implemented at the server room” [20]. External support parties should be granted only restricted access to the secure zones [20].

4.3 Basic Data Protection (BDP) Requirements for OPTIMAI Pilot Activities

Table 10 Lawful Basis Requirements

ID	BDP-LB	Requirement	Lawful Basis (LB)
Description	Data controllers must utilise an appropriate lawful basis for each data processing operation associated with OPTIMAI pilot activities.		
Implementation in OPTIMAI	<p>BDP-LB-01. Consent will only be an appropriate legal basis for data processing where it is freely given, specific, informed and given by unambiguous agreement. Data subjects should be able to withdraw this consent at any time.</p> <p>BDP-LB-02. Consent should not be relied upon in cases where there is a clear power imbalance between data subject and controller/processor and the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment (Recital 42 GDPR), such as the employer-employee relationship, where genuine free choice cannot be demonstrated.</p> <p>BDP-LB-03. In cases where consent cannot be relied upon, data controllers should consider whether legitimate interest or another basis is an appropriate lawful basis for data processing. A balancing test should be performed and documented with the assistance of a legitimate interest assessment.</p>		

Table 11 Special Categories of Data Requirements

ID	BDP-SCD	Requirement	Special Categories of Data (SCD)
Description	The processing of special categories of data in connection with OPTIMAI pilot activities shall be prohibited. Only with appropriate justification and safeguards is the processing of these categories lawful/fair/acceptable.		
Implementation in OPTIMAI	<p>BDP-SCD-01. Consent for the processing of special categories of personal data should be explicit, freely given, specific, informed and given by unambiguous agreement. Data subjects should be able to withdraw this consent at any time.</p> <p>BDP-SCD-02. Consent for processing of special categories of data should not be relied upon in cases where there is a clear power imbalance</p>		

	<p>between data subject and controller/processor, such as the employer-employee relationship, where genuine free choice cannot be demonstrated. (see addition above)</p> <p>BDP-SCD-03. Special categories of personal data may be processed on the basis of public interest, scientific or historical research purposes, on the condition that appropriate technical and organisational measures are implemented protecting the rights and freedoms of the data subjects.</p> <p>BDP-SCD-04. Partners should pay particular regard to the principle of data minimisation, as well as consider pseudonymisation where the data processing purposes permit this.</p>
--	---

Table 12 Data Controller and Processor Requirements

ID	BDP-DCP	Requirement	Data Controller and Processor (DCP)
Description		Data controllers and processors should correctly identify themselves and comply with GDPR requirements arising as a result of their controllership or by dint of being processor.	
Implementation in OPTIMAI		<p>BDP-DCP-01. Consortium partners must identify whether they are data controllers, processors, or party to joint controllerships with regards to specific data processing operations.</p> <p>BDP-DCP-02. Data controllers and processors must ensure appropriate security, technical and organisational means are implemented that protect the rights and freedoms of data subjects.</p> <p>BDP-DCP-03. Data controllers and processors must implement appropriate data protection policies.</p> <p>BDP-DCP-04. Joint controllers must transparently determine their respective responsibilities and should designate a contact point for data subjects.</p> <p>BDP-DCP-05. Whereby it is determined that a partner is acting as a data processor for a data controller, the relationship must be governed by a contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.</p> <p>BDP-DCP-06. Data processors and controllers should keep appropriate</p>	

	<p>records of data processing activities.</p> <p>BDP-DCP-07. Data controllers must conduct, at a minimum, data protection impact assessment threshold analyses prior to data processing activities.</p> <p>BDP-DCP-08. Data controllers and processors must notify data subjects and the applicable data protection authority of any breach in a timely manner.</p> <p>BDP-DCP-09. Data controllers should consult with affected parties ahead of new data processing activities.</p> <p>BDP-DCP-10. Data controllers must ensure that data is processed for specific lawful purposes, in line with the principles of data minimisation, and that such data is made available only to persons as necessary for achieving those purposes. Further processing must not be undertaken unless exceptions apply. Data must be retained only as long as necessary to achieve their purpose, or as long as required to meet any other legal obligation.</p>
--	--

Table 13 Data Subject Rights Requirements

ID	BDP-DSR	Requirement	Data Subject Rights (DSR)
Description		To the maximum extent possible, and subject to permissible exemptions (see for example, Subsection 4.2.6 Derogations for Research and Employment Purposes), OPTIMAI data subject rights must be upheld and protected.	
Implementation in OPTIMAI		<p>BDP-DSR-01. The data controller is to communicate all relevant information to the data subject in a concise, transparent, intelligible and easily accessible form, and must be aware that duties apply even where personal data was not collected by the data controller.</p> <p>BDP-DSR-02. The data subject must be notified about data processing activities and be given access to any data held about them and related information including about their rights. The data controller shall implement means to verify the identity of any persons making subject access requests.</p> <p>BDP-DSR-03. The data subject has the right to have incorrect information about them corrected and have incomplete information corrected including by supplementary statement.</p> <p>BDP-DSR-04. The data subject has the right for their data to be erased where it is no longer necessary; consent is withdrawn; they object to processing; the data has been unlawfully processed; etc..</p>	

	<p>BDP-DSR-05. The data subject has the right to have data processing restricted where the personal data's accuracy is contested; processing is unlawful and the subject requests restriction rather than erasure; the controller no longer has use for the data but the data subject does (e.g., for a legal claim); or the data subject has objected pending verification of whether the grounds of the controller override the subject's interest.</p> <p>BDP-DSR-06. The data subject has the right to receive their personal data “in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided”, where the processing is based on consent or is carried out by automated means.</p> <p>BDP-DSR-07. The data subject has the right to object to processing of their personal data and the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.</p> <p>BDP-DSR-08. The data subject has the right not to be subject to automated decision-making including profiling with legal (or similar) effects. Exceptions arise based on performance of contract, authorisation by law, and where explicit consent is obtained from the data subject.</p>
--	---

Table 14 International Data Transfer Requirements

ID	BDP-IDT	Requirement	International Data Transfers (IDT)
Description		International data transfers and transfers to international organisations, subject to exemptions (see Subsection 4.2.7 Transfers of Personal Data to Third Countries or International Organisations), must only take place where the rights and freedoms of data subjects can be ensured.	
Implementation in OPTIMAI		BDP-IDT-01. Data controllers and processors must, subject to derogations, transfer data to third countries and international organisations only where there are appropriate safeguards and assurances, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.	

5 Regulatory Framework to Support Lawful Conduct of Pilot Activities in the United Kingdom

5.1 Introduction

MTCL, or Microchip Technology Calcidot Ltd., is an end-user partner that designs and manufactures miniaturized modules for high reliability, security and medical applications. MTCL's site, located in Wales in the United Kingdom, has extensive micro-electronic packaging capabilities, specializing in niche medium volume manufacture for medical, wireless, telecommunications and security customers. MTCL will carry out three use cases on their site, which are detailed in **Subsection 5.2 Pilot description MTCL**.

In order to support the lawful conduct of pilot site activities at MTCL, a cross-section of relevant UK national law has been reviewed and will be presented here as an overview to support the end-user partner and responsible technical partners (supplying hardware and software tools and processing related data) in taking action to protect the rights and interests of pilot site employees, visitors, and any other affected persons.

This section will present an overview of relevant provisions of UK data protection law, employment law, equality law, and health and safety law.

Subsection 5.3 Data Protection Law will indicate the rights of data subjects and the responsibilities of data controllers and processors with particular regards for employment settings.

Subsection 5.4 Employment Law will lay out the rights of MTCL employees, particularly with regards to protections for protected disclosures, protection from unfair dismissal, and matters relating to reporting and refusal to work in unsafe environments.

Subsection 5.5 Equality Law will lay out employees' rights to not be discriminated against or harassed or victimised on the basis of protected characteristics, as well as duties regarding reasonable accommodations for persons with disabilities.

Subsection 5.6 Health and Safety Law lays out various requirements relating to the provision of safe working environments and equipment that facilitate employee welfare and empower employees to operate safely within the manufacturing environment.

Finally, actionable requirements are provided in tables in **Subsection 5.7 UK Data protection, Employment and Equality, and Health and Safety** on the basis of core points from these overviews.

5.2 Pilot description MTCL

Pilot activities at MTCL will be undertaken with a view to test 3 use cases (UCs) of the OPTIMAI solutions and ecosystem, including UC-1 zero defect quality inspection, UC-2 production line set-up calibration, and UC-3 production planning.

The following will briefly detail these use cases and their objectives, based on information collected by OPTIMAI technical partner ENG and provided by members of the OPTIMAI Consortium.

UC-1 Zero defect quality inspection. Currently, inspection of manufacturing of outputs for quality control is conducted at the end of manufacturing steps or at other points in the downstream process. During this process, human workers inspect samples using microscopes and base decisions and judgements on their expert knowledge. This case intends to test the automation of quality control methodologies for wafer sawing, PCB routing, and glue/epoxy dispensing. The objectives of the use case are real time defect detection, identification of upstream defect causes, and prediction and prevention of defects. The use case will be supported through the use of algorithms and the installation of sensors in the work environment and devices including tablets and augmented reality wearables will be utilised by workers.

UC-2 Production line set-up and calibration. The second use case is intended to utilise data from the first to support semi-automatic or automatic re-calibration of machine parameters with a view to preventing defects, a task which normally is largely manually executed. The objectives of this use case are quick defect detection responses with automatic and semi-automatic re-calibrations that are supported by operators utilising tablets and augmented reality tools. This use case will be supported by sensor devices, augmented reality and wearables, and AI tools.

UC-3 Production Planning. This use case will re-create the manufacturing environment in an interactive digital twin platform and facilitate connectivity between real world and virtual machines to enable rapid remote set-up. The objectives are to enable interaction between digital twins of the production line, simulation and testing of alternative set-ups to reach optimal solutions, and applying the optimal set up to the production line. This task will be supported through the use of sensor data, digital twin tools and tablets and augmented reality devices.

The details of the use cases and the deployed technologies have informed the results of UAB and TRI's ethical and legal analysis at each step of the ethics and legal work carried out in WP7 and WP9. What follows is an overview of some of the national legal parameters, observing which will maximise the respect for the rights and welfare of persons affected by OPTIMAI research activities undertaken in the context of these use cases.

5.3 Data Protection Law

Whilst the UK is no longer a member of the European Union (EU), the GDPR remains implemented within UK law, alongside the Data Protection Act (DPA) 2018 [21]. The key provisions outlined in the previous section remain applicable to all businesses operating in the United Kingdom. As such, data protection in the UK is still governed by the principles of:

- lawfulness, fairness, and transparency

- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality
- accountability.

Correspondingly, the rights of the data subject remain enshrined in UK law including:

- the right to information
- the right of access
- the right to rectification
- the right to erasure
- the right to restriction of data protection
- the right to data portability
- the right to object
- the right to avoid automated decision-making.

The UK Information Commissioner's Office (ICO) has provided specific guidance with regards to data protection in the employment context. It will be especially useful for UK based partner MTCL to bear in mind these best practice guidelines for satisfactorily implementing data protection requirements into workplace data processing activities, particularly with regards to OPTIMAI research and dissemination, communication, and exploitation activities.

5.3.1 Data Protection in the Employment Context and other ICO Guidance

The UK Information Commissioner's Office (ICO) has published comprehensive guidance relating to data protection in the work place in The Employment Practices Code. The Code has not been updated since the passing and implementation of the DPA 2018 and an updated version is expected, nevertheless the document is still presented as fit for media consumption and provides useful guidance that can support data protection related decision-making in the employment context [22]. A complete summary of the Code will not be provided here, however key points with possible relevance to OPTIMAI activities will be overviewed.

5.3.1.1 Employee Consultation

The UK ICO recommends that employees and/or trade unions be consulted about the development and implementation of practices and procedures that involve personal data processing in relation to employees [22].

5.3.1.2 Employees' Right to Access

Employees' have access rights to any information concerning them, subject to restrictions as already laid out and to be elaborated in the following subsection. If any identifiers (including names etc.) are processed about workers over the course of OPTIMAI, for example, the employee will usually be entitled access to this. The ICO recommends that the data controller informs the employee about any records held about them; that the employee is provided a description of the types of information processed as well as the purposes for which it is

processed and other organisations with whom it might be shared; that all information about them is shared in intelligible and clear form; that the information is provided in a hard copy or readily readable form or permanent electronic form; and any other information the controller has about the source of the information [22]. The data controller must also be able to verify the identity of those making subject access requests [22].

5.3.1.3 Collection of Information about Employees

The ICO recommends that newly appointed employees (or existing employees where this has not been done) are made aware of the nature and source of information stored about them, how it will be used and to whom it will be disclosed as well as their rights relating to it [22]. There should be a “clear and foreseeable” need for any data held about employees [22]. Employees should be provided with copies of their information subject to change so that it can be kept accurate and up to date [22].

Notably, the ICO states that consent is usually not necessary for keeping employees records [22]. In fact, the ICO states that consent is inappropriate if genuine choice over how data will be used cannot be offered and provides the specific example of a relevant inappropriate case [23]:

you are in a position of power over the individual – for example, if you are a public authority or an employer processing employee data

The ICO makes clear that consent is invalid in such a relationship as the data subject may fear adverse consequences for not consenting to the data processing operation [23]. Again, legitimate interest may be a preferable alternative, although this does not rule out consent for data processing relating to minor matters where free choice can be demonstrated [23].

5.3.1.4 Security

The ICO recommends applying security standards¹⁹ that take into account various risks to data subjects including from unauthorised access to, accidental loss of and destruction or damage to their data [22]. It is recommended that systems are designed such that only persons with legitimate interest can access personal data, and that audit trails are established on automated systems to log who accesses personal data [22].

5.3.1.5 Equal Opportunities Monitoring

The ICO emphasises that information pertaining to workers’ ethnic origin, disability, religion or sexual orientation that may be required for equal opportunities monitoring is sensitive data subject to sensitive data conditions [22]. Identifiable information should only be used for meaningful equal opportunities monitoring and should be anonymised otherwise [22]. Equal opportunities monitoring may be required in OPTIMAI in order to support the diversity of research participants.

5.3.1.6 Publication of Personal Data

The ICO recommends the following conditions when publishing information about employees; that there should be a legal obligation to do so; the information should not be clearly intrusive;

¹⁹ All partners are advised to adhere to the ISO 27001 standard.

consent should be obtained by the employee; or the information is in a form that does not identify the employee [22]. Data controllers should balance the publication of this information against employees' reasonable expectations, and where consent is a valid basis should ensure that employees are aware of the extent of the information published, how it will be published and the implications of its publication [22].

5.3.1.7 Monitoring of Employees

The Code offers guidance around monitoring, which it defines more severely as systematic data processing that relates to quality and performance monitoring [22]. Monitoring may include audio and video monitoring. OPTIMAI activities are not envisioned to entail systematic monitoring with regards to quality and performance of employees. Nevertheless, important lessons can be applied.

The ICO suggests clearly identifying the purposes and benefits of monitoring, potentially utilising a DPIA to evaluate adverse impacts [22]. Employees (or others inadvertently caught by monitoring) should be informed of any monitoring taking place, and why [22]. If sensitive information is collected, a sensitive data condition should be met [22]. The number of persons with access to monitoring information should be limited, and subject to security and confidentiality requirements [22]. Information obtained from monitoring should not be used in ways other than the purpose of the monitoring unless it is in the data subject's interest or regarding activity the employer could not be expected to ignore [22]. Additionally, if the information could adversely affect an employee, they should be presented with the information and allowed to make representations [22].

5.3.2 Exemptions

5.3.2.1 Sensitive Data Conditions

Article 9 of the UK GDPR sets out the conditions of processing special categories of personal data, which are, to reiterate, "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

These sensitive data processing conditions include where processing is by or for or based on [24]:

- (a) Explicit consent
- (b) Employment, social security and social protection (if authorised by law)
- (c) Vital interests
- (d) Not-for-profit bodies
- (e) Made public by the data subject
- (f) Legal claims or judicial acts
- (g) Reasons of substantial public interest (with a basis in law)

- (h) Health or social care (with a basis in law)
- (i) Public health (with a basis in law)
- (j) Archiving, research and statistics (with a basis in law)

Further conditions are outlined in Part 1 (b, h, i, j) and Part 2 (substantial public interest) Schedule 1 of the DPA 2018 [24].

Notably relevant to OPTIMAI, in relation to (b) above, the condition for processing is met where, according to Part 1 Schedule 1 it is necessary for the exercise of legal obligations or rights in connection with employment, social security or protection and where an appropriate policy document is put in place by the data controller. Additionally, Schedule 1 lays out research conditions, where the processing is “necessary for archiving purposes, scientific or historical research purposes or statistical purposes”.

Where reasons of substantial public interest are used as conditions for processing, according to Schedule 1 Part 2, an appropriate policy document must be in place.

Schedule 1 Part 2 lays out reasons of substantial public interest. Perhaps the most relevant condition here is processing for equality of opportunity or treatment, which “is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained”. Exclusions to this basis include:

- where it is carried out for the purposes of measures or decisions with respect to a particular data subject
- it is likely to cause substantial damage or substantial distress to an individual
- an individual who is the data subject (or one of the data subjects) has given notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject (and has not given notice in writing withdrawing that requirement)
- the notice gave the controller a reasonable period in which to stop processing such data, and that period has ended.

5.3.2.2 Exemptions in Relation to Freedom of Expression, and Information; and for Research, Statistics, and Archiving in the Public Interest

The UK DPA 2018 Schedule 2 Part 5 lays out exemptions to the following UK GDPR articles in relation to reasons of freedom of expression, and information:

- Article 5(1)(a) to (e) (principles relating to processing)
- Article 6 (lawfulness)
- Article 7 (conditions for consent)
- Article 8(1) and (2) (child's consent)
- Article 9 (processing of special categories of data)
- Article 10 (data relating to criminal convictions etc)
- Article 11(2) (processing not requiring identification)

- Article 13(1) to (3) (personal data collected from data subject: information to be provided)
- Article 14(1) to (4) (personal data collected other than from data subject: information to be provided)
- Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers)
- Article 16 (right to rectification)
- Article 17(1) and (2) (right to erasure)
- Article 18(1)(a), (b) and (d) (restriction of processing)
- Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing)
- Article 20(1) and (2) (right to data portability)
- Article 21(1) (objections to processing)
- Article 34(1) and (4) (communication of personal data breach to the data subject)
- Article 36 (requirement for controller to consult Commissioner prior to high risk processing)
- Article 44 (general principles for transfers)

The exemptions are based on reasons of “special purposes” which can refer to purposes of journalism; academia; art; or literature. The aforementioned GDPR provisions do not apply where the “controller reasonably believes that the application of those provisions would be incompatible with the special purposes”. The UK ICO highlights that such exemptions are also available only where; the processing is conducted with a view to publication of journalistic, artistic, or literary material; and that the material would be in the public interest taking into account matters including potential harm to the data subject [25]. If any exemptions are pursued, the data controller should be able to explain why, how and by whom the decision was made [25].

The UK ICO highlights that such exemptions are available only where “compliance with these provisions would be incompatible with the special purposes”; the processing is conducted with a view to publication of journalistic, artistic, or literary material; and that the material would be in the public interest taking into account matters including potential harm to the data subject [25].

Similarly, the UK DPA 2018 Schedule 2 Part 6 lays out exemptions (derogations) to provisions of the UK GDPR based on purposes of research, statistics and archiving, especially “scientific or historical research purposes,” or “statistical purposes”.

The provisions subject to derogation are:

- Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers)
- Article 16 (right to rectification)
- Article 18(1) (restriction of processing)
- Article 21(1) (objections to processing)

The UK ICO highlights that these exceptions apply only to the extent that compliance would prevent or seriously impair achieving the purposes of the processing; processing is subject to

appropriate safeguards for data subjects' rights and freedoms; where processing is not likely to cause substantial damage or distress to individuals; where it is not used for decisions about particular individuals (unless it is for approved medical research); and in relation to right of access, results are not made available in a manner that identifies individuals [25].

For archiving in the public interest, exemptions to the following provisions are available:

- Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);
- Article 16 (right to rectification)
- Article 18(1) (restriction of processing)
- Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing)
- Article 20(1) (right to data portability)
- Article 21(1) (objections to processing)

The UK ICO highlights that these exemptions only apply, again, where compliance would prevent or seriously impair achieving the purposes of the processing; where safeguards are in place to protect the rights and freedoms of data subjects; where it is not likely to cause substantial harm or distress to individuals; and where it is not used to make decisions about individuals (excepting authorised medical research) [25].

5.3.2.3 Appropriate Policy Document

Many (all with regards to Schedule 1 Part 2) exemptions will require that the data controller have an appropriate policy document in place. Part 4 of Schedule 2 outlines the content that such a policy document should include. The appropriate policy document should explain the controller's procedures for complying with the principles of the GDPR with reference to the data processing conditions as previously discussed as well as the controller's policies with regards to the retention and erasure of data processed under those conditions. This document should be reviewed as necessary. The document should be retained for 6 months after the relevant data processing operations have ceased.

5.4 Employment Law

Workers' rights in the United Kingdom are enshrined in and protected under the law through the Employment Rights Act (ERA) 1996. The Act enshrines various protections including for employees' wages, protection against unjustified detriment at work, protection from unfair dismissal, time-off work etc.

It is incumbent on all partners, especially end-user partners as employers, to ensure that any interactions with and requirements of UK employees arising as a result of OPTIMAI research and pilot activities do not endanger employees' enjoyment of the rights enshrined in British Law.

Employers have extensive obligations under the Employment Rights Act 1996 which they are expected to honour in full. Every requirement arising as a result of the employer-employee relationship cannot be summarised here, however this section will pay particular attention to

those with relevance to the kind of responsible and lawful research which the project seeks to uphold.

Such points of interest that warrant particular attention include:

- protected disclosures
- health and safety
- right not to be unfairly dismissed.

These core points warrant particular attention as it is imperative that OPTIMAL research and pilot activities do not threaten or undermine pilot site employees' safety, job security, or job quality and in order to ensure that OPTIMAL partners are appropriately accountable for safeguarding worker welfare to the extent that their activities impact their experiences at work.

5.4.1 Protected Disclosures

Part IV A of the Employment Rights Act (ERA) 1996 sets out the meaning and detail of protected disclosures. The ERA 1996 protects the workers from victimisation when they make protected disclosures to actors recognised/prescribed by law [26]. A qualifying disclosure can be made where the worker makes a disclosure in the reasonable belief, and in the public interest, one or more of the following as set out in Section 43B(1):

- that a criminal offence has been committed, is being committed or is likely to be committed
- that a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject
- that a miscarriage of justice has occurred, is occurring or is likely to occur
- that the health or safety of any individual has been, is being or is likely to be endangered
- that the environment has been, is being or is likely to be damaged, or
- that information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

The protection offered to employees is explicitly laid out in Part V Section 47B of the ERA 1996, which states that "[a] worker has the right not to be subjected to any detriment by any act, or any deliberate failure to act, by his [the employee's] employer done on the ground that the worker has made a protected disclosure". Section 47B(1A) prohibits employees from suffering detriment by any act or omission by their employers' or an agent/other worker (proxy) of the employer on the basis of the disclosure.

If UK employees who are participating in or are otherwise affected by OPTIMAL research and pilot activities make a qualifying disclosure based on a critical failure, the ERA 1996 protects them from adverse or detrimental consequences by their employer (or proxy). To that end, accountability and transparency should be promoted.

5.4.2 Health and Safety

Part V Section 44 of the ERA 1996 protects the worker from detriment because of specific matters relating to health and safety. This prohibits the detrimental treatment of workers involved

(through designation) in health and safety activities or from bringing health and safety concerns to the employer.

The Act protects workers:

- in circumstances of danger which the worker reasonably believed to be serious and imminent and which he or she could not reasonably have been expected to avert, he or she left (or proposed to leave) or (while the danger persisted) refused to return to his or her place of work or any dangerous part of his or her place of work, or
- in circumstances of danger which the worker reasonably believed to be serious and imminent, he or she took (or proposed to take) appropriate steps to protect himself or herself or other persons from the danger.

Part X Section 100 also expressly prohibits termination of employees on these grounds.

As such, any employees that raise health and safety concerns relating to OPTIMAI research and pilot activities, and take any reasonable steps to protect themselves or others or refuse to work in resulting dangerous conditions, are protected from dismissal and other detriments through any act or omission.

5.4.3 Unfair Dismissals

The OPTIMAI Consortium cannot condone any unjustifiable dismissals of employees participating in or affected by research and pilot activities. The ERA 1996 Part X sets out the right not to be unfairly dismissed. Section 98 lays out points determining whether a dismissal is fair or unfair. An employer will be required to present a justifiable reason for dismissal, based on grounds including capability, qualification, conduct, or redundancy etc. Many possible reasons for fair or unfair dismissal will be completely unrelated to OPTIMAI activities. Nevertheless, it should be noted that protected disclosures and health and safety cases as described above are not grounds for dismissal and would be considered unfair.

5.5 Equality Law

The OPTIMAI Consortium has acknowledged the importance of inclusive research practices and is aware of its obligation to support diverse and inclusive workspaces that are free from discrimination, harassment, and victimisation. In the context of OPTIMAI research and pilot activities, partners, especially end-users, must strive to protect the rights of all employees without discrimination and may need to make accommodations for particular employees where they have protected characteristics.

Non-discrimination protections fall under the framework of the Equality Act 2010 in the UK. The following subsections will explore particular aspects of this legislation with relevance for OPTIMAI partners, including:

- protected characteristics and definitions
- discrimination, harassment, and victimisation in relation to employment
- adjustments for persons with disabilities.

5.5.1 Protected Characteristics

The characteristics protected by the Equality Act 2010 are enumerated in Part 2 Section 4 and include:

- Age
- Disability
 - a person (P) will be regarded as having a disability where “P has a physical or mental impairment, and...the impairment has a substantial and long-term adverse effect on P's ability to carry out normal day-to-day activities”.
- Gender Reassignment
 - where P “...is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex”.
- Marriage and Civil Partnership
- Pregnancy and Maternity
- Race
 - where race includes colour, nationality, or ethnic or national origins
- Religion or Belief
- Sex
- Sexual Orientation

5.5.2 Discrimination, Harassment, and Victimisation in Relation to Employment

Part 2 Chapter 2 of the Act sets out criteria relating to direct and indirect discrimination against persons based on their protected characteristics.

Part 2 Section 15 of the Act defines discrimination as occurring where “[a] person (A) discriminates against another (B) if, because of a protected characteristic, A treats B less favourably than A treats or would treat others”.

Part 2 Section 19 defines indirect discrimination as occurring where “A person (A) discriminates against another (B) if A applies to B a provision, criterion or practice which is discriminatory in relation to a relevant protected characteristic of B's”, and where something constitutes discriminatory if:

- A applies, or would apply, it to persons with whom B does not share the characteristic,
- it puts, or would put, persons with whom B shares the characteristic at a particular disadvantage when compared with persons with whom B does not share it
- it puts, or would put, B at that disadvantage, and
- A cannot show it to be a proportionate means of achieving a legitimate aim.

Part 2 Section 26 of the Act sets out criteria with reference to harassment, where harassment is defined as a situation where:

- A engages in unwanted conduct related to a relevant protected characteristic, and
- the conduct has the purpose or effect of—
 - violating B's dignity, or

- creating an intimidating, hostile, degrading, humiliating or offensive environment for B.

Part 2 Section 27 of the Act sets out criteria with reference to victimisation, where victimisation is defined as a situation where:

- A person (A) victimises another person (B) if A subjects B to a detriment because—
 - B does a protected act²⁰, or
 - A believes that B has done, or may do, a protected act.

Part 5 Sections 39-60 of the Act outline discrimination, harassment and victimisation prohibitions in the employment context. Succinctly, employers cannot discriminate or victimise persons when offering or setting terms of employment or promotion, transfer and training based on protected personal characteristics.

It should be noted that any acts of discrimination, harassment and victimisation can be more widely construed and could be applicable to any unjustifiable distinctions (or responses to complaints) made between persons with different or combined protected characteristics in relation to project participants and their role in OPTIMAI project activities (for example, recruitment and selection processes for research participants). Indirect discrimination may also apply where research activities disadvantage persons based on their personal characteristics in ways that do not satisfy a legitimate aim (perhaps the absolute requirement of testing equipment incompatible with disability where no reasonable effort is made to accommodate that disability).

Schedule 9 of the Act lays out exemptions, notably that work requirements with discriminatory effects can be exempt where:

- it is an occupational requirement
- the application of the requirement is a proportionate means of achieving a legitimate aim, and
- the person to whom A applies the requirement does not meet it (or A has reasonable grounds for not being satisfied that the person meets it).

5.5.3 Adjustments for Persons with Disabilities

Part 2 Section 20 of the Act enshrines a duty to make reasonable adjustments for persons based on their disability. This duty is based on three requirements:

- the first requirement is a requirement, where a provision, criterion or practice of A's puts a disabled person at a substantial disadvantage in relation to a relevant matter in comparison with persons who are not disabled, to take such steps as it is reasonable to have to take to avoid the disadvantage
- the second requirement is a requirement, where a physical feature puts a disabled person at a substantial disadvantage in relation to a relevant matter in comparison with

²⁰ Where a protected act refers to complaints and related procedures.

persons who are not disabled, to take such steps as it is reasonable to have to take to avoid the disadvantage

- the third requirement is a requirement, where a disabled person would, but for the provision of an auxiliary aid, be put at a substantial disadvantage in relation to a relevant matter in comparison with persons who are not disabled, to take such steps as it is reasonable to have to take to provide the auxiliary aid.

As such, employers are expected to make reasonable accommodations for persons based on their disability, and end-user partners should evaluate whether any such adjustments can be applied to OPTIMAI research and pilot activities.

5.6 Health and Safety Law

The health and safety of OPTIMAI end-user workers is paramount, and ensuring their continued safety and welfare over the course of OPTIMAI research and pilot activities should be a priority. There are many and extensive laws and regulations governing safe working environments in the UK and end-user partners are expected to comply with all applicable legislation. Notable acts and instruments protecting worker health and safety include, but are not limited to, the Health and Safety at Work etc. Act 1974; The Management of Health and Safety at Work Regulations 1999; The Health and Safety (Consultation with Employees) Regulations 1996; and the Factories Act 1961. A more extensive list of sources is presented in **Appendix A: OPTIMAI Pilot National Legal Framework**.

We cannot overview all requirements entailed by these acts and others, however in support of the safe conduct of research and pilot activities arising from the OPTIMAI project and environments in which they take place, particular key matters will be outlined including:

- general duties of employers as specified in Health and Safety at Work etc. Act 1974
- general health and safety requirements with regards to working environment and equipment
- general provisions on welfare
- risk assessment requirements
- employee duties, capabilities and training
- duty of consultation

5.6.1 General Duties of Employers as Specified in Health and Safety at Work etc. Act 1974

Section 2 of Part 1 of the Health and Safety at Work etc. Act (HSWA) 1974 lays out the general health and safety related duties of employers to their employees, and may be viewed as the cornerstone of UK health and safety legislation. The core duties enumerated are:

- the provision and maintenance of plant and systems of work that are, so far as is reasonably practicable, safe and without risks to health
- arrangements for ensuring, so far as is reasonably practicable, safety and absence of risks to health in connection with the use, handling, storage and transport of articles and substances

- the provision of such information, instruction, training and supervision as is necessary to ensure, so far as is reasonably practicable, the health and safety at work of his [the employer's]²¹ employees
- so far as is reasonably practicable as regards any place of work under the employer's control, the maintenance of it in a condition that is safe and without risks to health and the provision and maintenance of means of access to and egress from it that are safe and without such risks
- the provision and maintenance of a working environment for his [the employer's] employees that is, so far as is reasonably practicable, safe, without risks to health, and adequate as regards facilities and arrangements for their welfare at work.

As MTCL is a manufacturer, it also holds particular responsibilities for articles and substances which are covered by Section 6. This provision generally requires:

- that all articles, substances (and fairground equipment) for use at work are designed and constructed (or installed) for safe use at work and while being maintained, handled, processed and stored. Notably, the statutory instrument The Provision and Use of Work Equipment Regulations 1992 requires that "[e]very employer shall ensure that work equipment is so constructed or adapted as to be suitable for the purpose for which it is used or provided"
- testing and examining is performed to verify the preceding
- information to be provided concerning safe use of the articles and substances and subsequent revisions.

As OPTIMAI partners will be supplying equipment for use by workers, they should support MTCL in compliance with safe use of that equipment through provision of safe equipment with clear and accessible safety information.

5.6.2 General Health and Safety Requirements with Regards to Working Environment and Equipment

OPTIMAI partners and especially end-users should strive towards the provision of safe working environments that pose minimal risks to the health and safety of research participants and those affected by the project's research and pilot activities. The Factories Act (FA) 1961 extensively sets out requirements for safe working environments that adequately protect the health and safety of employees. The OPTIMAI Consortium cannot condone situations where worker health and safety is not a high priority, and recognises that it should not alter current working environments or processes in any manner that would compromise employee health and safety.

FA 1961 Part 1 Section 1 sets out duties of cleanliness of working environments by employers, requiring removal of dirt and refuse daily; and weekly sweeping or washing of floors; and regular and revarnishing or painting and washing of walls.

²¹ The Act (and others) uses male pronouns in reference to employers and employees, we have added [the employer] and [the employee] respectively and where applicable in recognition that an employer or employee's gender is not predetermined.

FA 1961 Part 1 Section 2 prohibits overcrowding of the working environment, stating that “the number of persons employed at a time in any workroom shall not be such that the amount of cubic space allowed for each is less than 11 cubic metres”.

FA 1961 Part 1 Section 3 requires rooms to be at a reasonable temperature, with a thermometer provided, and such that methods used to maintain temperature do not result in the escape of dangerous fumes. Where the work consists largely of sitting and little physical effort, a temperature of less than 16 degrees Celsius is not considered reasonable after the first hour. Section 4 requires suitable ventilation for workrooms.

FA 1961 Part 1 Section 5 requires that suitable lighting be provided in the working environment, including requiring that windows be kept clean and free of obstruction.

FA 1961 Part 1 Section 6 requires effective drainage of rooms that are liable to be rendered wet by any process.

FA 1961 Part 2 Section 18 regulates workroom safety with regards to dangerous substances. UK end-user partner MTCL’s processes are not known to involve scalding, corrosive, or poisonous substances kept in any manner of pit. Nevertheless, this article requires that such substances are secured and adequate barriers and workplace design are in place to protect employees from exposure. In situations where employees are exposed to hazardous substances, the statutory instrument The Control of Substances Hazardous to Health Regulations 1988 requires health surveillance.

FA 1961 Part 2 Section 28 requires that floors, passages and stairs be kept properly maintained and unobstructed and free of substances that could cause slipping. This also requires adequate rails and fencing for stairs and floors. Section 29 requires safe access to each place of work, and safety measures where persons are liable to fall a distance greater than 2 meters.

FA 1961 Part 2 Sections 31 and 32 deal with health and safety requirements with regards to explosive or inflammable dust, gas, vapour or substances and steam boilers. The Act requires that processes involving dust liable to explode take place in an enclosed plant, sources of ignition be enclosed or removed, and dust be removed or prevented from accumulating. Steps should be taken to prevent the spread of effects from possible explosions. Areas containing explosive or “[i]nflammable gas or vapour under pressure greater than atmospheric pressure” are subject to stringent requirements, for instance requiring appropriate stoppage valves and precluding cutting and heating processes without adequate precautions. Steam boilers are to be properly maintained and no new boilers should be put into service without obtaining relevant specification certification from appropriate suppliers or actors.

The statutory instrument, The Personal Protective Equipment at Work Regulations 1992, requires the provision of personal protective equipment where there are risks to health and safety of employees where such risks are not mitigated adequately by other measures, and such equipment should be compatible with and sufficient to protect against the risks. The equipment is to be properly maintained and training and instruction provided on its use.

The statutory instrument The Provision and Use of Work Equipment Regulations 1992 requires that adequate measures be put in place to protect workers from machinery including through use of protective devices, etc. as well as provision of health and safety information and instructions of use of the equipment, and maintenance of the equipment.

The Regulatory Reform (Fire Safety) Order 2005 requires that workplaces have adequate and unobstructed emergency exits that are clearly marked and lead to safety.

5.6.3 General Provisions on Worker Welfare

As well as ensuring the health and safety from physical risks in the workplace, UK law also sets out the conditions for welfare of the employee in the workplace. The OPTIMAI Consortium and end-users in particular should ensure that the material needs and conveniences of workers are met as laid out in the Factories Act 1961 and any other acts or regulations.

The FA 1961 enjoins employers to provide suitable points for drinking water from a public main or sources approved by the District Council; adequate washing facilities; accommodation for clothing not worn during working hours; and sitting facilities where workers can do so without detriment to their work.

Additionally, the statutory instrument The Health and Safety (First-Aid) Regulations 1981 places upon employers a duty to provide equipment and facilities to render employees with first-aid and a sufficient number of trained individuals are available to provide the first-aid. Employees should be informed of first-aid arrangements including the location of equipment, facilities, and relevant personnel.

5.6.4 Risk Assessment and Management Requirements

The statutory instrument, The Management of Health and Safety at Work Regulations 1999, sets out extensive risk assessment requirements for employers which need to be adhered to by OPTIMAI end-users, in order to ensure the safety of the workplace, particularly emerging from any changes to processes, the environment, or equipment uses, stemming from OPTIMAI research and pilot activities.

The Regulation (Regulation 3) requires that the employer make suitable and sufficient assessment of:

- the risks to the health and safety of his [the employer's] employees to which they are exposed whilst they are at work; and
- the risks to the health and safety of persons not in his [the employer's] employment arising out of or in connection with the conduct by him [the employer] of his [the employer's] undertaking.

Measures should be implemented to mitigate the risks identified, with Regulation 6 enshrining a duty of health surveillance in relation to identified risks.

The risk assessment should be reviewed where there is reason to suspect that it may no longer be valid or there has been a significant change in the matters it relates to. As OPTIMAI activities

may change the material circumstances within the working environment, a risk assessment should be conducted unless the end-user can offer compelling justification for not doing so.

Schedule 1 of the Regulation outlines the principles of prevention that should be followed in managing health and safety risks, which are:

- avoiding risks
- evaluating the risks which cannot be avoided
- combating the risks at source
- adapting the work to the individual, especially as regards the design of workplaces, the choice of work equipment and the choice of working and production methods, with a view, in particular, to alleviating monotonous work and work at a predetermined work-rate and to reducing their effect on health
- adapting to technical progress
- replacing the dangerous by the non-dangerous or the less dangerous
- developing a coherent overall prevention policy which covers technology, organisation of work, working conditions, social relationships and the influence of factors relating to the working environment
- giving collective protective measures priority over individual protective measures; and
- giving appropriate instructions to employees.

Regulation 7 requires the appointment of competent persons to assist them “in undertaking the measures he [the employer] needs to take to comply with the requirements and prohibitions imposed upon him [the employer] by or under the relevant statutory provisions”, and such person(s) should be informed of all factors affecting the health and safety of workers.

Regulation 10 enshrines transparency requirements, whereby employees should be informed with relevant and comprehensible information about:

- the risks to their health and safety identified by the assessment
- the preventive and protective measures
- the procedures referred to in regulation 8(1)(a)²²
- the identity of those persons nominated by him in accordance with regulation 8(1)(b)²³
- the risks notified to him [the employee] in accordance with regulation.

The Regulatory Reform (Fire Safety) Order 2005 similarly requires risk assessment to be conducted with regards to fire hazards, along with the requirement to eliminate risks and appoint responsible persons and make appropriate arrangements.

5.6.5 Employee Duties, Capabilities and Training

²² “[E]stablish and where necessary give effect to appropriate procedures to be followed in the event of serious and imminent danger to persons at work in his undertaking”.

²³ “[N]ominate a sufficient number of competent persons to implement those procedures in so far as they relate to the evacuation from premises of persons at work in his undertaking”.

The OPTIMAL Consortium understands that employees will also hold health and safety duties, and should be supported in performing them especially as they relate to the safe conduct of research and pilot activities.

The HSWA 1974 Part 1 Section 7 lays out these duties, whereby each employee has the duty:

- to take reasonable care for the health and safety of himself [the employee] and of other persons who may be affected by his [the employee's] acts or omissions at work; and
- as regards any duty or requirement imposed on him [the employee's] employer or any other person by or under any of the relevant statutory provisions, to co-operate with him [the employer] so far as is necessary to enable that duty or requirement to be performed or complied with.

Furthermore, the Management of Health and Safety at Work Regulations 1999 Regulation 14 requires that:

Every employee shall use any machinery, equipment, dangerous substance, transport equipment, means of production or safety device provided to him [the employee] by his [the employee's] employer in accordance both with any training in the use of the equipment concerned which has been received by him [the employee] and the instructions respecting that use which have been provided to him [the employee] by the said employer in compliance with the requirements and prohibitions imposed upon that employer by or under the relevant statutory provisions.

The Regulation also imposes reporting duties on employees to inform the employer or responsible person of health and safety risks or any shortcomings in responses to risks.

Regulation 13 requires that each employee be provided adequate health and safety training upon being recruited or being exposed to new risks, notably, because of:

- the introduction of new work equipment into or a change respecting work equipment already in use within the employer's undertaking
- the introduction of new technology into the employer's undertaking.

This training should:

- be repeated periodically where appropriate
- be adapted to take account of any new or changed risks to the health and safety of the employees concerned; and
- take place during working hours.

The Regulatory Reform (Fire Safety) Order 2005 also makes the employer responsible for providing training with regards to fire safety.

5.6.6 Duty of Consultation

The statutory instrument The Safety Representatives and Safety Committees Regulations 1977 allows trade unions to appoint a safety representative to represent employees, who shall, according to Regulation 4, have functions:

- to investigate potential hazards and dangerous occurrences at the workplace (whether or not they are drawn to his [the representative's] attention by the employees he [the representative] represents) and to examine the causes of accidents at the workplace
- to investigate complaints by any employee he [the representative] represents relating to that employee's health, safety or welfare at work
- to make representations to the employer on matters arising out of sub-paragraphs (a) and (b) [of Regulation 4(1)]²⁴
- to make representations to the employer on general matters affecting the health, safety or welfare at work of the employees at the workplace
- to carry out inspections in accordance with Regulations 5, 6 and 7²⁵...
- to represent the employees he [the representative] was appointed to represent in consultations at the workplace with inspectors of the Health and Safety Executive and of any other enforcing authority
- to receive information from inspectors in accordance with section 28(8)²⁶ of the 1974 Act; and
- to attend meetings of safety committees where he attends in his [the representative] capacity as a safety representative in connection with any of the above functions.

The Health and Safety (Consultation with Employees) Regulations 1996 Regulation 3 requires that where there are employees who are not represented, they are to be consulted about matters relating to their health and safety in relation to:

- the introduction of any measure at the workplace which may substantially affect the health and safety of those employees

²⁴ These paragraphs are:

(a) to investigate potential hazards and dangerous occurrences at the workplace (whether or not they are drawn to his attention by the employees he represents) and to examine the causes of accidents at the workplace;

(b) to investigate complaints by any employee he represents relating to that employee's health, safety or welfare at work

²⁵ These regulations relate to inspections of the workplace; inspections following notable accidents; and the inspection of documents and provision of information. More detail can be found here: <https://www.legislation.gov.uk/ukxi/1977/500/contents/made>

²⁶ To quote:

Notwithstanding anything in the preceding subsection an inspector shall, in circumstances in which it is necessary to do so for the purpose of assisting in keeping persons (or the representatives of persons) employed at any premises adequately informed about matters affecting their health, safety and welfare, give to such persons or their representatives the following descriptions of information, that is to say—

(a) factual information obtained by him as mentioned in that subsection which relates to those premises or anything which was or is therein or was or is being done therein; and

(b) information with respect to any action which he has taken or proposes to take in or in connection with those premises in the performance of his functions;

and, where an inspector does as aforesaid, he shall give the like information to the employer of the first-mentioned persons.

- his [the employer's] arrangements for appointing or, as the case may be, nominating persons in accordance with regulations 6(1) and 7(1)(b) of the Management of Health and Safety at Work Regulations 1992²⁷
- any health and safety information he [the employer] is required to provide to those employees by or under the relevant statutory provisions
- the planning and organisation of any health and safety training he [the employer] is required to provide to those employees by or under the relevant statutory provisions; and
- the health and safety consequences for those employees of the introduction (including the planning thereof) of new technologies into the workplace.

The Regulatory Reform (Fire Safety) Order 2005 also enshrines duties of consultation with regards to fire safety.

5.7 UK Data protection, Employment and Equality, and Health and Safety Law Requirements

5.7.1 United Kingdom (UK) – Data Protection Law Requirements

Table 15 UK Lawful Basis Requirements

ID	UKDP-LB	Requirement	Lawful Basis (LB)
Description	Utilise an appropriate lawful basis for each data processing operation associated with OPTIMAI pilot activities.		
Implementation in OPTIMAI	<p>UK-LB-01. Consent will only be an appropriate legal basis for data processing where it is freely given, specific, informed and given by unambiguous agreement. Data subjects should be able to withdraw this consent at any time. In the employment or workplace context, the consent of employees may only be valid for minor matters where free choice can be demonstrated [23], such as image publication in deliverables or media releases. Other data subjects to consider include pilot site visitors subject to data collection.</p> <p>UK-LB-02. Consent should not be relied upon in cases where there is a clear power imbalance between data subject and controller/processor, such as the employer-employee relationship, where genuine free choice cannot be demonstrated. MTCL operators and other employees who are piloting OPTIMAI technologies or are within range of personal data collecting sensor devices, or are otherwise required to supply personal data over the course of research activities, are unlikely to be in a position to provide appropriate consent.</p>		

²⁷For more detail, please see <https://www.legislation.gov.uk/ukxi/1992/2051/contents/made>

	<p>UK-LB-03. In cases where consent cannot be relied upon, data controllers should consider whether legitimate interest or another basis is an appropriate lawful basis for data processing. A balancing test should be performed and documented with the assistance of a legitimate interest assessment. MTCL and others identified as data controllers should conduct this legitimate interest assessment in advance of processing personal data in relation to pilot activities.</p> <p>UK-LB-04. Where consent is inappropriate, data controllers should ensure that data processing activities are of a nature that could reasonably be expected by employees.</p>
--	---

Table 16 UK Special Categories of Data Requirements

ID	UK-SCD	Requirement	Special Categories of Data (SCD)
Description		The processing of special categories of data in connection with OPTIMAI pilot activities shall be prohibited without appropriate justification and safeguards, and as subject to specific exemptions (see Subsection 5.3.2 Exemptions).	
Implementation in OPTIMAI		<p>UK-SCD-01. Consent for the processing of special categories of personal data should be explicit, freely given, specific, informed and given by unambiguous agreement. Data subjects should be able to withdraw this consent at any time. In the employment or workplace context, the consent of employees may not be valid.</p> <p>UK-SCD-02. Consent for processing of special categories of data should not be relied upon in cases where there is a clear power imbalance between data subject and controller/processor, such as the employer-employee relationship, where genuine free choice cannot be demonstrated. MTCL operators and other workers pilot OPTIMAI technologies or are within range of personal data collecting sensor devices, or are otherwise required to supply personal data over the course of research activities, are unlikely to be in a position to provide appropriate consent for processing special categories of data.</p> <p>UK-SCD-03. In OPTIMAI, special categories of personal data may be processed for purposes including public interest, scientific or historical research, reasons of substantial public interest, or employment, social security and social protection. The reasons should be appropriately identified and documented. Technical and organisational measures safeguarding the rights of data subjects should be in place.</p>	

	<p>UK-SCD-04. Partners should pay particular regard to the principle of data minimisation, as well as consider pseudonymisation where the data processing purposes permit this.</p> <p>UK-SCD-05. Partners processing sensitive categories of data will be required to have an appropriate policy document. The appropriate policy document should explain the controller's procedures for complying with the principles of the UK GDPR with reference to the data processing conditions as well as the controller's policies with regards to the retention and erasure of data processed under those conditions. This document should be reviewed as necessary. The document should be retained for 6 months after the relevant data processing operations have ceased</p>
--	---

Table 17 UK Data Controller and Processor Requirements

ID	UK-DCP	Requirement	Data Controller and Processor (DCP)
Description		Data controllers and processors should correctly identify themselves and comply with UK GDPR requirements arising as a result of their controllership or by dint of being processor.	
Implementation in OPTIMAI		<p>UK-DCP-01. Consortium partners must identify whether they are data controllers, processors, or party to joint controllerships with regards to specific data processing operations.</p> <p>UK-DCP-02. Data controllers and processors must ensure appropriate security, technical and organisational means are implemented that protect the rights and freedoms of data subjects.</p> <p>UK-DCP-03. Data controllers and processors must implement appropriate data protection policies, as documented in an appropriate policy document where applicable.</p> <p>UK-DCP-04. Joint controllers must transparently determine their respective responsibilities and should designate a contact point for data subjects.</p> <p>UK-DCP-05. Whereby it is determined that a partner is acting as a data processor for a data controller, the relationship must be governed by a</p>	

	<p>contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.</p> <p>UK-DCP-06. Data processors and controllers should keep appropriate records of data processing activities.</p> <p>UK-DCP-07. Data controllers must conduct, at a minimum, data protection impact assessment threshold analyses prior to data processing activities and a DPIA where the outcome of such analysis indicates that data processing is of high risk to data subjects.</p> <p>UK-DCP-08. Data controllers and processors must notify data subjects and the applicable data protection authority of any breach in a timely manner.</p> <p>UK-DCP-09. Data controllers should consult with affected parties ahead of new data processing activities. In the case of MTCL, the end-user partner should consider appropriate consultation with employees or their representatives regarding changes to data processing activities.</p> <p>UK-DCP-10. Data controllers should ensure that data is processed for specific lawful purposes, in line with the principles of data minimisation, and that such data is made available only to persons as necessary for achieving those purposes and should implement audit trails to log who has access to personal data. Further processing should not be undertaken unless exceptions apply. Data should be retained only as long as necessary to achieve their purpose, or as long as required to meet any other legal obligation.</p>
--	--

Table 18 UK Data Subject Rights Requirements

ID	UK-DSR	Requirement	Data Subject Rights (DSR)
Description	To the maximum extent possible, and subject to Exemptions , the rights of OPTIMAI data subject's must be upheld and protected.		

**Implementation
in OPTIMAI**

UK-DSR-01. The data controller is to communicate all relevant information to the data subject (who could be an employee of MTCL or a site visitor, for example) in a concise, transparent, intelligible and easily accessible form, and must be aware that duties apply even where personal data was not collected by the data controller.

UK-DSR-02. The data subject must be notified about data processing activities and be given access to any data held about them and related information including about their rights and purposes of the data processing. The data controller shall implement means to verify the identity of any persons making subject access requests.

UK-DSR-03. The data subject has the right to have incorrect information about them corrected and have incomplete information corrected including by supplementary statement.

UK-DSR-04. The data subject has the right for their data to be erased where it is no longer necessary; consent is withdrawn; they object to processing; the data has been unlawfully processed; etc.

UK-DSR-05. The subject has the right to have data processing restricted where the personal data's accuracy is contested; processing is unlawful and the subject requests restriction rather than erasure; the controller no longer has use for the data but the data subject does (e.g., for a legal claim); or the data subject has objected pending verification of whether the grounds of the controller override the subject's interest.

UK-DSR-06. The data subject has the right to receive their personal data "in a structured, commonly used and machine-readable format and [has] the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided", where the processing is based on consent or is carried out by automated means.

UK-DSR-07. The data subject has the right to object to processing of their personal data and the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

UK-DSR-08. The data subject has the right not to be subject to automated decision-making including profiling with legal (or similar)

	effects. Exceptions arise based on performance of contract, authorisation by law, and where explicit consent is obtained from the data subject.
--	---

Table 19 UK International Data Transfer Requirements

ID	UK-IDT	Requirement	International Data Transfers (IDT)
Description	International data transfers and transfers to international organisations should only take place where the rights and freedoms of data subjects can be ensured, or as subject to exemptions (see Subsection 4.2.7 Transfers of Personal Data to Third Countries or International Organisations).		
Implementation in OPTIMAI	UK-IDT-01. Data controllers and processors must, subject to derogations, transfer data to third countries and international organisations only where there are appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.		

5.7.2 UK – Employment Law Requirements

Table 20 UK Employment Law Requirements

ID	UK-EmR	Requirement	Employment Rights (EmR)
Description	OPTIMAI partners, especially end-users, should not impinge on the employment rights of pilot site workers.		
Implementation in OPTIMAI	<p>UK-EmR-01. End-user employees must not come to any detriment as a result of making qualified disclosures regarding any critical failures arising due to OPTIMAI pilot or research activities.</p> <p>UK-EmR-02. End-user employees must not come to any detriment where they refuse to work within the OPTIMAI pilot testing area due to a reasonable belief that it is dangerous, or because they took reasonable steps to protect themselves or others from this danger.</p> <p>UK-EmR-03. End-users must refrain from unreasonably citing any OPTIMAI related pilot or research activity for terminating the employment of employees.</p>		

5.7.3 UK – Equality Law Requirements

Table 21 UK Equality Law Requirements

ID	UK-EqR	Requirement	Equality Rights (EqR)
Description		All partners, especially the MTCL as end-user partner, must adhere to equality law with respect to the rights of pilot site workers and other applicable individuals.	
Implementation in OPTIMAI		<p>UK-EqR-01. In overseeing and managing OPTIMAI pilot and research activities, partners must refrain from making decisions that would treat individuals less favourably than others on the basis of protected characteristics or would otherwise disadvantage them on that basis. Indicative examples would be an obligation to wear hardware that is incompatible with religious dress, or excluding persons from participation in pilot and research activities on the basis of protected characteristics without legitimate justification.</p> <p>UK-EqR-02. All OPTIMAI partners must refrain from all forms of harassment, discrimination and victimisation both on the grounds of protected characteristics or any other.</p> <p>UK-EqR-03. If any OPTIMAI pilot or research activities or something arising as a result of them would tend towards causing disadvantage to disabled workers in the pilot site, reasonable accommodations should be made to prevent any such disadvantage.</p>	

5.7.4 UK – Health and Safety Law Requirements

Table 22 General Duties of Employers Requirements

ID	UK-GD	Requirement	General Duties of Employers (GD)
Description		MTCL, with the support of partners, is required to discharge duties as outlined in the Health and Safety at Work etc. Act 1974.	
Implementation in OPTIMAI		<p>UK-GD-01. MTCL, and partners if necessary, must collaborate in ensuring the provision and maintenance of plant and systems of work that are, so far as is reasonably practicable, safe and without risks to health.</p> <p>UK-GD-02. MTCL, with the support of partners if necessary, are</p>	

	<p>responsible for making arrangements for ensuring, so far as is reasonably practicable, safety and absence of risks to health in connection with the use, handling, storage and transport of articles and substances.</p> <p>UK-GD-03. MTCL and partners must collaborate in the provision of such information, instruction, training and supervision as is necessary to ensure, so far as is reasonably practicable, the health and safety at work of employees.</p> <p>UK-GD-04. MTCL must so far as is reasonably practicable as regards any place of work under the employer's control, ensure maintenance of it in a condition that is safe and without risks to health and the provision and maintenance of safe means of access to and egress from it.</p> <p>UK-GD-05. MTCL, and partners if necessary, must collaborate in ensuring the provision and maintenance of a working environment for employees that is, so far as is reasonably practicable, safe, without risks to health, and adequate as regards facilities and arrangements for their welfare at work.</p> <p>UK-GD-06. MTCL, and partners if necessary, must collaborate in ensuring that that all articles, substances (and fairground equipment) for use at work are designed and constructed (or installed) for safe use at work and while being maintained, handled, processed and stored.</p>
--	--

Table 23 UK Work Environment and Equipment Requirements

ID	UK-WEE	Requirement	Work Environment and Equipment (WEE)
Description		MTCL, with partners, must ensure the safety of the working environment and equipment used by employees and participants in OPTIMAI project activities.	
Implementation in OPTIMAI		<p>UK-WEE-01. MTCL must ensure cleanliness of the working environment including through removal of dirt and refuse daily; and weekly sweeping or washing of floors; and regular and revarnishing or painting and washing of walls.</p> <p>UK-WEE-02. MTCL must take measures to prevent overcrowding of workrooms, and no OPTIMAI pilot or research activities should be conducive to or require the overcrowding of workrooms.</p>	

	<p>UK-WEE-03. MTCL must ensure that workrooms are at a reasonable temperature.</p> <p>UK-WEE-04. MTCL must ensure workrooms are adequately lit.</p> <p>UK-WEE-05. The workspace must be adequately secured against ignition sources and boilers should function safely and as certified.</p> <p>UK-WEE-06. Adequate personal protective equipment must be supplied to employees as necessary to protect them against risks that cannot be addressed through other methods, and any OPTIMAI wearable requirements should not take priority over necessary PPE.</p> <p>UK-WEE-07. MTCL, with the support of partners as necessary, must ensure that employees are adequately protected from machinery, that OPTIMAI pilot and research activities are not conducive to increasing risks from this machinery, and that adequate information is provided on the safe and proper use and maintenance of OPTIMAI devices.</p> <p>UK-WEE-08. MTCL, with the support of partners as necessary, must ensure that the workspaces have adequate and unobstructed emergency exits that are clearly marked and lead to safety and nothing arising from OPTIMAI pilot or research activities compromises this.</p>
--	--

Table 24 UK Worker Welfare Requirements

ID	UK-WW	Requirement	Worker Welfare (WW)
Description	MTCL, with the support of partners where it might be helpful, must ensure the welfare and comfort of pilot site workers.		
Implementation in OPTIMAI	<p>UK-WW-01. MTCL are required to provide suitable points for drinking water from a public main or sources approved by the District Council; adequate washing facilities; accommodation for clothing not worn during working hours; and sitting facilities where workers can sit without detriment to their work.</p> <p>UK-WW-02. MTCL must provide equipment and facilities to render workers with first-aid and ensure that a sufficient number of trained individuals are available to provide the first-aid. Employees should be</p>		

	informed of first-aid arrangements including the location of relevant equipment, facilities, and personnel.
--	---

Table 25 UK Risk Assessment and Management Requirements

ID	UK-RAM	Requirement	Risk Assessment and Management (RAM)
Description			MTCL must, with the support of partners if necessary, consider the necessity of and then if required conduct a risk assessment taking into account any dangers arising from OPTIMAI pilot and research activities, and take adequate measures to mitigate those risks.
Implementation in OPTIMAI			<p>UK-RAM-01. MTCL, with the support of partners where necessary, prima facie, must make a suitable and sufficient assessment of the risks to the health and safety of employees to which they are exposed whilst they are at work; and the risks to the health and safety of persons not in their employment arising out of or in connection with the conduct by MTCL of the undertaking, specifically with references to changes OPTIMAI research and pilot activities will bring about to processes and the working environment. If necessary, this should also be conducted with a view to identifying and mitigating fire safety risks. A justification should be provided and documented if MTCL believes this unnecessary. The risk assessment should be reviewed if necessary.</p> <p>UK-RAM-02. Documented measures must be implemented to mitigate the risks identified, and there should be health surveillance in relation to identified risks.</p> <p>UK-RAM-03. MTCL must ensure appointment of competent persons to assist them in undertaking the measures they need to take to comply with the requirements and prohibitions imposed upon them by or under the relevant statutory provisions of health and safety legislation, and such person(s) should be informed of all factors affecting the health and safety of workers, most pertinently, all factors relevant to OPTIMAI pilot and research activities.</p> <p>UK-RAM-04. Workers must be informed with relevant and comprehensible information about the risks to their health and safety</p>

	identified by the assessment; the preventive and protective measures; and any other meaningful information.
--	---

Table 26 UK Employee Duties, Capabilities, and Training Requirements

ID	UK-EDCT	Requirement	Employee Duties, Capabilities, and Training (EDCT)
Description			MTCL, with the support where necessary of partners, must ensure that workers participating in or affected by OPTIMAI pilot activities are sufficiently empowered to protect their health and safety.
Implementation in OPTIMAI			<p>UK-EDCT-01. MTCL employees have duties to themselves and others as enshrined in the law, and must use equipment in a careful manner as they were trained to do, and have responsibility for their health and safety as well as others'. OPTIMAI partners must support this where reasonable.</p> <p>UK-EDCT-02. MTCL with the support of OPTIMAI partners must provide adequate health and safety training for new equipment and technologies.</p>

Table 27 UK Employee Consultation Requirements

ID	UK-EC	Requirement	Employee Consultation (EC)
Description			MTCL, with the participation of partners if necessary, must consult with employees or their representatives regarding health and safety matters related to OPTIMAI pilot and research activities.

Implementation in OPTIMAI	UK-EC-01. MTCL and partners where applicable must fully cooperate with the trade union health and safety representative or other employee representatives, who should be informed about all matters material to the health and safety of employees, particularly those stemming from OPTIMAI pilot and research activities
--------------------------------------	---

6 Regulatory Framework to Support Lawful Conduct of Pilot Activities in Spain

6.1 Introduction

Televes SA (hereinafter TVES) is an antenna manufacturing plant that participates as end-user in the OPTIMAI Project. TVES will carry out the three OPTIMAI use cases that are foreseen to be piloted on end-users' facilities. They are located in A Coruña, Spain. The three use cases are: Zero defect quality inspection (UC1), Production line setup-calibration (UC2), and Production Planning (UC3). The first two use cases aim at identifying, detecting, and optimizing stoppages and/or incidents that may affect production efficiency during antenna manufacturing. As for the third use case, it has been planned to obtain a digital twin of the antenna manufacturing plant. It will support the simulation of production scenarios to analyse incidences that may cause losses in the assembly lines, thereby improving manufacturing processes. TVES will carry out three use cases on their site, which are presented in **Subsection 6.2 Pilot Descriptions TVES**.

With the aim of supporting TVES to be compliant with the national legal requirements referred to data protection law, employment law, equality law, and health and safety law, the following subsections will provide an overview of the main Spanish legal provisions on these matters.

Subsection 6.3 Data protection in the Employment Context **in the Employment Context** will present the specific privacy rights in the employment context laid down in the Spanish data protection legal framework, and further privacy and protection aspects to be considered in employment settings.

Subsection 6.4 Employment Law will identify a set of general legal requirements concerning employment rights in Spain that are particularly applicable to TVES pilot activities.

Subsection 6.5 Equality Law will lay out TVES pilot site employees' rights to not be discriminated against or harassed or victimised based on protected characteristics, as well as duties regarding reasonable accommodations for persons with disabilities.

Subsection 6.6 Health and Safety Law will present an overview of health and safety requirements to ensure that TVES pilot activities preserve TVES pilot site employees' right to effective health and safety protection in working environments.

Finally, actionable requirements are provided in tables in **Subsection 6.7 Spain Data Protection, Employment and Equality, Health and Safety Law Requirements**.

6.2 Pilot Descriptions TVES

UC1 - Zero defect quality inspection. The objectives of this use case are: i) the real-time detection of defects; and ii) prediction and prevention of upcoming defects by monitoring of production conditions.

As previously mentioned, the antenna manufacturing line is an error-prone manufacturing process, and the sources of defects are attributed to a combination of material defects, parts integration, and machine failures. Based on the installation of quality inspection sensors and the use of AI models, OPTIMAI will target the most common types of defects:

- i) *Material defects*: TVES uses materials coming from other sections as well as those that are produced in the antenna plant itself in the robotized antenna assembly line. Normally, those coming from other sections meet the quality requirements. However, materials processed in the antenna plant might be defective and not be detected as such before entering them in the line. The objective of this use case is to detect defective materials in real time to improve production efficiency.
- ii) *Final product quality failures*: Currently, TVES uses vision systems along the antenna assembly line to ensure antennas' quality. Sometimes, these systems fail so that OPTIMAI solutions may improve real time defect detection, identification of the defect causes, and prediction and prevention of defects.

UC2 - Production line setup-calibration. The objectives of this use case are: i) automating the reconfiguration of machines based on a contextual AI analysis of multiple sensors; and ii) accelerating operator machine interaction using augmented reality and computer vision.

This use case focuses on setting up and calibrating the equipment related to the quality control defined for UC1. Based on quality inspection results, the purpose is to automatically re-calibrate machine parameters so that either defects are not propagated or not manifested at all through the early identification and correction of suboptimal manufacturing. Moreover, line setup times will be improved as a result on this optimized calibration process. The following quality control scenarios will be examined: i) manufacturing reference changes; ii) stoppages in inspection/vision systems; iii) incidents in material feeding peripherals; iv) incidents in pallet conveyor systems; and v) software/hardware incidents in robotic cells. All these scenarios will be recorded during manufacturing and will provide OPTIMAI with valuable data to develop AI systems capable of extracting information that will be used to reconfigure machines and robotic cells in the antenna manufacturing plant.

UC3 - Production planning. The aim of UC3 is two-fold: i) virtualizing production by developing simulation environments to select optimal conditions for different types of products; and ii) connecting the virtual with the physical counterparts enabling the rapid setup of production according to the virtual replicas.

The virtualization process will include not only the specific robotic cells but also virtual sensors providing a complete virtual production environment. It will be key to identify optimal parameters for each product type, while the necessary actuation interface will be implemented to rapidly setup the respective robots.

By using OPTIMAI simulated scenarios, operators will be able to adjust and experiment with different setups in advance before they can have any effect on the production.

The following subsections attempt to provide insightful input regarding the main Spanish legal provisions that must be observed by TVES to ensure and protect the rights and welfare of pilot site employees.

6.3 Data protection in the Employment Context

The Spanish data protection law, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD),²⁸ sets out specific data protection rights that apply in the employment context.

Article 87 LOPDGDD lays down the right to privacy and use of digital devices in the work environment. It states that employees have the right to privacy when using digital devices provided by their employers. Employers may be able to access the information derived from such use with the sole purpose of verifying employees' fulfilment of their contractual obligations, as well as ensuring the integrity of the devices. Employers must establish criteria for the use of such devices, which must respect employees' right to privacy. Employees' representatives shall participate in the establishment of such criteria.

The right to digital disconnection is set out in Article 88 LOPDGDD. Employees have been granted the right not to be connected to digital devices for professional purposes during rest periods, paid leave, and holidays. Employers shall put in place internal policies addressed at employees, with the involvement of employees' representatives, to determine how to exercise this right, as well as to define training sessions and other awareness-raising activities for employees about the reasonable use of digital devices.

Article 89 LOPDGDD recognizes the employees' right to privacy in case of video monitoring and sound recording devices in the workplace. The use of video monitoring systems to control employees' activity is allowed if such monitoring activities comply with Spanish Labour laws, and if employees have been previously informed of the existence of this measure in an explicit, clear, and concise way. Workplace sound recording is only permitted if proportionate and necessary to ensure the safety of facilities, goods, and people. Under no circumstances shall video monitoring systems and sound recording devices be installed in places intended for employees' rest or leisure, such as changing rooms, toilets, canteens, and similar places.

Lastly, Article 90 LOPDGDD establishes the employees' right to privacy against the use of geolocation systems in the employment context. The processing of data obtained from geolocation systems deployed to control work activity is allowed if it falls under the Spanish legal framework and its limits, as will be explained below (See **Section 6.3.1.3 Monitoring of Employees**). Prior to the deployment, employees must have been expressly, clearly, and concisely informed of the existence of the data processing devices and of their data protection rights as data subjects.

6.3.1 AEPD Guidance on Data Protection in the Employment Context

²⁸ <https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf>

The Spanish Data Protection Agency (AEPD) published in 2021 the guide *La protección de datos en las relaciones laborales* with the aim of providing practical guidelines to help public and private organizations to comply with the Spanish data protection legal framework [27]. This guide was prepared by the AEPD with the involvement of the Spanish Ministry of Labour and Social Economy, employers' organizations, and trade unions.

A complete summary of the guide will not be provided here, although several points with possible relevance to OPTIMAI activities will be overviewed in the subsequent subsections.

6.3.1.1 Workers' Rights

Right of access: Regardless of the information provided (see **Subsection 4.2.5.1 The Right to Information**), employees have the right to confirmation that data processing is taking place and, if so, the right to know how such processing is taking place. Employees exercising the right of access may request a copy of the personal data being processed. Data controllers may comply with this right by facilitating remote access to a secure system that provides the data subject with direct access to their personal data (see **Subsection 4.2.5.2 The Right to Access** for further details).

Right to rectification: Employees can request the rectification of inaccurate data that is being processed, as well as the completion of incomplete data (see **Subsection 4.2.5.3 The Right to Rectification** for further details).

Right to erasure: Employees may request the erasure of their personal data in the situations listed in **Subsection 4.2.5.4 The Right to Erasure**.

Following Article 32 LOPDGDD, before proceeding to the rectification or erasure of personal data, personal data must be blocked. The blocking of data consists of preventing its processing (including its visualization) through the adoption of technical measures (unless required to make the data available to Public Prosecutor or Public Administrations).

Right to restriction of processing: It is a right of workers that can be exercised in case of inaccuracy, unlawfulness, lack of necessity and the exercise of the right to object (see **Subsection 4.2.5.5 The Right to Restriction of Processing** for further details).

Workers have the right to be informed about any rectification or erasure of personal data or restriction of processing, as well as the lifting of the restriction.

For the right to data portability; right to object; and the right not to be subject to automated decision-making, see **Subsection 4.2.5 Rights of the Data Subject**.

6.3.1.2 Confidentiality and Security

Article 5 LOPDGDD sets out the duty of confidentiality. In this regard, data controllers and processors as well as all persons involved in any data processing activity are subject to the duty of confidentiality.

Confidentiality ensures that personal data is only accessible to the data subject and to those within the organization that have the authority to process or consult it. Security measures must

not only guarantee confidentiality, but also the availability of data, and thus its recovery in case of any event, and its integrity, which entails protecting it against any unauthorized manipulation.

Policies must be put in place to ensure compliance with these two principles. It is essential to develop human resources policies that clearly define the functional profiles of each position, and training procedures. In this vein, the AEPD recommends [27]: i) designing the roles and responsibilities of the staff according to their relationship with the processing of personal data; ii) delivering adequate training to employees—considering their varying degrees of responsibility, raising awareness on their duties of confidentiality and security, as well as contributing to the development of a culture of commitment with data protection matters; iii) warning and training those employees who do not have a direct relationship with information systems and the processing of personal data, but may put at risk the confidentiality or security of the data (e.g., cleaning staff); iv) assessing the possibility of appointing a data protection officer, who can provide advice on accountability practices of data controllers.

6.3.1.3 Monitoring of Employees

According to Article 20.3 of the Workers' Statute (see **Section 6.4 Employment Law**), employers may adopt the monitoring and control measures deemed most appropriate to verify employees' compliance with their obligations and work duties, keeping in their adoption and deployment due consideration to human dignity.

The monitoring of employees is subject to a proportionality test of the monitoring measures to be adopted. This test involves assessing whether the monitoring measure:

- a) is likely to achieve the proposed objective (suitability test)
- b) is necessary: there is no other less invasive measure to achieve the proposed objective (necessity test)
- c) is weighted or balanced: it entails more benefits or advantages for the general interest than harm to other goods or values in conflict (proportionality test in the strict sense).

Once the test has been passed, the employer may adopt the monitoring measure, but will have to:

- inform workers about the existence of the monitoring measure, its purpose, and the purpose of the data processing
- respect the principle of data minimisation
- respect the principle of purpose limitation.

Employers do not have to obtain consent from employees to establish *access control mechanisms*. Nevertheless, employees' fundamental rights must be preserved. In this regard, the legitimate basis is the performance of a contract. However, privacy-intrusive access control mechanisms must be avoided if more privacy-friendly and equally effective mechanisms can be implemented. If access control mechanisms entail the processing of *biometric data*, the AEPD highlights the following aspects (which are also applicable to any processing of biometric data in the employment context) [27]:

1. lawful basis: performance of a contract with regards to the employers' right to adopt control measures to verify workers' compliance with their obligations and work duties
2. employees must be informed about the processing of biometric data
3. a data protection-by-design approach must be adopted
4. biometric data should be stored as biometric templates whenever possible
5. data should preferably be stored in a personal device, rather than in a centralized storage system. A specific encryption key should be used to effectively protect the data from unauthorized access
6. the biometric system used and the security measures implemented must ensure that it is not possible to reuse the biometric data for another purpose
7. encryption should be used to prevent unauthorized reading, copying, modification or deletion of biometric data
8. biometric systems should be designed in such a way that the identity link can be revoked
9. specific data formats or technologies that prevent the interconnection of biometric databases and the disclosure of unverified data should be used
10. biometric data must be deleted when they are no longer linked to the purpose which enabled their processing. If possible, automated mechanisms for data erasure should be implemented
11. if it is planned to implement a biometric identification system, a data protection impact assessment must be conducted before its deployment.

Monitoring may also include *video monitoring*. Although in OPTIMAI video monitoring is not foreseen, it is important to bear in mind the following aspects highlighted by the AEPD of Article 89 LOPDGDD:

1. lawful basis: performance of a contract with regards to the employers' right to adopt control measures to verify workers' compliance with their obligations and work duties
2. video monitoring should only be used when it is not possible to resort to other means that have less impact on privacy. In this sense, video monitoring systems for employees' control should only be adopted when the purpose pursued is proportional to the way the images are processed, and there is no other more suitable measure
3. the minimisation principle must be complied with
4. employers must inform employees and, where appropriate, their representatives, in an explicit, clear, and concise manner, about this measure
5. data processing occurs whether the cameras record images or display them in real time
6. under no circumstances shall video monitoring systems and sound recording devices be installed in places intended for employees' rest or leisure, such as changing rooms, toilets, canteens, and similar places
7. appropriate safety measures must be implemented based on the risk analysis, and on the impact assessment, if necessary.

As mentioned above, Article 90 of the LOPDGDD allows the use of geolocation systems to monitor workers. The AEPD provides the following recommendations when using geolocation systems [27]:

1. lawful basis: performance of a contract with regards to the employers' right to adopt control measures to verify workers' compliance with their obligations and work duties
2. employees and, where applicable, their representatives must be explicitly, clearly, and unequivocally informed about the existence and features of the geolocation system
3. employees must also be informed about the possible exercise of the rights of access, rectification, restriction of processing, and erasure
4. the principles of data minimization and purpose limitation must be applied
5. the principle of proportionality requires limiting this type of systems to situations where less privacy-invasive means do not exist.

Lastly, the AEPD states that the *monitoring of health data through wearables*, such as wristbands or watches is, in general, prohibited, unless established by law, for the following reasons [27]:

1. there is no legal basis. The processing of this data cannot rely on consent due to the power asymmetries between employees and employers
2. there is no lawful purpose
3. it goes against the principle of proportionality.

6.4 Employment Law

The reference legal framework for employment practices and workers' rights in Spain is the Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores²⁹ (hereinafter, Workers' Statute). It applies to those workers who voluntarily provide their remunerated services as employees within the scope of the organization and administration of a company.

As a general overview, the Workers' Statute outlines basic employee rights and obligations in the context of an employment relationship that falls under its scope of application. It is important to highlight that such rights and obligations must be compliant with the legal and statutory provisions of the Spanish legal framework, the collective agreements adopted, the will of the concerned parties (employer/employee) and the local and professional usages and customs in place. In addition, it establishes the different forms, procedures, and content that any labour contract may have. Legal requirements affecting the modification, suspension and termination of the labour contracts are also provided by the Spanish legislator in this Statute. Employers' obligations aimed at ensuring an effective implementation of employee rights are also clearly identified, especially those affecting health and safety, non-discrimination, equality, and unfair dismissals. The Workers' Statute also specifies sanctions for employee penalties and misconduct.

The following paragraphs attempt to identify a set of general legal requirements concerning Spanish employment rights that are particularly applicable to TVES pilot activities. Such requirements identification has been conducted with the aim: of i) protecting Spanish pilot

²⁹ <https://www.boe.es/eli/es/rdlg/2015/10/23/2/con>

employees' rights; and ii) delimiting employers' obligations to not compromise employees' enjoyment of the rights enshrined in the Workers' Statute.

TVES must be respectful of the basic employee rights recognized in the context of any employer-employee relationship as laid down in Article 4 (2) of the Workers' Statute. Thus, Spanish employees have the right to:

- effective employment, which is the right of the worker to be provided by the employer, in compliance with the employment contract signed, with the performance of duties in accordance with his or her job.
- promotion and professional training at work, including training aimed at adapting to changes in the job, as well as the development of training plans and actions aimed at favouring greater employability
- not being discriminated against directly or indirectly for employment, or once employed, for reasons of sex, marital status, age within the limits set by this law, racial or ethnic origin, social status, religion or beliefs, political ideas, sexual orientation, membership or not of a trade union, as well as for reasons of language. Employees shall not be discriminated against on the grounds of disability if they are fit to carry out the work in question
- their physical integrity and to an adequate occupational risk prevention policy
- their privacy and with due consideration for their dignity, including protection from harassment based on racial or ethnic origin, religion or belief, disability, age, or sexual orientation, and from sexual harassment and harassment based on sex
- timely receipt of the agreed or legally established remuneration.

Employees' obligations are set out in Article 5 of the Workers' Statute. Spanish pilot site employees must be compliant with the following obligations:

- fulfilling the specific duties of their job, in accordance with the rules of good faith and diligence
- observing the health and safety measures adopted
- complying with the orders and instructions of the employer in the regular exercise of their managerial powers
- contributing to increase productivity.

6.4.1 Health and Safety

The Workers' Statute recognizes in its Article 19, rights and duties to both employees and employers regarding health and safety. In this regard, and in light of the OPTIMAI pilot activities, the following set of rights and duties have been identified as applicable:

Health and Safety Workers' Rights:

- employees shall be entitled to effective occupational health and safety protection
- employees are obliged to observe the legal and statutory health and safety measures at work

- in the inspection and control of health and safety measures which are compulsory for the employer, employees have the right to participate through their legal representatives, if there are no specialised bodies or centres competent in the matter in accordance with the legislation in force
- health and safety officers or employees' legal representatives, who observe a serious and grave probability of an accident due to non-compliance with the applicable legislation on the matter, shall require the employer in writing to adopt the appropriate measures to eliminate such risk.

Health and Safety Employers' Duties:

- the employer is obliged to ensure that each employee receives sufficient and appropriate theoretical and practical training in preventive matters both at the time of hiring, whatever the type or duration of the contract, and when there are changes in the tasks performed or when new technologies or changes in work equipment are introduced.

6.4.2 Unfair Dismissals

The OPTIMAI Consortium cannot accept unfair dismissals of Spanish pilot employees who participate in the OPTIMAI pilot activities or that are affected by OPTIMAI research and pilot activities. The Workers' Statute states in its Article 52 the objective conditions under which a employment contract can be terminated fairly:

- employees ineptitude, known or acquired after their effective placement in the company
- employees' failure to adapt to technical changes made to their job, where such changes are reasonable. Beforehand, the employer must offer a training course aimed at facilitating the adaptation to such changes. Termination of the employment contract may not be decided by the employer until at least two months after the change was introduced or the adaptation training completed.

To be considered fair, the employer must sufficiently demonstrate that the objective cause supporting the dismissal specifically requires the termination of the contract of the concerned employee. These objective conditions established to terminate an employment contract requires the employer to observe a set of additional formal requirements: i) the employer's obligation to send a written communication to the worker stating the objective cause to terminate the employment contract; ii) make available to the employee, simultaneously with the delivery of the written communication, the indemnity of twenty days' compensation per year; iii) granting a period of notice of fifteen days, established from the delivery of the written communication to the employee, until the termination of the employment contract.

When the employer's termination decision is based on any of the causes of discrimination prohibited in the Spanish Constitution or in any other legal instrument, or when it has been produced in violation of the fundamental rights and public liberties of the employee, the termination decision shall be null. Such termination decision shall also be null in the case of pregnancy, birth, adoption, and foster care.

6.5 Equality Law

The OPTIMAI Consortium is strongly committed to the obligation of supporting diversity and inclusion in the context of the OPTIMAI pilot activities. OPTIMAI end-user partners must ensure that pilot activities are not discriminatory, nor may lead to employees' harassment and victimisation. To that end, the ethical and legal partners of the project (UAB & TRI) will monitor non-discrimination measures that OPTIMAI end-users put in place to minimise potential risks that may have negative impacts on the equality rights of the pilot site employees. Significant efforts and measures will be requested from OPTIMAI end-users—*according to their national legal frameworks*—for ensuring that pilot site employees are protected against discriminatory and non-inclusive working practices.

In Spain, the Workers' Statute incorporates the modifications referring to measures on equal treatment and non-discrimination at work laid down in Article 37 of the Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.³⁰ Such modifications aim at establishing measures to make the principle of equal treatment and non-discrimination real and effective in the access to employment, membership, and participation in trade unions and employers' organisations, working conditions, career advancement and regular training.

The principle of equal treatment implies the absence of any direct or indirect discrimination based on racial or ethnic origin, religion or belief, disability, age, or sexual orientation. However, it is worth noting that differences of treatment based on these protected characteristics shall not be considered as discrimination where the working activity concerned or the context in which it is carried out, such a characteristic constitutes a genuine and decisive job requirement. To that end, the purpose must be legitimate, and the requirement proportionate.

Thus, under Article 4(2)(c) of the Workers' Statute, employees have the right to not be directly or indirectly discriminated against for employment for reasons of sex, marital status, age, racial or ethnic origin, social status, religion or beliefs, political ideas, sexual orientation, membership or not of a trade union, as well as for reasons of language. Moreover, employees may not be discriminated against due to disability, if they are fit to perform the work or job in question. The same article in its subparagraph (2)(e) states that employees have the right to privacy and dignity, including protection from harassment based on racial or ethnic origin, religion or belief, disability, age, or sexual orientation, and from sexual harassment. As regards to the employers, any decision affecting working conditions which contains direct or indirect discrimination on the grounds of age, disability, sex, origin (including racial or ethnic origin), marital status, social status, religion or beliefs, political ideas, sexual orientation, membership or non-membership of trade unions and their agreements, family ties with other workers in the company, and language shall be considered null.

In addition, under the provisions enacted in the Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres³¹ (hereinafter, Ley Orgánica 3/2007), the principle of equal treatment between women and men implies the absence of any direct or indirect

³⁰ <https://www.boe.es/eli/es/l/2003/12/30/62/con>

³¹ <https://www.boe.es/eli/es/lo/2007/03/22/3/con>

discrimination³² on grounds of sex, maternity, the assumption of family obligations, and marital status. Any unfavourable treatment of women related to pregnancy or maternity constitutes direct discrimination on grounds of sex.

Companies are obliged to respect equality of treatment and opportunities in the workplace. To this end, they must adopt measures aimed at avoiding any type of discrimination between women and men in the workplace. These measures must be negotiated and, where appropriate, agreed upon with the legal representatives of the workers as established by labour legislation. The rights to reconcile personal, family and working life shall be recognised for male and female workers in a way that encourages the balanced assumption of family responsibilities, avoiding any discrimination based on their exercise.

According to the Ley Orgánica 3/2007, and without prejudice of the provisions laid down by the Spanish Criminal Code, any verbal or physical conduct of a sexual nature which has the purpose or has the effect of violating the dignity of a person, when it creates an intimidating, degrading or offensive environment, constitutes sexual harassment. Sexual harassment and harassment on grounds of sex shall be deemed to be discriminatory. Companies shall promote working conditions that prevent sexual harassment and harassment based on sex and shall establish specific procedures for its prevention and for dealing with complaints or claims that may be made by those who have been subjected to it.

6.5.1 Adjustments for Persons with Disabilities

Pursuant Article 35 of the Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social,³³ persons with disabilities have the right to work under conditions that guarantee the application of the principles of equal treatment and non-discrimination.

Direct discrimination shall exist where a person with a disability is treated less favourably than another person in a similar situation based on his or her disability. Indirect discrimination shall exist where an apparently neutral legal or regulatory provision, a contractual or contractual clause, an individual agreement or a unilateral decision of the employer is liable to place persons with disabilities at a particular disadvantage compared with other persons. In these cases, indirect discrimination exists when i) the provision does not objectively serve a legitimate aim; ii) the means of achieving that aim are not appropriate and necessary. The employer is obliged to take appropriate measures, according to the needs of the particular situation and in

³² Article 6 of the Ley Orgánica 3/2007, defines the concepts of direct and indirect discrimination. Accordingly, a direct discrimination on grounds of sex is defined as any situation in which a person is, has been or would be treated less favorably on grounds of sex than another person in a comparable situation. As regard to indirect discrimination, it may occur in those cases in which an apparently neutral provision, criterion, or practice puts persons of one sex at a particular disadvantage compared with persons of the other sex, unless that provision, criterion or practice can be objectively justified by a legitimate aim and the means of achieving that aim are necessary and appropriate.

³³ <https://www.boe.es/eli/es/rdlg/2013/11/29/1/con>

accordance with Article 40, to eliminate the disadvantage caused by the provision, clause, agreement or decision.

Harassment on grounds of disability, as defined in Article 2(f), shall in any case be considered a discriminatory act.

Employers are obliged to take appropriate measures to adapt the workplace and the accessibility of the company, according to the needs of each specific situation, in order to enable people with disabilities to have access to employment, to perform their work, to progress professionally and to access training, unless such measures place an excessive burden on the employer.

6.6 Health and Safety Law

Protecting health and safety of the OPTIMAL end-user employees who will voluntarily participate in the OPTIMAL pilot activities is one of the most crucial legal requirements that end-user employers must comply with according to their national labour legal framework.

In the case of Spain, TVES will observe the general provisions on health and safety laid down in the Workers' Statute as explained in **Section 6.4 Employment Law**. In addition, the Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales³⁴ stipulates the basic guarantees and responsibilities that are required to establish an adequate level of protection of employees' health and safety against risks arising from working conditions. According to its provisions, Spanish employees have the right to an effective safety and health protection at work. The employees' rights of information, consultation, participation, and training on preventive matters, as well as their right to stop labour activities when serious and imminent risks arise or to monitor their health status, are also part of the employees' right to an effective safety and health in working environments.

The monitoring related to the health status of the employees has a voluntary nature and must be carried out on the legal basis of the employees' consent. Exceptions shall only be made when i) it is essential to carry out the examinations in order to assess the effects of the working conditions on the health of workers; ii) to verify whether the state of health of the worker may constitute a danger to the worker, to other workers or to other persons connected with the undertaking, or iii) where it is laid down in a legal provision in relation to the protection of specific risks and activities involving special risks.

In any case, such health surveillance activities: i) must be proportional to the risks at stake and shall cause the least discomfort to the employees; and ii) must be respectful of the employees' dignity, privacy, and data protection rights. In this regard, information related to employees' health must be confidential. Data related to the health of employees may not be used for discriminatory purposes or to the detriment of the employee. Access to personal medical information shall be restricted to medical personnel and health authorities carrying out health surveillance of workers and shall not be made available to the employer or to other persons without the explicit consent of the worker. However, the employer and the persons or bodies

³⁴ <https://www.boe.es/eli/es/l/1995/11/08/31/con>

responsible for prevention shall be informed about the conclusions drawn from the examinations carried out in relation to the employee's suitability for the job or to the need to introduce or improve protective and preventive measures, so that they can carry out their preventive duties correctly.

The employees' right to effective health and safety protections entails the employer's obligation to protect them against risks at work. This duty must be exercised following the general principles of prevention for managing health and safety risks that have been set out in Article 15 of this Act:

- avoiding risks
- evaluating the risks that cannot be avoided
- combating the risks at source
- adapting the work to the individual, particularly regarding the design of workplaces, the choice of work equipment, working procedures and production methods with the aim of mitigating monotonous work and negative impacts on the employees' health
- replacing dangerous tasks or activities by the non-dangerous or the less dangerous tasks or activities
- planning, developing, and implementing a prevention policy which integrates technology, organisation of work, working conditions, social relationships, and factors related to the working environment
- prioritizing collective protective measures over individual ones
- providing appropriate instructions to the employees.

TVES will also have to consider the professional capabilities of their pilot site employees regarding health and safety at the time of allocating OPTIMAI pilot activities among them. Additional risks may arise from potential distractions among the employees. Consequently, appropriate preventive measures should be implemented to avoid foreseeable distractions among employees.

6.6.1 General health and Safety Requirements with Regards to Equipment and Means of Protection

Law 31/1995, in its Article 17 provides general health and safety requirements with regards to equipment and means of protection. Thus, Spanish employers shall take the necessary measures to ensure that work equipment is suitable for the work to be carried out and that they are suitably adapted for that purpose to guarantee the safety and health of employees. Where the use of work equipment is likely to present a specific risk to the safety and health of workers, the employer shall take the necessary measures to ensure that:

- the use of the work equipment is reserved to those responsible for such use
- the repair, conversion, maintenance, or servicing work is carried out by employees specifically trained for that purpose.

The employer shall provide their workers with personal protective equipment suitable for the performance of their duties and shall ensure that it is used effectively when, by reason of the nature of the work carried out, it is necessary. Such personal protective equipment shall be used

when the risks cannot be avoided or cannot be sufficiently limited by technical means of collective protection or by measures, methods, or work organisation procedures.

As OPTIMAI partners will be supplying equipment to be used by pilot sites employees, they should support TVES in complying with the safe use of that equipment. This support may entail: i) providing safe equipment with understandable and accessible safety information and guidelines; ii) providing additional preventive safety measures that shall be implemented; iii) and identifying potential safety and health risks that the supplied equipment may pose in terms of its normal use, inappropriate use, and misuse as laid down in Article 41 (1) of Law 31/1995. TVES must ensure that such information is provided to the pilot site employees in a comprehensive and accessible manner.

6.6.2 Risk Assessment and Management Requirements

Law 31/1995 highlights that the prevention of risks in the workplace must be integrated into the general management activities of the company through the design and application of a risk prevention plan which must specify the organisational structure, responsibilities, functions, practices, procedures, processes, and resources necessary to carry out the risk prevention action in the company, in accordance with the applicable legal framework. The main instruments for managing and implementing this plan are assessing the risks and planning preventive activities in accordance with the health and safety risks identified. The employer shall carry out an initial assessment of the risks to the health and safety of workers, considering the nature of the working activity and the characteristics of the existing jobs and of the employees who are to perform them. The same assessment shall apply to the choice of work equipment and chemical substances or preparations, as well as the design of workplaces. The assessment shall be updated when working conditions change and, in any case, shall be considered and reviewed when any damage to health has occurred. Additionally, where the result of the assessment makes it necessary, the employer shall carry out regular checks of the working conditions and the activity of workers in the performance of their services to detect potentially dangerous situations. If the results of the assessment reveal risk situations, the employer shall carry out those preventive activities necessary to eliminate or reduce and control such risks. These activities shall be planned by the employer, including the deadline for carrying it out for each preventive activity, the designation of those responsible, and the allocation of human and material resources necessary for its execution. The effective execution of these preventive measures shall be monitored by the employer on a regular basis.

Additionally, the employer shall specifically ensure the protection of employees who, due to their own personal characteristics or physiological condition, including recognised physical, mental or sensory disabilities, are particularly sensitive to the risks arising from work. To this end, employers shall take these aspects into account in the risk assessments and shall adopt the necessary preventive and protective measures. Employees shall not be employed in those jobs in which, due to their personal characteristics, biological condition or recognised physical, mental, or sensory disability, may place themselves in a situation of danger or, in general, when they are manifestly in states or transitory situations that do not meet the psychophysical requirements of the respective jobs.

In compliance with the duty to prevent risks at work, the employer shall designate one or more employees to carry out this activity, set up a prevention service or contract this service with a specialised entity outside the company. Designated employees may not suffer any prejudice because of conducting activities for the protection and prevention of risks at work. On the contrary, such employees shall enjoy the guarantees laid down for workers' representatives in Article 68(a), (b) and (c) and Article 56(4) of the consolidated text of the Workers' Statute Act. The employer has the obligation to provide the employees with relevant and comprehensible information regarding: i) the risks to the health and safety to which employees are exposed to; and ii) the preventive measures that must be put in place to avoid or minimize such risks.

6.6.3 Employee Duties, Capabilities, and Training

Employees' duties regarding the protection of their health and safety at work are specified in Article 29 of Law 31/1995. Thus, it is the responsibility of each worker to ensure their own health and safety at work, as well as that of other persons who may be affected by their professional activity. This duty must be accomplished according to the employee's capabilities, their training, the employer's instructions, and complying with the preventive measures adopted in each case. Based on their professional capabilities and training and following the employers' instructions, employees must:

- properly use, in accordance with their nature and foreseeable risks, the machines, apparatus, tools, hazardous substances, transport equipment and, in general, any other means with which they carry out their activity
- correctly use the means of protection and protective equipment provided by the employer, in accordance with the instructions received from the employer
- make proper use of existing safety devices or those installed in the workplace
- immediately inform their direct line manager, the workers designated to carry out protective and preventive activities or, where appropriate, the prevention service, of any situation which, in their opinion, involves a risk to the health and safety of workers
- contribute to the fulfilment of the obligations established by the competent authority in order to protect the health and safety of employees at work
- cooperate with the employer to enable the employer to ensure safe working conditions that do not pose risks to the safety and health of employees.

In compliance with the employers' duty of protection, TVES must ensure that each employee receives sufficient and appropriate theoretical and practical training in preventive matters, both at the time of hiring and when there are changes in the working activities performed or when new technologies or changes in work equipment are introduced. Training should be specifically focused on the job performed by each employee, adapted to the evolution of risks and the emergence of new risks, and repeated periodically, if necessary.

6.6.4 Duty of Consultation

As prescribed in Article 33 of Law 31/1995, Spanish employers have the duty of consulting employees or their representatives before adopting relevant decisions that may affect:

- the planning and organisation of work and the implementation of new technologies, in all matters relating to the consequences that these may have for the health and safety of employees, arising from the choice of equipment, the determination and suitability of working conditions, and the impact of environmental factors at work
- the organisation and development of health protection and occupational risk prevention activities in the company, including the designation of the employees in charge of these activities or the use of an external prevention service
- the designation of employees in charge of emergency measures
- the information and documentation procedures referred to in Articles 18(1) and 23(1) of this Law.³⁵
- the design and organisation of preventive training
- any other action likely to have a substantial effect on the health and safety of employees.

These consultations implement the employees' right to participation and representation in matters related to occupational risk prevention set out in the provisions laid down in Article 34 of Law 31/1995. Employees shall have the right to make proposals to the employer, as well as to the participatory and representative bodies provided for in Chapter V of this Act, aimed at improving the levels of health and safety protection in the company.

6.7 Spain Data Protection, Employment and Equality, Health and Safety Law Requirements

6.7.1 Spain (SP) – Data Protection Requirements

Table 28 Spain Lawful Basis Requirements

ID	SP-LB	Requirement	Lawful Basis (LB)
Description	Utilise an appropriate lawful basis for each data processing operation associated with OPTIMAI pilot activities.		

³⁵ Article 18(1) states that the employer shall take appropriate measures to ensure that workers are provided with all necessary information regarding:

- Safety and health risks of workers at work, including the specific risks related to their tasks
- The protection and prevention measures adopted to address safety and health risks
- Measures to be adopted in emergency situations

Article 23(1) lays down the employer's obligation of drafting and keeping at the disposal of the labour authority the following documentation:

- Health and safety risk assessment and planning of preventive actions
- Protective and preventive measures to be adopted and, where appropriate, protective equipment to be used
- Results of periodic checks on working conditions
- Conduct health checks to workers and provide the results
- List of accidents at work and occupational illnesses that have caused workers to be unable to work for more than one working day.

Implementation in OPTIMAI	<p>SP-LB-01. Consent will only be an appropriate legal basis for data processing where it is freely given, specific, informed and given by unambiguous agreement. Workers should be able to withdraw this consent at any time.</p> <p>SP-LB-02. Consent should not be relied upon in cases where there is a clear power imbalance between data subject and controller/processor, such as the employer-employee relationship, where genuine free choice cannot be demonstrated. TVES operators and other employees who pilot OPTIMAI technologies or are within range of personal data collecting sensor devices, or are otherwise required to supply personal data over the course of research activities, are not in a position to provide appropriate consent.</p> <p>SP-LB-03. Data controllers must consider the appropriate lawful basis for personal data processing, whether performance of a contract with regards to the employers' right to adopt control measures to verify workers' compliance with their obligations and work duties, or legitimate interest or another lawful basis. In case of relying on legitimate interest, a balancing test should be performed and documented with the assistance of a legitimate interest assessment. TVES and others identified as data controllers should conduct this legitimate interest assessment in advance of processing personal data in relation to pilot activities.</p>
----------------------------------	---

Table 29 Spain Data Subject Rights Requirements

ID	SP-DSR	Requirement	Data Subject Rights (DSR)
Description			The data protection rights of pilot sites employees must be upheld and protected.
Implementation in OPTIMAI			<p>SP-DSR-01. The data controller is to communicate all relevant information to the data subject (who could be an employee of TVES or a site visitor, for example) in a concise, transparent, intelligible and easily accessible form, and must be aware that duties apply even where personal data was not collected by the data controller.</p> <p>SP-DSR-02. Data subjects have the right to confirmation that data processing is taking place and, if so, the right to know how such processing is taking place. Employees exercising the right of access may request a copy of the personal data being processed.</p> <p>SP-DSR-03. Data subjects have the right to have incorrect information about them corrected and have incomplete information corrected.</p>

	<p>SP-DSR-04. Data subjects have the right for their data to be erased when it is no longer necessary; consent is withdrawn; processing is objected; the data has been unlawfully processed; etc. Before proceeding to the rectification or erasure of personal data, personal data must be blocked.</p> <p>SP-DSR-05. Data subjects have the right to have data processing restricted where the personal data's accuracy is contested; processing is unlawful and the subject requests restriction rather than erasure; the controller no longer has use for the data, but the data subject does (e.g., for a legal claim); or the data subject has objected pending verification of whether the grounds of the controller override the subject's interest. Employees have the right to be informed about any rectification or erasure of personal data or restriction of processing, as well as the lifting of the restriction.</p> <p>SP-DSR-06. Data subjects have the right to receive their personal data "in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided", where the processing is based on consent or is carried out by automated means.</p> <p>SP-DSR-07. Data subjects have the right to object to processing of their personal data. In this case, the controller shall no longer process the personal data unless compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise or defence of legal claims can be demonstrated.</p> <p>SP-DSR-08. Data subjects have the right not to be subject to automated decision-making including profiling with legal (or similar) effects. Exceptions arise based on performance of contract, authorisation by law, and where explicit consent is obtained from the data subject.</p>
--	---

Table 30 Spain Confidentiality and Security Requirements

ID	SP-C&S	Requirement	Confidentiality and Security (C&S)
Description		Data controllers and processors, as well as all persons involved in any data processing activity, are subject to the duty of confidentiality and are required to put in place all the necessary security measures.	

Implementation in OPTIMAI	<p>SP-C&S-01. Personal data must only be accessible to the data subject and to those within the organization that have the authority to process or consult it.</p> <p>SP-C&S-02. Security measures must not only guarantee confidentiality, but also the availability of data, and thus its recovery in case of any security event, and its integrity, which entails protecting it against any unauthorized manipulation.</p>
----------------------------------	---

Table 31 Spain Right to Privacy Requirements

ID	SP-RP	Requirement	Right to privacy (RP)
Description	TVES pilot site employees have the right to privacy and use of digital devices in the work environment.		
Implementation in OPTIMAI	<p>SP-RP-01. TVES pilot site employees have the right to privacy when using digital devices provided by their employers.</p> <p>SP-RP-02. TVES may be able to access the information derived from such use with the sole purpose of verifying employees' fulfilment of their contractual obligations, as well as of ensuring the integrity of the devices.</p> <p>SP-RP-03. TVES must establish criteria for the use of such devices, which must respect the employees' right to privacy.</p> <p>SP-RP-04. TVES pilot site employees' representatives shall participate in the establishment of such criteria.</p>		

Table 32 Spain Right to Digital Disconnection Requirements

ID	SP-RDD	Requirement	Right to Digital Disconnection (RDD)
Description	TVES pilot site employees have the right not to be connected to digital devices for professional purposes during rest periods, paid leave, and holidays.		
Implementation in OPTIMAI	SP-RDD-01. TVES shall put in place internal policies addressed at employees, with the involvement of employees' representatives, that determine how to exercise this right and define training sessions and other awareness-raising activities for employees about the reasonable use of digital devices.		

Table 33 Spain Employee Monitoring Requirements

ID	SP-EM	Requirement	Employee Monitoring (EM)
Description		TVES may adopt the monitoring and control measures deemed most appropriate to verify employees' compliance with their obligations and work duties. The adoption and deployment of such measures must take into consideration the right to human dignity.	
Implementation in OPTIMAI		<p>SP-EM-01. The monitoring of employees is subject to a proportionality test of the monitoring measures to be adopted.</p> <p>SP-EM-02. TVES pilot site employees must be informed about the existence of the monitoring measure, and the purpose of the data processing.</p> <p>SP-EM-03. Compliance with the principles of data minimisation and purpose limitation is required.</p>	

Table 34 Spain Use of Video Monitoring Systems Requirements

ID	SP-VMS	Requirement	Use of Video Monitoring Systems (VMS)
Description		TVES pilot site employees have the right to privacy in case of video in the workplace.	
Implementation in OPTIMAI		<p>SP-VMS-01. The use of video monitoring systems to control employees' activity is allowed if such monitoring activities comply with Spanish Labour laws. Lawful basis: performance of a contract with regards to the employers' right to adopt control measures to verify workers' compliance with their obligations and work duties.</p> <p>SP-VMS-02. Video monitoring should only be used when it is not possible to resort to other means that have less impact on privacy. In this sense, video monitoring systems for employees' control should only be adopted when there is proportionality between the purpose pursued and the way in which the images are processed, and if there is no other more suitable measure.</p> <p>SP-VMS-03. Compliance with the data minimisation principle is required.</p> <p>SP-VMS-04. TVES must inform the employees and, where appropriate, their representatives, in an explicit, clear, and concise manner, about this measure.</p>	

	<p>SP-VMS-05. Under no circumstances shall video monitoring systems be installed in places intended for employees' rest or leisure, such as changing rooms, toilets, canteens, and similar places.</p> <p>SP-VMS-06. Appropriate safety measures must be implemented based on the risk analysis, and on the impact assessment, if necessary.</p>
--	--

Table 35 Spain Use of Sound Recording Systems Requirements

ID	SP-SRS	Requirement	Use of Sound Recording Systems (SRS)
Description	TVES pilot site employees have the right to privacy in case of deployment of sound recording systems in the workplace.		
Implementation in OPTIMAI	<p>SP-SRS-01. Workplace sound recording is only permitted if proportionate and necessary to ensure the safety of facilities, goods, and people.</p> <p>SP-SRS-02. Under no circumstances shall video monitoring systems and sound recording devices be installed in places intended for employees' rest or leisure, such as changing rooms, toilets, canteens, and similar places.</p>		

Table 36 Spain Use of Geolocation Systems Requirements

ID	SP-GS	Requirement	Use of Geolocation Systems (GS)
Description	TVES pilot site employees have the right to privacy in case of deployment of geolocation systems in the employment context.		
Implementation in OPTIMAI	<p>SP-GS-01. The processing of data obtained from geolocation systems deployed to control work activity is allowed if it falls under the Spanish legal framework. Lawful basis: performance of a contract with regards to the employers' right to adopt control measures to verify employees' compliance with their obligations and work duties.</p> <p>SP-GS-02. TVES pilot site employees and, where applicable, their representatives must be explicitly, clearly, and unequivocally informed about the existence and features of the geolocation system.</p> <p>SP-GS-03. TVES pilot site employees must also be informed about the possible exercise of the rights of access, rectification, restriction of processing and erasure.</p>		

	<p>SP-GS-04. Compliance with the principles of data minimisation and purpose limitation is required.</p> <p>SP-GS-05. The principle of proportionality requires limiting this type of systems to situations where less privacy-invasive means do not exist.</p>
--	---

6.7.2 Spain – Employment Law Requirements

Table 37 Spain Employment Law Requirements

ID	SP-EmR	Requirement	Employees' Rights (EmR)
Description	TVES should not impinge on the employment rights of pilot site employees.		
Implementation in OPTIMAI	<p>SP-EmR-01. TVES pilot site employees shall receive professional training at work about the OPTIMAI solutions and the pilot activities before its start.</p> <p>SP-EmR-02. TVES pilot site employees shall not be directly or indirectly discriminated against on the grounds of sex, marital status, age within the limits set by law, racial or ethnic origin, social status, religion or beliefs, political ideas, sexual orientation, membership or not of a trade union, language, or disability. In case of disability, workers cannot be discriminated against if they are fit to carry out the work or employment In question.</p> <p>SP-EmR-03. TVES pilot activities shall respect employees' physical integrity. To this end, adequate health and safety policies should be in place.</p> <p>SP-EmR-04. TVES must refrain from unreasonably citing any OPTIMAI related pilot or research activity for dismissing OPTIMAI pilot sites employees.</p>		

Table 38 Spain Employees' Obligations Requirements

ID	SP-EmO	Requirement	Employees' Obligations (EmO)
Description	TVES pilot site employees must comply with a set of obligations.		
Implementation in OPTIMAI	SP-EmO-01. TVES pilot site employees shall fulfil the instructions to conduct the pilot activities, in accordance with the rules of good faith and diligence.		

	SP-EmO-02. TVES pilot site employees must observe all the health and safety measures in place for conducting the pilot activities.
--	---

6.7.3 Spain – Equality Law Requirements

Table 39 Spain Equality Law Requirements

ID	SP-EqR	Requirement	Equality Rights (EqR)
Description		TVES pilot site employees shall not be directly or indirectly discriminated against on the grounds of sex, marital status, age within the limits set by this law, racial or ethnic origin, social status, religion or beliefs, political ideas, sexual orientation, membership or not of a trade union, language, or disability.	
Implementation in OPTIMAI		<p>SP-EqR-01. TVES must respect the principle of equal treatment. This principle implies the absence of any direct or indirect discrimination based on racial or ethnic origin, religion or belief, disability, age, or sexual orientation. However, differences of treatment based on these protected characteristics shall not be considered as discrimination where the job concerned or of the context in which it is carried out, such a characteristic constitutes a genuine and determining requirement. To that end, the purpose must be legitimate, and the requirement proportionate.</p> <p>TVES is also obliged to respect equality of treatment and opportunities in the workplace, and, to this end, they must adopt measures aimed at avoiding any type of discrimination between women and men in the workplace.</p> <p>SP-EqR-02. TVES must refrain from all forms of harassment, discrimination, and victimisation both on the grounds of protected characteristics or any other.</p> <p>SP-EqR-03. TVES pilot site employees with disabilities have the right to work under conditions that guarantee the application of the principles of equal treatment and non-discrimination. TVES pilot sites must take appropriate measures to adapt the workplace and the accessibility to the shop floor, according to the needs of each specific situation. These measures shall be implemented to enable people with disabilities to perform their work, to progress professionally and to access training. If any OPTIMAI pilot activity, or any situation arising as a result of them, tends towards causing disadvantage to disabled workers, reasonable accommodations should be made to prevent such disadvantage.</p>	

6.7.4 Spain – Health and Safety Law Requirements

Table 40 Spain General Duties of Employers Requirements

ID	SP-GD	Requirement	General Duties of Employers (GD)
Description		TVES is required to protect pilot site employees against occupational health and safety risks following the general principles of prevention for managing health and safety risks.	
Implementation in OPTIMAI		<p>SP-GD-01. Avoiding health and safety risks and evaluating the risks that cannot be avoided.</p> <p>SP-GD-02. Combating the risks at source.</p> <p>SP-GD-03. Adapting the work to the individual, particularly regarding the design of workplaces, the choice of work equipment, working procedures, and production methods with the aim of mitigating monotonous work negative impacts on the employees' health.</p> <p>SP-GD-04. Adapting to technical progress.</p> <p>SP-GD-05. Replacing dangerous tasks or activities by non-dangerous or the less dangerous tasks or activities.</p> <p>SP-GD-06. Planning, developing, and implementing a prevention policy which integrate technology, organisation of work, working conditions, social relationships and factors related to the working environment.</p> <p>SP-GD-07. Prioritizing collective protective measures over individual ones.</p> <p>SP-GD-08. Providing appropriate instructions to pilot site employees. TVES must ensure that each employee receives sufficient and appropriate theoretical and practical training in preventive matters. Training must be delivered if there are changes in the working activities or when new technologies or changes in work equipment are introduced. Training should be specifically focused on the job performed by each employee, adapted to the evolution of risks and the emergence of new risks, and repeated periodically, if necessary.</p> <p>SP-GD-09. Evaluating the professional capabilities of their pilot site employees regarding health and safety at the time of allocating OPTIMAI pilot activities among them. Additional risks may arise from potential distractions among the employees. Consequently, appropriate preventive measures should be implemented to avoid foreseeable distractions among employees.</p>	

Table 41 Spain Duties of Employers with Regards to Equipment and Means of Protection Requirements

ID	SP-EDMP	Requirement	Duties of Employers with Regards to Equipment and Means of Protection (EDMP)
Description		To guarantee the health and safety of pilot site employees, TVES shall take the necessary measures to ensure that work equipment is suitable for the pilot activities to be carried out and that they are suitably adapted for that purpose.	
Implementation in OPTIMAI		<p>SP-EDMP-01. Where the use of work equipment is likely to present a specific risk to the safety and health of workers, TVES shall take the necessary measures to ensure:</p> <ul style="list-style-type: none"> - The use of the work equipment is reserved to those responsible for such use. - Repair, conversion, maintenance, or servicing work is carried out by employees specifically trained for that purpose. <p>SP-EDMP-02. As OPTIMAI partners will be supplying equipment to be used by pilot site employees, they should support TVES in complying with the safe use of that equipment. This support may entail:</p> <ul style="list-style-type: none"> i) providing safe equipment with understandable and accessible safety information and guidelines; ii) providing additional preventive safety measures that shall be implemented; and, iii) identifying potential safety and health risks that the supplied equipment may pose in terms of its normal use, inappropriate use, and misuse. <p>TVES must ensure that such information is provided to the pilot site employees in a comprehensive and accessible manner.</p>	

Table 42 Spain Risk Assessment and Management Requirements

ID	SP-RAM	Requirement	Risk Assessment and Management (RAM)
Description		TVES—with the support of partners, if necessary—must consider the necessity of and then if required conduct a health and safety risk assessment considering any dangers arising from OPTIMAI pilot and research activities and take adequate measures to mitigate those risks.	

<p>Implementation in OPTIMAI</p>	<p>SP-RAM-01. TVES shall carry out an initial assessment of the risks to the safety and health of workers arising from the OPTIMAI pilot activities. The assessment must include the nature of the pilot activity, the characteristics of the existing jobs and of the workers who are to perform them. The same assessment shall apply to the choice of work equipment and the layout of workplaces.</p> <p>SP-RAM-02. The assessment shall be updated when working conditions change. In any case, it shall be considered and reviewed, when any damage to health has already occurred.</p> <p>SP-RAM-03. Where the result of the assessment makes it necessary, TVES shall carry out regular checks of the working conditions and the activity of employees in the performance of their services to detect potentially dangerous situations. If the results of the assessment reveal risk situations, TVES shall carry out those preventive activities necessary to eliminate or reduce and control such risks. These activities shall be planned by the employer, including: i) the deadline for carrying out each preventive activity, ii) the designation of those responsible and, iii) the human and material resources necessary for its execution.</p> <p>SP-RAM-04. TVES shall specifically ensure the protection of workers who, due to their own personal characteristics or biological condition, including recognised physical, mental or sensory disabilities, are particularly sensitive to the risks arising from work.</p> <p>SP-RAM-05. TVES has the obligation to provide pilot site employees with relevant and comprehensive information regarding: i) the risks to the health and safety to which employees are exposed to; ii) and the preventive measures that must be put in place to avoid or minimize such risks</p>
---	--

Table 43 Spain Employee Duties, Capabilities, and Training Requirements

ID	SP-EDCT	Requirement	Employee Duties, Capabilities, and Training (EDCT)
Description			TVES—with the support of the rest of partners if necessary—must ensure that employees participating in or affected by OPTIMAI pilot activities are sufficiently empowered to protect their health and safety.
Implementation in OPTIMAI			SP-EDCT-01. Pilot site employees shall ensure their own health and safety at work, including the health and safety of other persons who may be affected by their tasks.

	<p>SP-EDCT-02. Pilot site employees shall:</p> <ul style="list-style-type: none"> - Properly use, in accordance with their nature and foreseeable risks, the machines, tools, transport equipment and, in general, any other means with which they carry out their activity. - Correctly use the means of protection and protective equipment provided by TVES, in accordance with the instructions received from TVES. - Make proper use of existing safety devices. - Immediately inform their direct line manager, and the employees designated to carry out protective and preventive activities or, where appropriate, the prevention service, of any situation which involves a risk to the safety and health of employees. - Contribute to the fulfilment of the obligations established by the competent authority in order to protect the safety and health of workers at work. - Cooperate with TVES to ensure safe working conditions that do not pose risks to the safety and health of employees.
--	---

Table 44 Spain Duty of Consultation Requirements

ID	SP-DC	Requirement	Duty of Consultation (DC)
Description		TVES—with the participation of partners, if necessary—must consult with pilot site employees or their representatives regarding health and safety matters related to OPTIMAI pilot and research activities.	
Implementation in OPTIMAI		<p>SP-DC-01. TVES has the duty of consulting its employees or their representatives before adopting relevant decisions that may affect:</p> <ul style="list-style-type: none"> - The planning and organisation of the pilot activities and the implementation of new technologies, in all matters relating to the consequences that these may have for the safety and health of employees, arising from the choice of equipment, the determination and suitability of working conditions and the impact of environmental factors at work. - The organisation and development of health protection and occupational risk prevention activities in the company, including the 	

	<p>designation of the employees in charge of these activities or the use of an external prevention service.</p> <ul style="list-style-type: none"> - The designation of employees in charge of emergency measures. - The information and documentation procedures referred to in Articles 18(1) and 23(1) of Law 31/1995. - The design and organisation of preventive training. - Any other action likely to have a substantial effect on the safety and health of employees.
--	---

7 Regulatory Framework to Support Lawful Conduct of Pilot Activities in Greece

7.1 Introduction

KLEE, or KLEEMANN HELLAS SA, is a company located in Greece that manufactures lifts and sells them across a number of international markets. KLEEMAN has over 30 years of expertise and experience in manufacturing lifts and also operates manufacturing sites in Serbia and China as well as subsidiaries in 15 more countries. Only KLEE's Greek site will be engaged over the course of the OPTIMAI project.

In order to support the lawful conduct of pilot site activities at KLEE, a cross-section of relevant Greek national law has been reviewed and will be presented here as an overview to support the end-user partner and responsible technical partners (supplying hardware and software tools and processing related data) in taking action to protect the rights and interests of pilot site employees, visitors, and any other persons affected by OPTIMAI pilot activities.

This section will present an overview of relevant provisions of Greek data protection law, employment law, equality rights law, and health and safety law.

Subsection 7.3 Data Protection Law will indicate the rights of data subjects and the responsibilities of data controllers and processors with particular regards for employment and research settings.

Subsection 7.4 Employment Law will lay out the rights of KLEE employees, particularly with regards to work hours, termination and telework.

Subsection 7.5 Equality Law will lay out employees' rights to not be discriminated against, harassed or victimised on the basis of protected characteristics, as well as duties regarding reasonable accommodations for persons with disabilities.

Subsection 7.6 Health and Safety Law lays out various requirements relating to the provision of safe working environments and equipment that facilitate employee welfare and empower employees to operate safely within the manufacturing environment.

Finally, actionable requirements are provided in **Subsection 7.7 Greece Data Protection, Employment and Equality, and Health and Safety Requirements**.

7.2 Pilot Description KLEE

Pilot activities at KLEE will be undertaken with a view to test three use cases (UC) of OPTIMAI solutions, including UC-1 zero defect quality inspection, UC-2 production line set-up calibration, and UC-3 production planning.

The following will briefly detail these use cases and their objectives, based on information collected by OPTIMAI technical partner ENG and provided by members of the OPTIMAI Consortium.

UC-1 Zero defect quality inspection. This use case will be applied to lift hydraulic power units. This is conducted in a test lab, a separate sound-proof room where “the operating conditions of each hydraulic lift order are simulated based on the building characteristics, investigating possible problems related to cracked pumps, oil flow rate and several re-adjustments in the hydraulic power unit”. This typically requires manual inspection and expert knowledge and is time consuming. The objective of this use case is the automation of the inspection process with a view to reducing costs related to quality control and production, and the identification of defects that are not identified through manual inspection in order to improve final product quality. This will be achieved through a suite of OPTIMAI solutions including sensors, tablets, augmented reality wearables and AI tools.

UC-2 Production line set-up and calibration. This use case aims to support optimal set-up of the hydraulic unit valve block. A solution will be developed to assist direct adjustments of the valve block based on quality control measurements from noise, vibrations and speed, and to facilitate human operators in rapidly adjusting the hydraulic unit's parameters. The objectives of this use case are to automate the calibration procedure in order to reduce calibration time and to improve the quality of the final product through set-up optimisation of the hydraulic power unit. This will be achieved through a suite of OPTIMAI solutions including sensors, tablets, augmented reality wearables and AI tools.

UC-3 Production Planning. For this use case, digital twins will be created of the hydraulic power unit that will be combined with AI models that map design choices to the power unit's performance and related defects. This digital manufacturing environment and simulation will allow mechanical engineers to explore the impact of different design choices and to combine the behaviour of the physical and virtual units during lab testing in order to rapidly identify discrepancies. The objectives of this use case are to reduce defective parts through improved unit design, and to connect virtual and physical quality control, thereby facilitating the implementation of corrective actions in line with virtual counterparts. This will be achieved through a suite of OPTIMAI solutions including sensors, tablets, augmented reality wearables and AI tools.

7.3 Data Protection Law

The legislation on the protection of personal data in Greece includes the General Data Protection Regulation (EU) 2016/679 (GDPR), and Law 4624/2019³⁶.

For the most part, Greek OPTIMAI Consortium partners are directed to **Section 4 The General Data Protection Regulation and Basic Data Protection Recommendations for OPTIMAI Pilot Activities** in order to support their compliance with the GDPR. Chapter C of Law 4624/2019 outlines supplementary measures for the implementation of the GDPR in Greece. Those

³⁶ Note: The national provisions have been criticized by commentators and the HDPa that in its Opinion 1/2020 indicated derogations from the wording used in Article 9(2) (g) and (h) GDPR that may lead to serious misinterpretations. The Authority pointed out especially that the legislative text repeats some of the provisions of Article 9 (2) GDPR without complying with the requirements set by EU Law – namely that it needs a clear and precise basis – with reference to Recital 41 GDPR.

provisions with particular relevance to OPTIMAI pilot and research activities will be outlined below.³⁷

7.3.1 Processing of Special Categories of Personal Data

Article 22(1)-(3) of Law 4624/2019 lays out exemptions to the processing of special categories of personal data. In derogation of Article 9(1) of the GDPR, public and private bodies may process special categories of personal data where it is:

- (a) for the purpose of exercising the rights arising from the right to social security and social protection, and for fulfilling the obligations arising therefrom;
- (b) for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or the management of health or social care systems or pursuant to a contract with a health professional or other person who is subject to a duty of professional secrecy or supervised by him/her; or
- (c) for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, in addition to the measures referred to in the second subparagraph of paragraph 3 [see below], the provisions ensuring professional secrecy provided for in a law or code of conduct must in particular be complied with.

Furthermore, public bodies may process such data where it is “strictly necessary for reasons of essential public interest”.

Specific measures necessary to safeguard the rights of data subjects are outlined in paragraph 3 of Article 22, which include:

- (a) technical and organisational measures to ensure that the processing complies with the GDPR;
- (b) measures to ensure that ex post verification and determination of whether and by whom personal data have been entered, amended or removed is possible;
- (c) measures to raise awareness among staff involved in the processing;
- (d) access rights restrictions to controllers and processors;
- (e) pseudonymisation of personal data;
- (f) encryption of personal data;
- (g) measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services relating to the processing of personal data, including

³⁷ The English translation of this law was used as source material: [https://www.dpa.gr/sites/default/files/2020-08/LAW%204624 2019 EN TRANSLATED%20BY%20THE%20HDPA.PDF](https://www.dpa.gr/sites/default/files/2020-08/LAW%204624%2019%20EN%20TRANSLATED%20BY%20THE%20HDPA.PDF)

the ability to rapidly restore the availability and access in the event of a physical or technical incident;

- (h) procedures for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- (i) specific rules to ensure compliance with this Law and the GDPR in case of transfer or processing for other purposes;
- (j) designation of a DPO.

7.3.2 Processing of Personal Data in the Context of Employment

Article 27 of Law 4624/2019 lays out data controller responsibilities with regards to the processing of personal data in the employment context. According to Article 27(1) employee personal data “may be processed for the purposes of the contract of employment where the processing is strictly necessary for deciding whether to enter into a contract of employment, or for the performance of a contract of employment once it has been concluded”.

Paragraph 2 deals with the issue of consent of employees. Where an employee’s consent is used as an authorising criterion, the following two points must be considered:

- (a) the employee’s dependence, as set out in the contract of employment and
- (b) the circumstances under which consent was given.

It should be noted, that the Hellenic Data Protection Authority (HDPa) affirmed in its Opinion 1/2020 that the case of processing for the carrying out the obligations and exercising rights in the field of employment, social security and social protection law there is neither a specification of rights nor clarification if the law refers to rights of the data controller or the data subject.

Furthermore, again, the circumstances of the employee-employer relationship militate against consent as being a suitable basis for most data processing operations in the employment context. The HDPa expressed the opinion that the reference to the employment contract as sole legal ground is contrary both to Article 88 (1) and 6 (1) GDPR and results in far reaching restrictions of rights and freedoms of employees in their workplace. According to Opinion 1/2020 of the HDPa, consent is acceptable as legal basis only if all other legal grounds are not applicable and the conditions set in Articles 4 (11) and 7 GDPR are strictly respected.

Paragraph 4 permits the processing of special categories of personal data:

if it is necessary for the exercise of their [the employees’] rights or for compliance with legal obligations arising from employment, social security and social protection law, and there is no reason to believe that the data subject’s legitimate interests in relation to processing take precedence.

Where consent is used for such operations, again points a) and b) above should be referred to.

Paragraph 7 prohibits the processing of personal data through CCTV unless it is necessary for the protection of persons and goods, thereby ruling out performance assessment. Employees

are to be informed in writing of the installation and operation of CCTV. Nevertheless, the HDPa has emphasized that the specification of the rules in national legislation does not comply with the conditions set in Article 88 (2) GDPR, ie. the introduction of suitable and specific measures.

It is worth mentioning here that the HDPa has issued in 2001 “Recommendation on Data Protection in the workplace”. It is not a binding legal instrument in a strict sense but more of a kind of “soft law”. However the HDPa has based its interpretation and position in relation to the application of the general rules in this specific employment context also on this Recommendation. The HDPa regards its recommendations applicable (also after the entry in force of GDPR) if and to the extent that these Recommendations are not contrary to the provisions of the GDPR.

7.3.3 Processing and Freedom of Expression and Information; for Archiving Purposes in the Public Interest; and Scientific or Historical Research Purposes or for the Collection and Maintenance of Statistical Information

Articles 28-30 of Law 4624/2019 broadly deal with the responsibilities of data controllers pertaining to processing operations in service of the public good and for the exercise of the rights to freedom of expression and information.

These articles provide for derogation and restriction of data subject rights “where the exercise of that right is likely to render impossible or seriously impair the achievement of the objectives” of the processing operation. Nevertheless, adequate measures must be taken to secure data subject rights, particularly:

- (a) access rights restrictions to controllers and processors;
- (b) pseudonymisation of personal data;
- (c) encryption of personal data;
- (d) designation of a DPO.

7.3.4 Rights to information, access, and erasure

Articles 31 to 35 of Law 4624/2019 clarify the implementation of data subject rights and exemptions in Greece.

It is worth to note that the HDPa has explicitly stated that, within its enforcement powers, it will interpret the provisions of the GDPR Implementation Law in the context of the GDPR, and they shall assess the validity of these provisions from the perspective of compliance with the GDPR and the Data Protection Law Enforcement Directive. According to the DPA, the Law 4624/19 does not conform to the substantial and procedural requirements of Article 23 (2) GDPR, i.e. the adoption of specific provisions containing at least the purposes of processing, scope of restrictions, safeguards to prevent abuse, risks etc. It is noteworthy that the Authority in its Opinion 1/2020 has announced that it will assess on a case by case basis, if and to what extent the restrictions introduced by the national legislation violate the GDPR as well as the requirements set out in the Charter and ECHR.

Pursuant to Article 31(1), regarding the right to information to be provided to the data subject, the following exemptions exist, which are where the data:

- (a) concerns further processing of data stored in a written form in which the controller directly addresses the data subject, the purpose is compatible with the original purpose of collection in accordance with the GDPR, communication with the data subject is not in digital form and the interest of the data subject in being informed according to the circumstances of the case, in particular as regards the context in which the data have been collected, is not deemed to be high;
- (b) in the case of a public body, would compromise the proper performance of the controller's tasks within the meaning of points (a) to (e) of Article 23(1) of the GDPR, and the interest of the controller in not providing information overrides the data subject's interest;
- (c) would compromise national or public security, and the interest of the controller in not providing information overrides the data subject's interest;
- (d) would prevent the establishment, exercise or defence of legal claims, and the interest of the controller in not providing information overrides the interest of the data subject;
- (e) would compromise the confidentiality of the data transfer to public bodies.

However, the data controller must still furnish reasons for forgoing the provision of information to the data subject.

With regards to the provision of information where the data has not been collected from the data subject, the following exemptions apply:

(a) in the case of public bodies:

(aa) would compromise the proper performance of the controller's tasks within the meaning of points (a) to (e) of Article 23(1) of the GDPR, or (bb) would compromise national or public security; and, therefore, the data subject's interest in obtaining the information recedes,

(b) in the case of private bodies:

(aa) would prejudice the establishment, exercise or defence of legal claims, or the processing includes personal data resulting from contracts established under private law and is aimed at preventing damages caused by criminal offences, unless the data subject has an overriding legitimate interest in obtaining the information; or (bb) the competent public authority has specified to the controller that the publication of the data would compromise national defence, national security and public security...

Where the information is not provided to the data subject, the data controller must provide reasons for not providing the information, and:

the controller shall take appropriate measures to protect the data subject's legitimate interests, including the provision to the public of the information referred to in Article

14(1) and (2) of the GDPR in an accurate, transparent, intelligible and easily accessible form, in clear and plain language.

The right of access to the data subject may be restricted on the following grounds:

- (a) the data subject is not informed in accordance with point (bb) of indents (a) and (b) of paragraph 1 of the previous Article; or
- (b) the data (aa) were recorded only because they cannot be erased due to retention requirements provided for in legal or regulatory provisions, or
- (bb) only serve purposes of protection or control of data, and the provision of information would require a disproportionate effort, and the necessary technical and organisational measures render impossible their processing for other purposes.

The reasons for refusal should be documented and justified “unless the disclosure of the factual or legal reasons on which the refusal is based would compromise the purpose pursued by the refusal to provide information”.

Where processing is non-automated and erasure is not possible without disproportionate effort and the risks to the data subject are not significant, the right to erasure of the data subject does not apply with the exception of provisions as laid out in Article 17(3) of the GDPR.

The right to object is not applicable “where a public body is concerned, if there is a compelling public interest in the processing which overrides the interests of the data subject or if processing is mandatory by law”.

7.4 Employment Law

The Greek legal framework enshrines various protections including for employees’ wages, protection against unjustified detriment at work, protection from unfair dismissal, time-off work etc. Articles 648 to 680 of the Greek Civil Code on “contract of employment” are the basic provisions that govern the employment relationship between employers and employees. In addition, the Greek Parliament has recently adopted the new Greek Employment Law No. 4808/2021, which includes provisions regarding the digital employment card, Employment Inspection Authority, health and safety, prevention of violence and harassment at the workplace, balance of work and family life, remote working, work schedule, termination of employment, employees’ unions etc.

Key points stemming from Greek employment law of relevance to KLEE and OPTIMAI pilot and research activities include [28, 29]:

- employees may not undertake more than 150 hours overtime per year
- standard working hours are 40 per week for full-time employees
- terminations of employees should be for objectively justifiable reasons and prohibited where employees exercise their lawful rights
- employees may request telework whilst there is a documented risk to their health at the place of employment

- employees have a right to disconnect.

It is incumbent on all partners, especially KLEE as employer, to ensure that any interactions with and requirements of Greek employees arising as a result of OPTIMAI research and pilot activities do not endanger employees' enjoyment of the rights enshrined in Greek Law. Employers have extensive obligations under the employment legal framework which they are expected to honour in full.

7.5 Equality Law

The OPTIMAI Consortium recognises the importance of inclusive and non-discriminatory research activities and supporting working environments free from discrimination in all its forms. To that end, the OPTIMAI Consortium must comply with relevant ethical principles and national legislation to ensure fair treatment of all persons affected by its research and pilot activities.

In Greece, equality and non-discrimination are enshrined in Law 4443/2016 which prohibits discrimination at work and in employment.

7.5.1 Protected Characteristics

Law 4443/2016 prohibits discrimination on the basis of the following personal characteristics [30]:

- Race
- Colour
- National or ethnic origin
- Genealogical descent
- Religion or other belief
- Disability or chronic condition
- Age
- Social status
- Sexual orientation
- Gender identity or gender characteristics

7.5.2 Discrimination and harassment prohibitions as understood by Law 4443/2016

Law 4443/2016 understands direct discrimination as referring to situations where one person receives favourable treatment compared to that received or would be received by another person in a similar situation due to one of the protected characteristics listed above [30]. Indirect discrimination occurs where “a provision, criterion or practice of a neutral nature” affects a group sharing a protected characteristic in a manner more negatively than other persons in a similar situation [30]

Of particular relevance to OPTIMAI, Law 4443/2016 prohibits discrimination based on “the terms and conditions of work and employment, in particular as regards remuneration, dismissal, health and safety at work and in the event of unemployment, rehabilitation and re-employment” [30].

Harassment is understood as discrimination where “unwanted conduct” in relation to protected personal characteristics with the purpose or effect of violating the person’s dignity and “of creating an intimidating, hostile, degrading, humiliating or offensive environment” [30]. Law 4808/2021 requires that companies of more than 20 persons adopt policies preventing violence and harassment in the workplace, laying out the rights and obligations of employees and employers and policies relating to handling and investigation of complaints [28, 29]. Greek employers must conduct a *psychosocial risk assessment*, including of those stemming from different kinds of harassment, and put in place mitigation measures to those psychosocial risks [29].

A notable provision in Greek Law 4808/2021 includes a prohibition of retaliation, that is, the employer is prohibited from terminating employment of an employee or being responsible for any other unfavourable treatment towards them where the employee pursues their legal rights in response to cases of harassment etc. [29].

It should be noted that any acts of discrimination, harassment and victimisation can be more widely construed and could be applicable to any unjustifiable distinctions (or conduct arising from complaints) made between persons with different or combined personal characteristics in relation to project participants and their role in OPTIMAI project activities (for example, recruitment and selection processes for research participants). Indirect discrimination may also apply where research activities disadvantage persons based on their personal characteristics in ways that do not satisfy a legitimate aim (perhaps the absolute requirement of testing equipment incompatible with disability where no reasonable effort is made to accommodate that disability).

There are notable exceptions to this law. Differences in treatment may not be prohibited in such cases where “due to the nature or context of the professional activities it constitutes an essential and fundamental professional prerequisite, and provided that the objective in question is legitimate and the condition is proportional” [30].

7.5.3 Reasonable Accommodations

Law 4443/2016 requires that measures towards reasonable accommodations be implemented in order that all persons, without discrimination, can access a job, perform in it and progress through it, and avail of vocational training opportunities so long as these measures do not place a disproportionate burden on the employer [30].

As such, employers are expected to make reasonable accommodations for persons based on their disability, and end-user partners should evaluate whether any such adjustments can be applied to OPTIMAI research and pilot activities.

7.6 Health and Safety Law

The health and safety of OPTIMAI end-user employees is paramount, and ensuring their continued safety and welfare over the course of OPTIMAI research and pilot activities should be a priority.

With regard to issues of health and safety at work, employers have the obligations laid down in Articles 5 to 12 of Framework Directive 89/391/EEC transposed into Greek law by virtue of Presidential Decree 17/1996 and codified by virtue of Law 3850/2010. More specifically, Law 3850/2010 stipulates that employers must use the services of a safety technician, and in particular circumstances, an occupational physician.

7.6.1 The Roles of Safety Technician and Occupational Physician

A suitably qualified safety technician (ST) must be employed in the workplace, who will be responsible for advising the employer, employees and their representatives with regards to matters of health and safety. The Government of Greece has outlined their particular responsibilities, stating that the technician [31, 32]:

- advises on the design, planning, construction and maintenance of installations, on the introduction of new production processes, on the supply of resources and equipment, on the choice and efficacy of personal protective equipment and on the configuration and layout of workstations and the working environment and the organisation of the production process in general;
- inspects the safety aspects of installations and technical resources prior to their commissioning and of production processes and working methods prior to their introduction and oversees the application of measures to ensure safety and health at work and prevent accidents by informing the relevant line managers or senior management.

Additionally, the safety technician is mandated to inspect the safety of work stations and report on issues and make mitigation recommendations; oversee the correct use of PPE; investigate and analyse causes of accidents; oversee fire and alarm drills; inform employees of health and safety risks and rules and ensure that employees are abiding by the rules and avoiding health and safety risks; and attend and organise health and safety training for employees [31].

As such, it is essential for KLEE to adequately inform the safety technician of any new workplace processes and activities introduced to the workplace as a result of OPTIMAI research and pilot actions. The safety technician therefore will be an invaluable asset in monitoring and supporting workplace safety and advising on the appropriate integration of OPTIMAI solutions and their use as well as any alterations that may need to be made to the physical environment in order to facilitate their safe use.

Under Presidential Decrees 94/87, 70A/88, 399/94 and 186/95, as amended, undertakings of over 50 employees (or just one if they work with lead, asbestos or biological or carcinogenic agents) must have a suitably qualified occupational physician (OP) [33, 34]. The occupational physician makes recommendations pertaining to measures to ensure employees' physical and

mental health. As outlined verbatim by the Government of Greece, the occupational physician advises on [35]:

- the design, planning and modification of the production process and the construction and maintenance of installations in keeping with safety and health at work rules;
- the protective measures required during the introduction and use of materials and the supply of equipment;
- the physiology and psychology of work, ergonomics and health at work, the configuration and layout of workstations and the work environment and the organisation of the production process;
- the organisation of the first aid service;
- the initial placement of and temporary or permanent changes to workstations for health reasons and the integration or reintegration of disadvantaged persons in the production process, including recommended adaptations to the workstation;
- but the occupational physician cannot be asked to verify whether or not a worker's absence due to illness is justified.

Of particular relevance to OPTIMAI, the occupational physician is required to carry out medical examinations of workers to ensure fitness of work following change of workstation and evaluate the suitability of workers for particular jobs [35]. Furthermore, as outlined verbatim by the Government of Greece [35], the occupational physician:

- inspects workstations at regular intervals and reports any issues, proposes measures to address the issues and oversees their application;
- explains why personal protective equipment needs to be used correctly;
- investigates the causes of occupational illnesses, analyses and evaluates the results of the investigation and recommends measures to prevent such illnesses;
- oversees compliance by the workers with the safety and health at work rules, informs them of the risks inherent in their work and advises on how to avoid them;
- provides urgent treatment in the event of an accident or sudden illness; and carries out vaccination programmes for workers on the instructions of the public health department of the prefecture in which the undertaking is located.

KLEE therefore requires the services of a suitably qualified occupational physician whom should also be adequately informed of OPTIMAI driven changes to the workplace and may be required to evaluate the medical fitness of participating employees [35].

Employers are required to conduct an occupational health and safety risk assessment with the ST and OP, or an external service, and for the purposes of OPTIMAI should consider reviewing existing assessments [36].

7.6.2 Duties linked to Directive 89/391/EEC

The health and safety obligations of Greek employers stem from Directive 89/391/EEC which, as mentioned, has been transposed into Greek law. Key provisions from this directive with relevance to OPTIMAI will be outlined here.

Firstly, Article 6(2) of the Directive lays out the principles of prevention, which are:

- (a) avoiding risks;
- (b) evaluating the risks which cannot be avoided:
- (c) combating the risks at source;
- (d) adapting the work to the individual, especially as regards the design of work places, the choice of work equipment and the choice of working and production methods, with a view, in particular, to alleviating monotonous work and work at a predetermined workrate and to reducing their effect on health.
- (e) adapting to technical progress;
- (f) replacing the dangerous by the non-dangerous or the less dangerous;
- (g) developing a coherent overall prevention policy which covers technology, organization of work, working conditions, social relationships and the influence of factors related to the working environment;
- (h) giving collective protective measures priority over individual protective measures;
- (i) giving appropriate instructions to the workers.

Article 8(1)-(5) lays out the employer's responsibility with regards to fire, first-aid and evacuation. The employer is required to take measures for first aid, fire safety and the evacuation of employees based on the nature of activities and size of the undertaking, as well as arrange contacts with any related and relevant external services that can help achieve and support these aims. The employer is to designate employees to implement these measures. Employers are to inform employees who may be exposed to serious and imminent danger of the risks as well as take steps for their protection; take action and give instructions to employees in serious, imminent and unavoidable danger to stop working and evacuate; and are required to refrain from asking employees in most circumstances from working in dangerous situations. Employees are not to face any detriment for leaving their work stations due to any such dangers. The employer is also required to ensure that employees are suitably empowered to take steps to use any means at their disposal to protect themselves when immediate superiors cannot be contacted, again without facing any detriment from the employer.

Article 9(1)-(2) lays out additional obligations held by employers. The employer must carry out a health and safety risk-assessment; decide on protective measures to be taken based on this and protective equipment to be used; and keep a list of accidents causing workers to be unfit. Relatedly, by Law 3850/2010 all accidents are required to be reported within 24 hours of occurrence [37].

Article 10(1)-(3) outlines the employer's responsibility with regards to worker information. The employer is required to impart information to employees (and employers of employees engaged on the premises) related to "the safety and health risks and protective and preventive measures and activities in respect of both the undertaking and/ or establishment in general and each type of workstation and/ or job".

Article 11(1)-(6) lays out obligations of the employer relating to the consultation and participation of workers, requiring employers to consult with employees and/or their representatives on all questions relating to health and safety. Representatives (such as ST) have the right to request measures be taken to mitigate hazards and submit such proposals to them. The employees/representatives can appeal to the national health and safety authority if they believe such measures are inadequate. Employee representatives may submit their observations to the authority during inspection.

Article 12(1)-(4) enshrine the duty to provide adequate training pertaining to health and safety risks at work, triggered for reasons including change in equipment or the introduction of new technologies.

Article 13(1)-(2) lays out worker obligations. The worker is responsible for, as far as possible, their health and safety and of those affected by their acts or omissions at work, in accordance with training and instructions by the employer, entailing responsible use of equipment, installations and the environment, PPE, reporting to responsible persons serious dangers, and to cooperate with tasks relating to health and safety.

Article 15 requires that specific risks be mitigated for at-risk groups (for example, ensuring wheel chair ramps are present to support swift evacuation of persons in wheelchairs).

7.7 Greece Data Protection, Employment and Equality, and Health and Safety Law Requirements

7.7.1 Greece (GR) – Data Protection Law Requirements

Table 45 Greece Lawful Basis Requirements

ID	GR-LB	Requirement	Lawful Basis
Description	Utilise an appropriate lawful basis for each data processing operation associated with OPTIMAI pilot activities.		

<p>Implementation in OPTIMAI</p>	<p>GR-LB-01. Consent will only be an appropriate legal basis for data processing where it is freely given, specific, informed and given by unambiguous agreement. Data subjects should be able to withdraw this consent at any time. In the employment or workplace context, the consent of employees may only be valid for minor matters where free choice can be demonstrated, such as image publication in deliverables or media releases. Other data subjects to consider include pilot site visitors subject to data collection.</p> <p>GR-LB-02. Consent should not be relied upon in cases where there is a clear power imbalance between data subject and controller/processor, such as the employer-employee relationship, where genuine free choice cannot be demonstrated. KLEE operators and other employees who are piloting OPTIMAI technologies or are within range of personal data collecting sensor devices, or are otherwise required to supply personal data over the course of research activities, are unlikely to be in a position to provide appropriate consent.</p> <p>GR-LB-03. In cases where consent cannot be relied upon, data controllers should consider whether legitimate interest or another basis is an appropriate lawful basis for data processing. A balancing test should be performed and documented with the assistance of a legitimate interest assessment. KLEE and others identified as data controllers should conduct this legitimate interest assessment in advance of processing personal data in relation to pilot activities.</p> <p>GR-LB-04. Where consent is inappropriate, data controllers should ensure that data processing activities are of a nature that could reasonably be expected by employees.</p>
---	---

Table 46 Greece Special Categories of Data Requirements

ID	GR-SCD	Requirement	Special Categories of Data
<p>Description</p>		<p>The processing of special categories of data in connection with OPTIMAI pilot activities shall be prohibited without appropriate justification and safeguards or unless otherwise subject to exemption or derogation (see Subsection 7.3.1 Processing of Special Categories of Personal Data).</p>	

Implementation in OPTIMAI	<p>GR-SCD-01. Consent for the processing of special categories of personal data should be explicit, freely given, specific, informed and given by unambiguous agreement. Data subjects should be able to withdraw this consent at any time. In the employment or workplace context, the consent of employees may not be valid.</p> <p>GR-SCD-02. Consent for processing of special categories of data should not be relied upon in cases where there is a clear power imbalance between data subject and controller/processor, such as the employer-employee relationship, where genuine free choice cannot be demonstrated.</p> <p>GR-SCD-03. In OPTIMAI, special categories of personal data may be processed on the basis of public interest, scientific or historical research purposes, reasons of substantial public interest, or employment including appropriate health assessments, social security and social protection. The reasons should be appropriately identified and documented.</p> <p>GR-SCD-04. KLEE and partners should ensure that comprehensive Technical Security Measures and organisational measures are implemented to protect the rights of data subjects whose special categories of data are processed.</p>
--------------------------------------	---

Table 47 Greece Data Controller and Processor Requirements

ID	GR-DCP	Requirement	Data Controller and Processor
Description			<p>Data controllers and processors should correctly identify themselves and comply with Greek data protection requirements arising as a result of their controllership or by dint of being processor.</p>
Implementation in OPTIMAI			<p>GR-DCP-01. Consortium partners must identify whether they are data controllers, processors, or party to joint controllerships with regards to specific data processing operations.</p> <p>GR-DCP-02. Data controllers and processors must ensure appropriate security, technical and organisational measures are implemented that protect the rights and freedoms of data subjects.</p> <p>GR-DCP-03. Joint controllers must transparently determine their respective responsibilities and should designate a contact point for data</p>

	<p>subjects.</p> <p>GR-DCP-04. Whereby it is determined that a partner is acting as a data processor for a data controller, the relationship must be governed by a contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.</p> <p>GR-DCP-05. Data processors and controllers should keep appropriate records of data processing activities.</p> <p>GR-DCP-06. Data controllers must conduct, at a minimum, data protection impact assessment threshold analyses prior to data processing activities and a DPIA where the outcome of such analysis indicates that data processing is of high risk to data subjects.</p> <p>GR-DCP-07. Data controllers and processors must notify data subjects and the applicable data protection authority of any breach in a timely manner.</p> <p>GR-DCP-08. Data controllers should ensure that data is processed for specific lawful purposes, in line with the principles of data minimisation, and that such data is made available only to persons as necessary for achieving those purposes and should implement audit trails to log who has access to personal data. Further processing should not be undertaken unless exceptions apply. Data should be retained only as long as necessary to achieve their purpose, or as long as required to meet any other legal obligation.</p>
--	---

Table 48 Greece Data Subject Rights Requirements

ID	GR-DSR	Requirement	Data Subject Rights
Description	Subject to particular exemptions (see Data Protection), to the maximum extent practicable the rights of OPTIMAI data subjects must be upheld and protected.		

**Implementation
in OPTIMAI**

GR-DSR-01. The data controller is to communicate all relevant information to the data subject (who could be an employee of KLEE or a site visitor, for example) in a concise, transparent, intelligible and easily accessible form, and must be aware that duties apply even where personal data was not collected by the data controller.

GR-DSR-02. The data subject must be notified about data processing activities and be given access to any data held about them and related information including about their rights and purposes of data processing. The data controller shall implement means to verify the identity of any persons making subject access requests.

GR-DSR-03. The data subject has the right to have incorrect information about them corrected and have incomplete information corrected including by supplementary statement.

GR-DSR-04. The data subject has the right for their data to be erased where it is no longer necessary; consent is withdrawn; they object to processing; the data has been unlawfully processed; etc.

GR-DSR-05. The subject has the right to have data processing restricted where the personal data's accuracy is contested; processing is unlawful and the subject requests restriction rather than erasure; the controller no longer has use for the data but the data subject does (e.g., for a legal claim); or the data subject has objected pending verification of whether the grounds of the controller override the subject's interest.

GR-DSR-06. The data subject has the right to receive their personal data "in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided", where the processing is based on consent or is carried out by automated means.

GR-DSR-07. The data subject has the right to object to processing of their personal data and the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

GR-DSR-08. The data subject has the right not to be subject to automated decision-making including profiling with legal (or similar)

	effects. Exceptions arise based on performance of contract, authorisation by law, and where explicit consent is obtained from the data subject.
--	---

Table 49 Greece International Data Transfer Requirements

ID	GR-IDT	Requirement	International Data Transfers
Description		International data transfers and transfers to international organisations should only take place where the rights and freedoms of data subjects can be ensured, and subject to applicable exemptions and derogations.	
Implementation in OPTIMAI		GR-IDT-01. Data controllers and processors must, subject to derogations, transfer data to third countries and international organisations only where there are appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.	

7.7.2 Greece – Employment Law Requirements

ID	GR-EmR	Requirement	Employment Rights
Description		OPTIMAI partners, especially KLEE, should not impinge on the employment rights of pilot site workers.	
Implementation in OPTIMAI		<p>GR-EmR-01. KLEE employee research participants must not be required to work more than the standard work hours plus statutorily permissible overtime hours, particularly due to responsibilities stemming from engagement with OPTIMAI research and pilot activities.</p> <p>GR-EmR-02. KLEE employee research participants must not be dismissed for any activities arising as a result of their participation in OPTIMAI unless they would normally be justifiable grounds for dismissal.</p> <p>GR-EmR-03. Where practicable and applicable, participation in OPTIMAI research and pilot activities must not prevent KLEE employee research participants from authorised teleworking.</p>	

Table 50 Greece Employment Law Requirements

7.7.3 Greece – Equality Law Requirements

Table 51 Greece Equality Law Requirements

ID	GR-EqR	Requirement	Equality Rights
Description		All partners, especially the KLEE as end-user partner, must adhere to equality law with respect to the rights of pilot site workers and other applicable individuals.	
Implementation in OPTIMAI		<p>GR-EqR-01. In overseeing and managing OPTIMAI pilot and research activities, partners must refrain from making decisions that would treat individuals less favourably than others on the basis of protected characteristics or would otherwise disadvantage them on that basis. An indicative example would be an obligation to wear hardware that is incompatible with religious dress, or excluding persons from participation in pilot and research activities on the basis of protected characteristics without legitimate justification.</p> <p>GR-EqR-02. All OPTIMAI partners must refrain from all forms of harassment, discrimination and victimisation on the grounds of protected characteristics or any other.</p> <p>GR-EqR-03. If any OPTIMAI pilot or research activities or something arising as a result of them would tend towards causing disadvantage to disabled workers in the pilot site, reasonable accommodations should be made to prevent any such disadvantage.</p> <p>GR-EqR-04. KLEE must ensure that it has adopted and is adequately implementing anti-harassment policies to protect OPTIMAI research participants operating at the pilot site, including having taken such measures as conducting and actioning a psychosocial risk assessment.</p>	

7.7.4 Greece – Health and Safety Law Requirements

Table 52 Greece Safety Technician and Occupational Physician Requirements

ID	GR-STOP	Requirement	Safety Technician and Occupational Physician
Description		KLEE, with the support of partners, must ensure that the roles of safety technician and occupational physician are filled and these actors are sufficiently facilitated in supporting a safe working environment.	

Implementation in OPTIMAI	<p>GR-STOP-1. A suitably qualified safety technician and occupational physician should be active in the KLEE pilot site and should be promptly informed and consulted about all changes to work processes and environment occurring as a result of OPTIMAI research and pilot activities. The safety technician should be present at relevant technical meetings to support their work.</p> <p>GR-STOP-2. The ST and OT should be provided with any relevant OPTIMAI documentation and physical devices or access to workspaces for inspection.</p> <p>GR-STOP-3. If necessary, the OT should be facilitated in carrying out any medical exams of KLEE employee research participants in connection with their participation in OPTIMAI pilot and research activities.</p> <p>GR-STOP-4. KLEE, and technical partners if required, should implement hardware/process changes based on any recommendations that might be made by the ST and OP.</p>
--------------------------------------	--

Table 53 Greece Risk Assessment and Management Requirements

ID	GR-RAM	Requirement	Risk Assessment and Management
Description			<p>KLEE must, with the support of partners if necessary, consider the necessity of and then if required conduct a risk assessment taking into account any dangers arising from OPTIMAI pilot and research activities, and take adequate measures to mitigate those risks.</p>
Implementation in OPTIMAI			<p>GR-RAM-01. KLEE, with the support of partners where necessary, prima facie, must make a suitable and sufficient assessment of the risks to the health and safety of employees to which they are exposed whilst they are at work; and the risks to the health and safety of persons not in their employment arising out of or in connection with the conduct by him of their undertaking, specifically with reference to changes OPTIMAI research and pilot activities will bring about to processes and the working environment. If necessary, this should also be conducted with a view to identifying and mitigating fire safety risks. A justification should be provided if KLEE believes this unnecessary. The risk assessment should be reviewed if necessary.</p> <p>GR-RAM-02. Documented measures should be implemented to mitigate the risks identified, and there should be health surveillance in relation to identified risks.</p>

	GR-RAM-03. Employees should be informed with relevant and comprehensible information about the risks to their health and safety identified by the assessment; the preventive and protective measures; and any other meaningful information required in support of their health and safety.
--	---

Table 54 Greece Employee Duties, Capabilities, and Training Requirements

ID	GR-EDCT	Requirement	Employee Duties, Capabilities, and Training
Description	KLEE, with the support of partners where necessary, must ensure that employees participating in or affected by OPTIMAI pilot activities are sufficiently empowered to protect their health and safety.		
Implementation in OPTIMAI	<p>GR-EDCT-01. KLEE employees have duties to themselves and others as enshrined in the law, and must use equipment in a careful manner as they were trained to do, and have responsibility for their health and safety as well as others'. OPTIMAI partners must reasonably support this.</p> <p>GR-EDCT-02. KLEE with the support of OPTIMAI partners must provide adequate health and safety training for new equipment and technologies.</p>		

Table 55 Greece Other Duties Requirements

ID	GR-OD	Requirement	Other Duties
Description	KLEE must ensure that it complies with all statutory duties relating to the health and safety of its employees and site visitors, being mindful of changes to the environment and work processes caused by OPTIMAI pilot and research activities		

<p>Implementation in OPTIMAI</p>	<p>GR-OD-01. KLEE must ensure adequate accessibility and availability of medical stations, fire safety equipment and fittings, and escape routes and any other measures necessary to protect the health and safety of employees and site visitors.</p> <p>GR-OD-02. KLEE, with assistance of partners if necessary, must inform employees of any health and safety risks arising from OPTIMAI research and pilot activities or from any resulting changes to the environment and work processes and any preventive measures to secure their health and safety.</p> <p>GR-OD-03. OPTIMAI KLEE employee research participants must not suffer any unfavourable treatment for refusing to take part in any OPTIMAI research activities/use of any devices that present a risk to their health and safety, and should also not face unfavourable treatment if required to take any reasonable action available to them to secure their health and safety.</p> <p>GR-OD-04. If any element of OPTIMAI research or pilot activities or something arising as a result of them causes risks to specific at-risk groups, measures should be taken to mitigate these risks.</p>
---	---

8 Conclusion

This deliverable has offered a comprehensive (though not exhaustive) overview of national law applicable to research activities undertaken in pilot sites in the UK, Spain, and Greece. Relevant areas of law that were evaluated include data protection law, employment law, equality law, and health and safety law. These areas of law were chosen based on the context of research taking place in an industrial employment context that would utilise hardware devices capable of multimedia data capture, in environments that could feature health and safety risks for human research participants. Furthermore, these areas of law were chosen to help support both end-user partners and technical partners in conducting research that does not undermine the rights inherent to employees as enshrined in national law in the respective pilot countries with regards to their working conditions, and to help ensure that all activities are inclusive and non-discriminatory.

Legal requirements have been formulated based on our understanding of the national legal context, as well as bearing in mind the provisions of the GDPR, and are presented in **Subsections 4.3 Basic Data Protection (BDP) Requirements for OPTIMAI Pilot Activities; 5.7 UK Data protection, Employment and Equality, and Health and Safety Law Requirements; 6.7 Spain Data Protection, Employment and Equality, Health and Safety Law Requirements; and 7.7 Greece Data Protection, Employment and Equality, and Health and Safety Law Requirements.**

End-user partners, as well as technical partners where necessary, are enjoined to adhere to all legal requirements presented, as well as adhering to national law and international law and regulations more broadly and to the extent that any of their existing obligations are not defined in this deliverable. Partners are urged to document measures taken to adhere to these requirements and share them with ethical and legal partners (UAB and TRI) in order to support them in their ethical and legal monitoring responsibilities.

End-user partners and technical partners must also observe the ethical requirements applicable to the OPTIMAI piloting activities presented in this Deliverable (See **Section 3 Ethical Procedures and Guidelines for Pilot Activities**), as well as the general ethical requirements included in *D9.1* and *D2.1*. Likewise, end-users must follow the ethical recommendations provided by the OPTIMAI Ethics Board in Section 3, who will be monitoring the execution of the piloting activities from an ethical and legal perspective together with UAB and TRI. Lastly, the CERTH Ethical Panel is currently assessing the piloting activities and the legal and ethical requirements, mitigation measures and procedures that have been provided by UAB and TRI to grant the Ethical Approval that would allow the start of the pilot activities.

9 References

1. van de Poel, I. (2013). Translating Values into Design Requirements. In D. P. Michelfelder, N. McCarthy, & D. E. Goldberg (Eds.), *Philosophy and Engineering: Reflections on Practice, Principles and Process* (pp. 253–266). Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-007-7762-0_20
2. Hashmi, M., Casanovas, P., & de Koker, L. (2018). Legal Compliance Through Design: Preliminary Results. In *Proceedings of the 2nd Workshop on Technologies for Regulatory Compliance* (pp. 59–72). Presented at the TERECON 2018 Technologies for Regulatory Compliance, Groningen, Netherlands.
3. Carr Communications. (2021, August 23). Pilots. Retrieved from <https://optimai.eu/optimai-pilots/>
4. Wright, D., Barnard-Wills, D., Cochrane, L., Garstka, K., Gurzawska, A., Hughes, J., ... Warso, Z. (nd). The Touchpoint table: A new methodology for ethical, data protection and societal impact assessment of projects. *unpublished paper*.
5. Silverman, D. (2013). *Doing Qualitative Research: A Practical Handbook* (4th ed.). Great Britain: SAGE Publications Ltd.
6. Foddy, W. (1994). *Constructing Questions for Interviews and Questionnaires: Theory and Practice in Social Research: Written by William Foddy, 1994 Edition*,. Cambridge University Press.
7. High-Level Expert Group on AI. (2019). Ethics guidelines for trustworthy AI. Retrieved August 5, 2020, from <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>
8. European Commission. (n.d.). What is personal data? *European Commission - European Commission*. Text. Retrieved March 7, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
9. Data Protection Commission (Ireland). (n.d.). What are “personal data” and when are they “processed”? | Data Protection Commission. *What are “personal data” and when are they “processed”? | Data Protection Commission*. Retrieved March 7, 2022, from <https://www.dataprotection.ie/dpc-guidance/what-is-personal-data>
10. Ross, D. (2017). Processing biometric data? Be careful, under the GDPR. *Processing biometric data? Be careful, under the GDPR*. Retrieved from <https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/>
11. Oza, M. (2020, December 1). ‘Behavioral Biometrics’: A Brief Introduction from the Perspective of Data Protection Law. *CITIP blog*. Retrieved March 7, 2022, from <https://www.law.kuleuven.be/citip/blog/behavioral-biometrics-a-brief-introduction-from-the-perspective-of-data-protection-law/>

12. Data Protection Commissioner (Ireland). (nd). Principles of Data Protection | Data Protection Commission. *Principles of Data Protection | Data Protection Commission*. Retrieved April 5, 2022, from <https://www.dataprotection.ie/individuals/data-protection-basics/principles-data-protection>
13. Data Protection Commission (Ireland). (2019). Guidance Note: Legal Bases for Processing Personal Data. Retrieved from <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf>
14. SMOOTH Consortium. (nd). Data protection in an employment context. *GDPRHANDBOOK*. Retrieved March 7, 2022, from <https://www.gdprhandbook.eu/data-protection-employment-context>
15. Article 29 Data Protection Working Party. (2017). Opinion 2/2017 on data processing at work. Retrieved from <https://ec.europa.eu/newsroom/article29/items/610169>
16. European Data Protection Board. (2021). EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research. Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf
17. European Data Protection Supervisor. (2020). A Preliminary Opinion on data protection and scientific research. Retrieved from https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf
18. Data Protection Commissioner (Ireland). (nd). Data Protection Impact Assessments. *Data Protection Impact Assessments | Data Protection Commission*. Retrieved March 8, 2022, from <https://www.dataprotection.ie/organisations/know-your-obligations/data-protection-impact-assessments>
19. European Data Protection Board. (2020). Guidelines 3/2019 on processing of personal data through video devices. Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en
20. European Union Agency For Network and Information Security. (2016). Guidelines for SMEs on the security of personal data processing. Retrieved from <https://op.europa.eu/en/publication-detail/-/publication/0056ef98-d315-11e6-ad7c-01aa75ed71a1>
21. Information Commissioner's Office (UK). (2022, January 24). The UK GDPR. ICO. Retrieved March 9, 2022, from <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/>
22. Information Commissioner's Office (UK). (nd). The Employment Practices Code. Retrieved from https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

23. Information Commissioner's Office (UK). (2022, January 18). When is consent appropriate? ICO. Retrieved March 9, 2022, from <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/>
24. Information Commissioner's Office (UK). (2021, February 15). Special category data. ICO. Retrieved March 9, 2022, from <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>
25. Information Commissioner's Office (UK). (2022, February 1). Exemptions. ICO. Retrieved March 9, 2022, from <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/>
26. Thomas Reuters Practical Law. (nd). Protected disclosure. *Practical Law*. Retrieved March 10, 2022, from [http://uk.practicallaw.thomsonreuters.com/8-200-3427?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](http://uk.practicallaw.thomsonreuters.com/8-200-3427?transitionType=Default&contextData=(sc.Default)&firstPage=true)
27. La Agencia Española de Protección de Datos. (2021). La protección de datos en las relaciones laborales. Retrieved from <https://www.aepd.es/es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf>
28. Andriopoulos, S., Dede, A., & Lantzou, D. (2021). Employment 2021. Retrieved April 11, 2022, from <https://practiceguides.chambers.com/practice-guides/comparison/688/7406/11855-11858-11864-11867-11869-11872-11876-11882-11885>
29. Iason Skouzos Tax Law. (2021, July 21). Law 4808/2021 (labor arrangements). *ιάρων Σκουζός - TaxLaw*. Retrieved from <https://www.taxlaw.gr/en/practice-areas/law-4808-2021-labor-arrangements/>
30. Government of Greece. (2022). Law 4443/2016. *Gov.gr*. Retrieved April 8, 2022, from <https://www.gov.gr/en/sdg/work-and-retirement/equal-treatment/general/law-4443-2016>
31. Government of Greece. (2021). What are the responsibilities of the safety technician? *Gov.gr*. Retrieved April 8, 2022, from <https://www.gov.gr/en/sdg/work-and-retirement/health-and-safety-at-work/health-and-safety-at-work-frequently-asked-questions/what-are-responsibilities-of-safety-technician>
32. Government of Greece. (2021). What qualifications are required of the safety technician? *Gov.gr*. Retrieved April 8, 2022, from <https://www.gov.gr/en/sdg/work-and-retirement/health-and-safety-at-work/health-and-safety-at-work-frequently-asked-questions/what-qualifications-are-required-of-safety-technician>
33. Government of Greece. (2021). Which undertakings must have an occupational physician? *Gov.gr*. Retrieved April 8, 2022, from <https://www.gov.gr/en/sdg/work-and-retirement/health-and-safety-at-work/health-and-safety-at-work-frequently-asked-questions/which-undertakings-must-have-occupational-physician>

34. Government of Greece. (2021). What qualifications are required of an occupational physician? *Gov.gr*. Retrieved April 8, 2022, from <https://www.gov.gr/en/sdg/work-and-retirement/health-and-safety-at-work/health-and-safety-at-work-frequently-asked-questions/what-qualifications-are-required-of-occupational-physician>
35. Government of Greece. (2021). What are the responsibilities of the occupational physician? *Gov.gr*. Retrieved April 8, 2022, from <https://www.gov.gr/en/sdg/work-and-retirement/health-and-safety-at-work/health-and-safety-at-work-frequently-asked-questions/what-are-responsibilities-of-occupational-physician>
36. Government of Greece. (2021). Which undertakings are required to prepare a written occupational risk assessment? *Gov.gr*. Retrieved April 8, 2022, from <https://www.gov.gr/en/sdg/work-and-retirement/health-and-safety-at-work/health-and-safety-at-work-frequently-asked-questions/which-undertakings-are-required-to-prepare-written-occupational-risk-assessment>
37. Government of Greece. (2021). Must accidents at work be reported? *Gov.gr*. Retrieved April 8, 2022, from <https://www.gov.gr/en/sdg/work-and-retirement/health-and-safety-at-work/health-and-safety-at-work-frequently-asked-questions/must-accidents-at-work-be-reported>

10 Appendix A: OPTIMAI Pilot National Legal Framework

Table 56 OPTIMAI Pilot National Legal Framework

Legal Framework			
Area of Law	Country		
	United Kingdom	Greece	Spain
Data Protection Law	Data Protection Act 2018 UK GDPR	Law 4624/2019	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
Employment Law	Employment Rights Act 1996	Law 4808/2021	Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores
Equality Law	Equality Act 2010	Law 4443/2016	Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social

Health and Safety Law	<p>The Health and Safety at Work etc. Act 1974</p> <p>The Management of Health and Safety at Work Regulations 1999</p> <p>The Health and Safety (Consultation with Employees) Regulations 1996</p> <p>The Factories Act 1961</p> <p>The Control of Substances Hazardous to Health Regulations 1988</p> <p>The Personal Protective Equipment at Work Regulations 1992</p> <p>The Provision and Use of Work Equipment Regulations 1992</p> <p>The Regulatory Reform (Fire Safety) Order 2005</p> <p>The Health and Safety (First-Aid) Regulations 1981</p> <p>The Safety Representatives and Safety Committees Regulations 1977</p>	<p>Presidential Decrees:</p> <p>94/87</p> <p>70A/88</p> <p>399/94</p> <p>186/95</p> <p>17/1996</p> <p>Law 3850/2010</p>	<p>Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales</p>
------------------------------	---	---	---

11 Appendix B: OPTIMAI Human Research Participant Information Sheet and Consent Form



PART I:

Information sheet: Voluntary Participation in the OPTIMAI piloting activity

[Name of the piloting site]

Information about the OPTIMAI project

The OPTIMAI project, coordinated by CERTH, aims to optimize the industrial production with the use of digital technologies to reduce defects, maximize productivity and decrease scrap.

The OPTIMAI solution is equipped with several key enabling digital technologies (e.g., smart sensors, machine learning, digital twins, augmented reality and artificial intelligence (AI)) that can optimize all aspects of manufacturing processes namely production yield, speed and cost. OPTIMAI will increase yield rate by minimizing defects in production through the use of real-time AI analysis of sensory data for early defect detection and prediction. Product quality will be improved and productivity rate will be increased, since fewer defects and downtimes will occur. The production process will be further optimized through virtualization and simulation modules for the production planning. Operators can simulate different configuration setup scenarios in digital twin of the production line in order to find the optimised setup before transferring it to the real production line. In this way, time needed for the preproduction is eliminated as well as scrap and resources that are used during testing. In addition, OPTIMAI will provide tools for the dynamic (re)-configuration and adjustment of production equipment, by directly exploiting quality control feedback to adjust machine parameters and realizing a context aware AR environment where human operators can rapidly reach informed production decisions regarding the calibration of machines in order to improve productivity and avoid deficiencies. To test its vision, OPTIMAI's concept put emphasis of the industrial application of its solution and thus foresees extensive pilot demonstrations in a wide set of industry domains in order to examine and facilitate its adoption in different domains and have the widest possible impact. The goal of OPTIMAI is not to replace human operators but to enhance their capabilities and support their upskilling.

Information about [please, choose: TVES antenna manufacturing plant/ MTCL microelectronic assembly/ KLEE elevator manufacturing]

[A detailed and clear description of the use cases and the corresponding piloting activities must be inserted by each pilot site].

Training and further information

The participation in the piloting activity requires prior training on the OPTIMAI solutions and the potential risks that their use may raise in the context of the piloting activities. Clear instructions on health and safety measures to be observed by all participants are also required to be provided before the start of the piloting activities.

Voluntary participation and right to withdraw

Your participation in the piloting activity is completely voluntary. You are free to withdraw from the piloting activity at any time and without any consequences.

Incentives

Your participation in the piloting activity is completely voluntary and will not be rewarded. Monetary compensations or any other type of rewards are prohibited.

Contact persons

If you have any question or wish to contact us for further clarifications or suggestions, please contact:

[Contact details of the responsible at TVES/MTCL/KLEE]

If you have a general query or you require further information about the OPTIMAI Project, you can also contact:

Christina Tsita, Research Associate, +30 2311 257724, tsita@iti.gr

Nikolaos Dimitriou, Postdoctoral Research Associate, + 30 2311 257797, nikdim@iti.gr

Centre for Research and Technology Hellas (CERTH), Information Technologies Institute (ITI), Thessaloniki, Greece, 6km Charilaou-Thermis, 57001

PART II:

Informed Consent Form to participate in OPTIMAI piloting activities

[Name of the piloting site]

Thank you for considering taking part in the OPTIMAI piloting activities. The responsible for the piloting activities in [TVES/MTCL/KLEE] must explain the project to you before you agree to take part. If you have any questions arising from the Information Sheet or this Consent Form, please request clarifications before you decide whether to participate.

Complete this consent form if you are willing to participate in the OPTIMAI piloting activities by ticking the boxes and then signing at the bottom. By ticking “yes”, you are consenting to the corresponding element of the piloting activities. By ticking “no”, you do not consent to that part of the piloting activities. If you tick “no” for any of the following elements, you may not be able to participate in the piloting activities.

I have read and understood the OPTIMAI information sheet regarding the piloting activities in [TVES/MTCL/KLEE]. I have had the opportunity to consider the information and to ask questions that have been answered to my satisfaction.	Yes	No
I had enough time to decide on my participation in the piloting activity.	Yes	No
I understand that my participation is voluntary. I am free to refuse to participate or to withdraw at any time without any consequences	Yes	No
I have been informed of the contact person, in the case I have questions and queries about the OPTIMAI project or the piloting activities.	Yes	No
I was given a copy of the Information Sheet and the signed Consent Form.	Yes	No
I have received training on how to use OPTIMAI solutions.	Yes	No
I have received instructions on health and safety, and I commit to observe them at all times.	Yes	No
I freely and voluntarily agree to participate in the piloting activities under the conditions set out in the Information Sheet.	Yes	No

By signing below, you accept to participate in the piloting activities conducted in [TVES/MTCL/KLEE] according to the requirements explained above.

Name and surname of the participant:

Place, date:

Signature of the
participant:

[TVES/MTCL/KLEE] pilot site responsible's statement:

I have explained the nature, purpose and procedures to be undertaken as part of [TVES/MTCL/KLEE] piloting activities. I have provided explanations regarding potential risks and the measures in place to address them. [TVES/MTCL/KLEE] has provided clear instructions on how to use the OPTIMAI solutions and how to conduct the piloting activities to ensure health and safety. I have provided full answers to all the questions received from the participant concerning the piloting activities and the OPTIMAI project. I confirm that the individual has not been coerced into giving consent. The participant understands my explanations and has freely given informed consent.

Name and surname of [TVES/MTCL/KLEE] pilot site
responsible:

Place,

Date:

Signature of [TVES/MTCL/KLEE] pilot site
responsible

12 Appendix C: OPTIMAI Pilot Research Ethics Application for CERTH

Ref. No: XXXXX

Submitted to: Ethical Committee
_____ of CERTH

Date Submitted: XX/05/2022

Review Completed:

Researcher(s) Notified:

Application for Ethical Approval from CERTH Research Ethics Panel

Name of researcher: *Dr. Dimitrios Tzovaras*

Email: *Dimitrios.Tzovaras@iti.gr*

Project Title: “OPTIMAI: Optimizing Manufacturing Processes through Artificial Intelligence and Virtualization” (Horizon 2020 – GA: 958264)

Project Description:

The OPTIMAI project³⁸, coordinated by CERTH, aims to optimize the industrial production in today’s competitive global environment, where businesses need to be agile, flexible, resilient, and possess dynamic capabilities. In this context, the advent of advanced digital technologies makes it possible for firms to completely innovate the concept of quality control in order to eliminate defects, maximize productivity and decrease scrap.

The OPTIMAI solution is equipped with several key enabling digital technologies (e.g., smart sensors, machine learning, digital twins, augmented reality and artificial intelligence (AI)) that can optimize all aspects of manufacturing processes namely production yield, speed and cost. OPTIMAI will increase yield rate by minimizing defects in production through the use of real-time AI analysis of sensory data for early defect detection and prediction. Product quality will be improved and productivity rate will

³⁸ <https://optimai.eu/>

be increased, since fewer defects and downtimes will occur. The production process will be further optimized through virtualization and simulation modules for the production planning. Operators can simulate different configuration setup scenarios in digital twin of the production line in order to find the optimised setup before transferring it to the real production line. In this way, time needed for the preproduction is eliminated as well as scrap and resources that are used during testing. In addition, OPTIMAI will provide tools for the dynamic (re)-configuration and adjustment of production equipment, by directly exploiting quality control feedback to adjust machine parameters and realizing a context aware AR environment where human operators can rapidly reach informed production decisions regarding the calibration of machines in order to improve productivity and avoid deficiencies. To test its vision, OPTIMAI's concept put emphasis of the industrial application of its solution and thus foresees extensive pilot demonstrations in a wide set of industry domains in order to examine and facilitate its adoption in different domains and have the widest possible impact.

In practice, at the shop floor of involved factories, a multi-sensorial network will be installed to monitor typical production parameters that affect the efficiency of the production line (e.g. power, temperature, vibration etc.), as well as quality control to detect defective products via metrology sensors (e.g. laser, industrial cameras, ultrasonic probes etc.). In each of the three pilot sites (Greece, Spain and United Kingdom) a combination of these solutions will be deployed according to their particularities. Three use cases are foreseen in the project for the pilots: i) *Zero defect quality inspection*, which focuses on the detecting defects on the products, analysing their causes and predicting emerging deficiencies; ii) *Production line setup-calibration*, which develops and automated quality control loop between inspection and machine setup and builds a context aware interaction environment for operator and production equipment; iii) *Production planning*, which targets to the virtualization of the production line that will enable cost and time efficient production planning.

Context of this request:

The purpose of this request is to obtain the ethical approval from CERTH Research Ethics Panel to conduct the OPTIMAI piloting activities for each use case in the different OPTIMAI piloting sites in Greece, Spain and United Kingdom. To that end, CERTH, as Coordinator of the OPTIMAI Project with the assistance of OPTIMAI legal and ethical partners (Autonomous University of Barcelona and Trilateral Research Ltd), provide the following information to enable the ethical assessment of the piloting activities by CERTH Research Ethics Panel.

Description of the use cases in each OPTIMAI pilot site:³⁹

Pilot activities in Spain are conducted by Televés SA (TVES). The scenario proposed for the OPTIMAI project is the TVES antenna manufacturing plant. Three use cases are defined: The first two use cases are defined with the objective of identifying, detecting and optimizing stoppages and/or incidents that affect production efficiency during antenna manufacturing. UC1 focuses on incidents that affect the Overall Equipment Effectiveness (OEE) through its quality parameter while UC2 analyses the production efficiency losses due to availability and performance decreases. In UC3 it is proposed to obtain a digital twin of the antenna manufacturing plant that will allow simulating production scenarios and drawing important conclusions. UC3 will consider factors that currently do not affect the OEE indicator but do reduce the real production capacity (need for periodic preventive maintenance, scheduled interventions for process improvements or modifications, operator training, etc.).

³⁹ These descriptions have been extracted from 'D2.6 OPTIMAI use cases definition'.

UC1 - Zero defect quality inspection: The objectives of this use case are: i) the real-time detection of defects; ii) prediction and prevention of upcoming defects by monitoring of production conditions.

Antenna manufacturing line is an error-prone manufacturing process and the sources of defects are attributed to a combination of material defects, parts integration and machine failures. Installation of quality inspection sensors and the use of AI models, OPTIMAI will target the most common types of defects:

- **Material defects:** As mentioned in the Description of Actions (DoA), in the robotized antenna assembly line, materials used are coming from other sections (Plastics, Zamak, Antenna Workshop, FMS lines etc.) as well as materials that are processed in the Antenna Plant itself. Those coming from other sections meet the required quality guarantees, however, there are materials that are processed in the Antenna Plant that might not be detected as defective before entering the line. A detection at source of these defective materials in real time would improve production efficiency.
- **Final product quality failures:** As mentioned in the DoA, along the line there are vision systems in charge of guaranteeing the quality of the product. The most common failure is an incorrect assembly of the elements that make up the antennas. By monitoring the assembly operation processes, OPTIMAI will predict when a process is possible to start failing and generating defective products in order to prevent it.

UC2 - Production line setup-calibration: As mentioned in the DoA, the objectives of this use case are; i) automating the reconfiguration of machines based on a contextual AI analysis of multiple sensors; ii) accelerating operator machine interaction using augmented reality and computer vision.

This use case concentrates on setting up and calibrating the equipment related to the quality control defined for UC1. Based on quality inspection results, the aim is to automatically re-calibrate machine parameters so that either defects are not propagated (so that no more defective parts are produced) or not manifested at all through the early identification and correction of suboptimal manufacturing. Moreover, line setups time will be improved as a result on this optimised calibration process. Related with the quality control scenarios and as stated in DoA, will be examined:

- **Manufacturing reference changes:** Production efficiency is affected by needed stoppages different products assembled on the line.
- **Stoppages in inspection/vision systems:** Stoppages caused by quality control system affect throughput or availability regardless of whether the systems are accurate or false positives.
- **Incidents in material feeding peripherals.**
- **Incidents in pallet conveyor systems.**
- **Software / hardware incidents in robotic cells.**

These events will be recorded during manufacturing and will provide OPTIMAI with valuable data on which to develop AI systems that will extract information that will be used to optimally reconfigure machines / robotic cells in the antenna manufacturing plant.

UC3 - Production planning: As stated in the DoA, this UC objectives are to; i) virtualize production developing a complete simulation environment to select optimal condition for different types of products and ii) connect the virtual with the physical counterparts enabling the rapid setup of production according to the virtual replicas.

Here the target is to replicate using virtual twins of each production step in order to simulate production scenarios. The virtualization will include not only the specific robotic cells but also virtual sensors providing a complete virtual production environment. It will be key to identify optimal parameters for

each product type while the necessary actuation interface will be implemented to rapidly setup the respective robots.

As the priority of TVES is to maintain a high quality in their products, these systems have false failures as a counterpart to not sneak real failures. Eliminating false failures in any of these systems would also substantially improve the production efficiency of the line.

By using OPTIMAI simulated scenarios, operators will be able to adjust and experiment with different setups in advance, before they can have any effect on actual production.

Pilot activities in UK are conducted by Microchip Technology Inc. (MTCL). The scenario proposed for the OPTIMAI project is the MTCL microelectronic assembly.

UC1 - Zero defect quality inspection: The objectives of this use case are; i) real time detection of defects; ii) identification of defect cause even upstream; iii) real time prediction of upcoming defects and prevention of deficiencies.

Currently quality verification is performed through manual inspection either right after each manufacturing step or at a suitable downstream process stage. This normally consists of a sample inspection carried out with the use of a microscope and heavily reliant on the inspector's knowledge. OPTIMAI will aim to improve this process by delivering automated quality control methodologies for wafer sawing, PCB routing and glue/epoxy dispensing.

UC2 - Production line setup-calibration: The objectives of this use case are: i) quick response to defect detection with automatic and semi-automatic re-calibrations, ii) take into account operators' experience and their ability to react and facilitating them with AR interfaces.

By taking data from the previous use case UC1, this use case focusses on setting up and calibrating the equipment. Currently this is mostly manual process and relies on operator's experience. OPTIMAI's ambition is to either semi-automatically or automatically re-calibrate machine parameters based on quality inspection results, removing the opportunity for defects to be produced focussing on the following areas for each process.

- Controlling the resistivity of De Ionised water supply during wafer sawing
- Dynamically adjusting airline inlet pressure in PCB routing
- Dynamically adjusting nozzle pressure in Glue and Epoxy dispense

This will be carried out with the aid of near real time data and augmented reality.

UC3 - Production planning: The objectives of this use case are: i) allow operators to interact with the virtual twin of the production line, to ii) apply different setups to find optimal solutions before realizing impact on the actual production line, iii) apply directly the optimal setup to the actual production line.

In the most ambitious section of the project each of the production steps will be recreated in the virtual world. The aim will be not only to re-create the machines but the whole working environment and generate an interactive platform to communicate effectively in the virtual space. Finally, the ability to connect the virtual and real-world machines will enable rapid set-ups of machines remotely.

Pilot activities in Greece are conducted by Kleemann Hellas. (KLEE). The scenario proposed for the OPTIMAI project is the KLEE elevator manufacturing.

UC1 - Zero defect quality inspection: This use case aims at: i) automating the quality inspection process, while decreasing costs related to quality control and productivity and ii) identifying defects that are not spotted in the manual inspection in order to improve final product quality.

This use case will be developed in the lift's hydraulic power unit. The power unit is one of the most critical components for the smooth and normal lift operation and KLEE has designed a test lab for the unit's quality testing. This lab is a separate soundproof room, where the operating conditions of each hydraulic lift order are simulated based on the building characteristics. In 2020, nearly 5% of the tested hydraulic lift systems have presented problems related to cracked pumps, oil flow rate and several re-adjustments in the hydraulic power unit. Currently, the quality control is not automated and it requires manual inspections and expert's knowledge and experience, while deficiencies in the calibration of the valve block are hard to spot and require considerable testing time while negatively affecting the operation of the lift in terms of speed, vibrations and sound.

UC2 - Production line setup-calibration: The objectives of this use case are to: i) automate the calibration procedure in order to reduce calibration time and ii) improve the final product quality by providing optimal setup of the hydraulic power unit.

This use case aims at providing optimal setup of the hydraulic power unit valve block. To meet this goal, OPTIMAI will develop a solution that will assist the i) direct adjustments of the valve block based on quality control measurements from noise, vibrations and speed; ii) human operator to rapidly adjust the hydraulic unit's parameters, including the valve block, using OPTIMAI's AR and HCI environment.

UC3 - Production planning: This use case will: i) reduce the defective parts via improved unit design and ii) connect the virtual with the physical quality control, to facilitate the implementation of corrective actions according to the virtual counterparts.

In this use-case, OPTIMAI's virtualization technology will be used to create digital twins of hydraulic power units that will be combined with AI models that map design choices to the units performance and any related defects. These models will be trained based on the data that will be collected from the test lab and they will focus on repeated errors and defects. With this use-case, mechanical engineers will be able to explore the impact of different design choices and to compare the behaviour of the actual unit with its virtual twin, during the lab testing in order to rapidly notice any discrepancies.

Legal and ethical monitoring activities regarding the piloting activities:

As part of Task 9.4 'Ethical and Legal monitoring', WP9 Partners have conducted several legal and ethical monitoring activities to ensure that all OPTIMAI piloting activities are legally and ethically compliant. Jointly with the OPTIMAI Ethics Board, WP9 Partners have provided legal requirements and ethical recommendations for the pilots to ensure compliance with EU and national legal frameworks, and mitigation measures to address ethical issues that may arise from the use of cutting-edge technologies in the shop floor, and to guarantee the well-being of the piloting site workers.

In this regard, a set of general requirements were provided in D2.1 'User and ethics and legal requirements - 1st version' and D9.1 'Report on the OPTIMAI ethical and legal framework' and specific ethical and legal requirements for the piloting activities were included in D9.2 'Report on OPTIMAI ethical, legal and societal risks - 1st version'. In D7.3 'Ethics recommendations and regulatory framework', ethical procedures were described and legal requirements from the national legal frameworks of each pilot site regarding data protection, employment, equality and health and safety were provided. Additionally, D9.2 contained the integrated impact assessment of OPTIMAI research activities, with special emphasis on identifying and addressing potential risks arising in the

piloting activities. Lastly, to ensure the voluntary participation of piloting site workers, an information sheet and a consent form have been designed and can be found attached. In order to perform all these activities, WP9 Partners have held several specific meetings with TVES, MTCL and KLEE.

In light of the above, we request CERTH's Ethics Committee to review and approve the piloting activities to be conducted by TVES, MTCL and KLEE.

Signed:

Researcher

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Ethical Committee Members

Athanasios Konstandopoulos

Anagnostis Argiriou

Georgia Aifantopoulou

Ioannis Kompatsiaris

Olga Kammona