



Architecture for Scalable, Self-human-centric, Intelligent, Secure, and Tactile next generation IoT



D3.4 Legal and Regulatory Constraints Analysis and Specification

Deliverable No.	D3.4	Due Date	31-Oct-2021
Type	Report	Dissemination Level	Public
Version	1.0	WP	WP3
Description	This deliverable includes details of legal and regulatory constraints in different countries that have to be considered when designing ASSIST-IoT solutions.		



Copyright

Copyright © 2020 the ASSIST-IoT Consortium. All rights reserved.

The ASSIST-IoT consortium consists of the following 15 partners:

UNIVERSITAT POLITÈCNICA DE VALÈNCIA	Spain
PRODEVELOP S.L.	Spain
SYSTEMS RESEARCH INSTITUTE POLISH ACADEMY OF SCIENCES IBS PAN	Poland
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	Greece
TERMINAL LINK SAS	France
INFOLYSIS P.C.	Greece
CENTRALNY INSTYTUT OCHRONY PRACY-PAŃSTWOWY INSTYTUT BADAWCZY	Poland
MOSTOSTAL WARSZAWA S.A.	Poland
NEWAYS TECHNOLOGIES BV	Netherlands
INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	Greece
KONECRANES FINLAND OY	Finland
FORD-WERKE GMBH	Germany
GRUPO S 21SEC GESTION SA	Spain
TWOTRONIC GMBH	Germany
ORANGE POLSKA SPOLKA AKCYJNA	Poland

Disclaimer

This document contains material, which is the copyright of certain ASSIST-IoT consortium parties, and may not be reproduced or copied without permission. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

The information contained in this document is the proprietary confidential information of the ASSIST-IoT Consortium (including the Commission Services) and may not be disclosed except in accordance with the Consortium Agreement. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the Project Consortium as a whole nor a certain party of the Consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and accepts no liability for loss or damage suffered by any person using this information.

The information in this document is subject to change without notice.

The content of this report reflects only the authors' view. The Directorate-General for Communications Networks, Content and Technology, Resources and Support, Administration and Finance (DG-CONNECT) is not responsible for any use that may be made of the information it contains.

Authors

Name	Partner	e-mail
Carlos Guardiola	P01 UPV	carguaga@upv.es
Konstantinos Votis	P04 CERTH	kvotis@iti.gr
Francisco Blanquer	P05 TL	ho.fblanquer@terminal-link.com
Anna Dąbrowska	P07 CIOP-PIB	andab@ciop.lodz.pl
Krzysztof Baszczyński	P07 CIOP-PIB	krbas@ciop.lodz.pl
Joanna Szkudlarek	P07 CIOP-PIB	joszka@ciop.lodz.pl
Grzegorz Owczarek	P07 CIOP-PIB	growc@ciop.lodz.pl
Marcin Jachowicz	P07 CIOP-PIB	majac@ciop.lodz.pl
Piotr Dymarski	P08 MOW	p.dymarski@mostostal.waw.pl
Ron Schram	P09 NEWAYS	ron.schram@newayselectronics.com
Fotios Konstantinidis	P10 ICCS	fotios.konstantinidis@iccs.gr
Sami Piittisjärvi	P11 Konecranes	sami.piittisjarvi@konecranes.com
Klaus Schusteritz	P12 FORD-WERKE	kschust4@ford.com
Oscar López	P13 S21SEC	olopez@s21sec.com
Lambis Tassakos	P14 TwoTronic	Lambis.Tassakos@gmail.com
Zbigniew Kopertowski	P15 OPL	Zbigniew.Kopertowski@orange.com

History

Date	Version	Change
13-Jul-2021	0.1	ToC and task assignments
11-Oct-2021	0.5	Integrated version of the document
15-Oct-2021	0.8	Version for internal review
28-Oct-2021	0.9	Draft ready for submission
	1.0	Official release

Key Data

Keywords	Legal regulations, law, requirements, standards, human rights, ethics, personal data protection, cybersecurity, artificial intelligence
Lead Editor	P07 CIOP-PIB – Anna Dąbrowska
Internal Reviewer(s)	Alex van den Heuvel, P09 NEWAYS Theoni Dounia, P06 INFOLYSIS

Executive Summary

The deliverable outlines the results of Task 3.4 activities that are focused on the analysis of legal regulations and specification of regulatory constraints in the ASSIST-IoT pursuits. The identified legal regulations have been divided into two categories: one related to the whole project, and the second one oriented to specific pilots. The general regulations mainly concerned legal aspects related to human rights and freedoms, personal data protection, privacy, cybersecurity, data governance, 5G, electronic devices, and the use of artificial intelligence. On the other hand, the pilot-oriented regulations additionally include documents related to machinery, occupational safety and health, product safety and emissions. The report summarises the implications of the abovementioned regulations on both the ASSIST-IoT Data Management plane, as well as pilot domains. This means that it includes considerations that should be taken into account at various stages of project execution in order to be in line with the law. Particular attention is also given in the report to legal challenges resulting from the implementation of the artificial intelligence in relation to ensuring personal data protection and privacy. Finally, in order to overcome those challenges, contact with regulatory bodies and authorities has been initiated that hopefully will result in legal guidance at both the European and national level.

Table of contents

Table of contents	5
List of tables	6
List of figures	6
List of acronyms	7
1 About this document	9
1.1 Deliverable context	9
1.2 The rationale behind the structure	9
2 Introduction	10
3 Review of legal regulations	10
3.1 General legal regulations related to ASSIST-IoT pursuits	11
3.1.1 European regulations	11
3.1.2 National regulations	13
3.2 Legal regulations related to pilot domains	14
3.2.1 Port automation (Pilot 1)	14
3.2.2 Smart Safety of Workers (Pilot 2)	15
3.2.3 Cohesive vehicle monitoring and diagnostics (Pilot 3)	17
3.3 Selected standards relevant to ASSIST-IoT pursuits	18
3.3.1 Standards related to electronic devices and machinery	18
3.3.2 Standards related to cybersecurity and data protection	19
3.3.3 Standards related to 5G technology	20
3.3.4 Standards related to OSH	21
4 Legal aspects related to the Data Management plane	23
4.1 Safety	23
4.2 Data protection and privacy	23
4.3 Cybersecurity	24
5 Implications of legal aspects on pilots	24
5.1 Implications on Port Automation pilot	24
5.1.1 Personal data protection, privacy, and cybersecurity	24
5.1.2 Workers safety	25
5.1.3 Environmental sustainability	25
5.2 Implications on Smart Safety of Workers pilot	25
5.2.1 Personal data protection and privacy	25
5.2.2 General provisions for safety and health at work on the construction site	26
5.2.3 PPE essential health and safety requirements	29
5.2.4 Ethics	32
5.3 Implications on Cohesive Vehicle Monitoring and Diagnostics pilot	33
5.3.1 Personal data protection	33

5.3.2 Emissions	36
5.3.3 Safety	37
6 Legal guidance from the European and national regulatory bodies and authorities	38
6.1 Published proposals for EU regulations	38
6.2 Identified regulatory bodies and authorities	39
7 Conclusions	42
References	43
A Official letters	44

List of tables

Table 1 Standards related to electronic devices and machinery	18
Table 2 Standards related to cybersecurity and data protection	19
Table 3 Standards related to 5G technology	20
Table 4 Standards related to occupational safety and health	21
Table 5 Example of information on a subcontractor's employee	26
Table 6 A list of regulatory bodies and authorities contacted for legal guidance in pilot domains	39
Table 7 A list of regulatory bodies and authorities contacted for legal guidance in personal data protection, cybersecurity and artificial intelligence	40
Table 8 A list of national regulatory bodies and authorities	41

List of figures

Figure 1 A view of the electrical power installation	27
Figure 2 Visualisation of dangerous zones	29
Figure 3 Protective helmet	30
Figure 4 High visibility vest	30
Figure 5 Protective footwear	31
Figure 6 Anonymised driver face to conform with personal data protection rules	35
Figure 7 Anonymised license plate to conform with personal data protection rules	36
Figure 8 Evolution of the legislated emission limit for EU diesel light vehicles (left); NEDC and WLTC certification cycles (centre) and vehicle with PEMS system (right)	36

List of acronyms

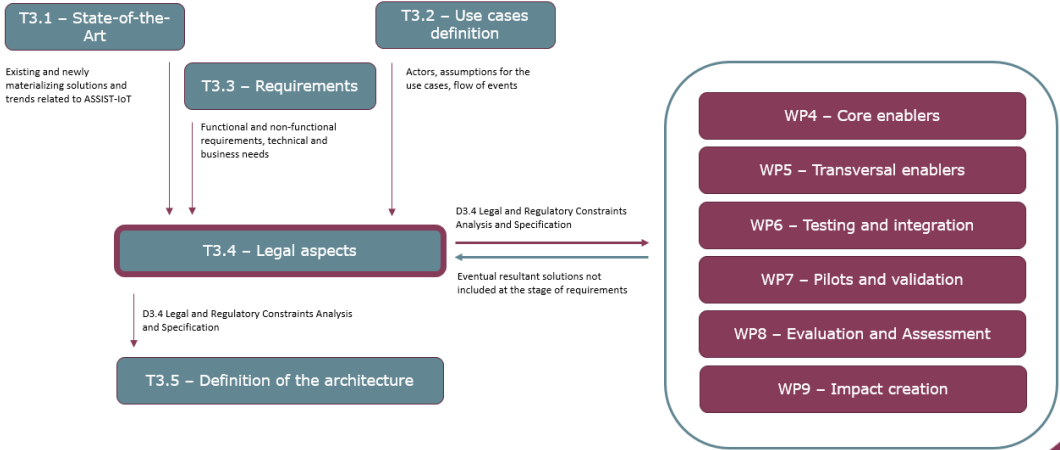
Acronym	Explanation
ABS	Anti-lock Braking System
AI	Artificial Intelligence
AR	Augmented Reality
DLT	Distributed Ledger Technology
EDPB	European Data Protection Board
EEA	European Economic Area
EMC	Electromagnetic Compatibility
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
GPSD	General Product Safety Directive
GSM	Global System for Mobile Communications
HDPa	Hellenic Data Protection Authority
ICNIRP	International Commission on Non-Ionizing Radiation Protection
ICT	Information and Telecommunication Technology
IoT	Internet of Things
ISC	In-Service Conformity
LTE	Long Term Evolution
LVD	Low Voltage Directive
MEC	Multi-access Edge Computing
ML	Machine Learning
MTC	Machine-Type of Communications
NEDC	New European Driving Cycle
NGIoT	Next Generation Internet of Things
OBD	On-Board Diagnostics
OEM	Original Equipment Manufacturer
OSH	Occupational Safety and Health
PCM	Powertrain Control Module
PEMS	Portable Emission Measurement System
PPE	Personal Protective Equipment
RDE	Real Driving Emissions
REC	Research Ethics Committee

RFID	Radio-frequency identification
SAWAPS	Small-area Wireless Access Points
TFEU	Treaty on the Functioning of the European Union
UMTS	Universal Mobile Telecommunications System
VIN	Vehicle Identification Number
WLTC	Worldwide harmonised Light-duty vehicles Test Cycle
WLTP	Worldwide harmonised Light-duty vehicles Test Procedures

1 About this document

The aim of this deliverable is to ensure that ASSIST-IoT pursuits are compliant with all current legal regulations, especially in the pilot domains. It contains details of legal and regulatory constraints in different countries that have to be considered when designing ASSIST-IoT solutions. Considering the huge scope of the ASSIST-IoT pursuits and numerous relevant legal aspects, this deliverable should be treated as an indication of the legal aspects that should be considered during development, integration, as well as demonstration and validation of project results. However, in order to get familiar with detailed legal requirements, further exploration of particular documents may be needed.

1.1 Deliverable context

Keywords	Lead Editor
Objectives	<p>O1: D3.4 discusses legal aspects for the Data Management Plane</p> <p>O2-O5: D3.4 provides a summary of legal requirements for all the ASSIST-IoT pursuits with a special focus on the pilot domains and the use of AI in relation to security, privacy and personal data protection</p>
Work plan	
Milestones	This deliverable is not directly linked with any specific milestone but as it deals with legal aspects related to all the ASSIST-IoT pursuits, it indirectly contributes to MS7.
Deliverables	This deliverable takes into account D3.1 State-of-the-Art and Market Analysis and D3.2 Use Cases Manual & Requirements and Business Analysis - Initial in terms of defining the scope of legal aspects to be considered within the D3.4, as well as D2.2 Data Management Plan and D2.3 Ethics and Privacy Manual in terms of following already adopted in the ASSIST-IoT procedures.

1.2 The rationale behind the structure

As the aim of this deliverable is to ensure that ASSIST-IoT pursuits are compliant with all current legal regulations (see section 1.1), therefore, the structure of this document includes both the results of the review of existing legal regulations, as well as their analysis in terms of the Data Management plane and three pilot domains. In particular, it includes the following sections:

- **Section 3** contains a review of European and national legal regulations,
- **Section 4** indicates legal aspects that should be considered in the Data Management plane,
- **Section 5** summarises legal implications on pilot domains,

- **Section 6** contains the identification of EU regulatory institutions at the proposal stage as well as a summary of activities done in order to establish connections with European and national regulatory bodies and authorities,
- **Section 7** refers to conclusions that summarise the implications of the deliverable on research activities to be performed within the ASSIST-IoT.

2 Introduction

The main objective of Task 3.4 is to ensure that ASSIST-IoT pursuits are compliant with all current legal regulations. According to Article 288 of the Treaty on the Functioning of the European Union (TFEU), five types of legal acts can be distinguished at the European level: regulation, directive, decision, recommendations and opinions. Regulations, directives and decisions are binding legal acts, while the recommendation and the opinion are not. A regulation is an act that must be entirely applied across the EU, while a directive is an act that sets up a goal that all EU countries must achieve without dictating the means of achieving it. It is worth highlighting that according to Article 291 of the TFEU “*Member States shall adopt all measures of national law necessary to implement legally binding Union acts.*”. This means that directives are transposed by the EU Member States into their national law. Therefore, for the purpose of analysis and specification of legal and regulatory constraints in relation to the ASSIST-IoT enablers, technical solutions and services, the methodology adopted includes a top-down approach with the following levels of legal aspects consideration:

- EU-wide – that focuses on pilot domains, i.e. port automation (pilot 1), smart safety of workers (pilot 2), as well as cohesive vehicle monitoring and diagnostics (pilot 3), and addresses all areas covered by ASSIST-IoT, such as personal data protection, privacy, security, ethics, machinery, smart devices, 5G, occupational safety and health, artificial intelligence
- national – that relates to identification of any national regulations from seven European countries represented by the ASSIST-IoT consortium that either transpose the EU acts or may be more restrictive than those at the EU level,
- local – that introduces further specific regulations at the companies level, in which the specific pilot will be implemented.

Firstly, the activities within Task 3.4 were related to the identification of relevant regulations and their review (section 3). Then, based on the identified regulations, their implications on pilot domains were summarised (section 4) and legal challenges for the data management plane were described (section 5). Finally, relevant regulatory bodies and authorities dealing with legal aspects related to ASSIST-IoT pursuits were identified and reached (section 6) in order to engage them in legal guidance and to ensure compliance of project results with regulations forthcoming during the project execution. For that purpose, also proposals for regulations were identified and reviewed in order to take into consideration the potentially upcoming changes in the existing regulations.

3 Review of legal regulations

Given the scope of the ASSIST-IoT pursuits, the following areas of legal regulations have been identified for review: human rights, data protection, privacy, cybersecurity, data governance, Internet of Things, electronic devices, 5G, artificial intelligence, as well as others - specific to individual pilots. From a significant number of documents, those that seemed the most relevant to the enablers, solutions and services to be developed, integrated and tested within the project, have been identified, categorised and described. The categorisation adopted includes:

- general legal regulations (at the European and national level) that are relevant for the ASSIST-IoT as a whole,
- legal regulations specific to certain pilots and not relevant to other domains,
- standards including specific requirements for the ASSIST-IoT pursuits (both general and pilot-related).

The aim of this section is to indicate potential sources of more detailed information about legal requirements concerning technical development, as well as integration and even validation within the ASSIST-IoT project.

3.1 General legal regulations related to ASSIST-IoT pursuits

3.1.1 European regulations

Human rights and fundamental freedoms - Charter of Fundamental Rights of the European Union

The Charter contains rights and freedoms under six titles: I - dignity, II – freedoms, III – equality, IV – solidarity, V – citizens' rights, VI – justice, VII – general provisions. The Charter of Fundamental Rights brings together all the personal, civic, political, economic and social rights enjoyed by people within the EU in a single text. It covers all the rights found in the case law of the Court of Justice of the EU, the rights and freedoms enshrined in the European Convention on Human Rights, other rights and principles resulting from the common constitutional traditions of EU countries and other international instruments. The Charter includes 'third generation' fundamental rights, such as: data protection, guarantees on bioethics and transparent administration.

Data protection - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business. It contains provisions and requirements related to the processing of personal data of individuals (formally called data subjects in the GDPR) who are located in the EEA, and applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of individuals inside the EEA.

Privacy - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

It deals with the regulation of a number of issues such as confidentiality of information, treatment of traffic data, spam and cookies. In particular, the subject of the Directive is the "right to privacy in the electronic communication sector" and free movement of data, communication equipment and services. The Privacy Directive also applies to legal persons. The first general obligation in the Directive is to provide security of services. The addressees are providers of electronic communications services. This obligation also includes the duty to inform the subscribers whenever there is a particular risk, such as a virus or other malware attack. The second general obligation is for the confidentiality of information to be maintained. The Member States should prohibit listening, tapping, storage or other kinds of interception or surveillance of communication and "related traffic", unless the users have given their consent or conditions of Article 15(1) have been fulfilled.

Cybersecurity - Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

It aims to achieve a high level of cybersecurity, cyber resilience and trust in the European Union (EU) by setting:

- objectives, tasks and organisational matters for a strengthened and renamed European Union Agency for Cybersecurity (ENISA), with a new permanent mandate;
- a framework for voluntary European cybersecurity certification schemes for Information and communications technology (ICT) products, services and processes.

The regulation establishes a European cybersecurity certification framework to:

- improve the functioning of the internal market by increasing the level of cybersecurity in the EU and enabling a harmonised approach at EU level to European cybersecurity certification schemes with a view to creating a digital single market for ICT products, services and processes;
- set up a mechanism to establish certification schemes that confirm ICT products, services and processes that have been evaluated in accordance with such schemes comply with specified security requirements to protect the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or functions or services offered by, or accessible via, those products, services and processes throughout their life cycle.

Data governance - Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. An integral part of the European Union's Digital Single Market initiative, this Regulation aims to remove unjustified barriers to the movement of non-personal data in the EU and thus to assist in unlocking the potential of Europe's Data Economy

The aims of the Regulation are the following:

- to improve the mobility of non-personal data across borders in the single market;
- to ensure that the powers of competent authorities to request and receive access to data for regulatory purposes remain unaffected;
- to make it easier for professional users of data storage or other processing services to switch service providers and to port data, while not creating an excessive burden on service providers or distorting the market.

5G: Commission Implementing Regulation (EU) 2020/1070 of 20 July 2020 on specifying the characteristics of small-area wireless access points pursuant to Article 57 paragraph 2 of Directive (EU) 2018/1972 of the European Parliament and the Council establishing the European Electronic Communications Code

The document specifies requirements for the low power small-area wireless access points (SAWAPS) used for 5G in order to ensure their public acceptance and sustainable deployment.

Artificial Intelligence:

- **European Commission, 2021, Coordinated Plan on Artificial Intelligence 2021 review**

The document outlines the goal of creating EU global leadership on human-centric AI with Member States. This is the next step of published in 2018 Coordinated Plan on Artificial Intelligence and it puts forward a concrete set of joint actions for the European Commission and Member States on how to create EU global leadership on trustworthy AI. The plan formulates the following three needs: 1) to accelerate investments in AI technologies to drive resilient economic and social recovery facilitated by the uptake of new digital solutions; 2) to act on AI strategies and programmes by implementing them fully and in a timely manner to ensure that the EU reaps the full benefits of first-mover adopter advantages; and 3) to align AI policy to remove fragmentation and address global challenges.

- **European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 2020**

The White Paper sets out policy options on how to promote the uptake of AI and address the risks associated with certain uses of this new technology. Within the document the main risks related to the use of AI are identified: 1) the application of rules designed to protect fundamental rights (including personal data and privacy protection and non-discrimination), and 2) safety and liability-related issues. Moreover, it indicates possible adjustments to existing EU legislative framework relating to AI, as well as drafts a scope of a EU regulatory

framework. With this White Paper, the Commission launched a consultation of Member States civil society, industry and academics, of concrete proposals for a European approach to AI.

- **European Commission, Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, 2020**

The Report indicates safety and liability issues related to the use of AI. It highlights that the current legislation contains a number of gaps that need to be addressed, in particular in the General Product Safety Directive, Machinery Directive, the Radio Equipment Directive and the New Legislative Framework. Regarding the liability, it explains how new technologies challenge the existing frameworks and in what way these challenges could be addressed.

Electronic devices

- **Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety**

The General Product Safety Directive (GPSD) specifies EU rules on product safety. Under the directive, a product is safe if it meets all statutory safety requirements under European or national law.

- **Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits**

The Low Voltage Directive (LVD) covers electrical equipment designed for use within certain voltage limits which is new to the Union market when it is placed on the market. It relates to the equipment operating with an input or output voltage of between (a) 50 and 1000 V for alternating current, (b) 75 and 1500 V for direct current.

- **Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility**

The Electromagnetic Compatibility (EMC) Directive ensures that electrical and electronic equipment does not generate, or is not affected by, electromagnetic disturbance. It limits electromagnetic emissions from equipment in order to ensure that, when used as intended, such equipment does not disturb radio and telecommunication, as well as other equipment

- **Directive 2014/53/EU of the European Parliament and of the Council of April 16, 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC**

In order to ensure an efficient use of radio spectrum so as to avoid harmful interference, all such equipment should fall within the scope of this Directive. The essential requirements for the radio equipment are described in Article 3 of the Directive.

3.1.2 National regulations

Spain:

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales / Organic Law 3/2018, of December 5, on Protection of Personal Data and guarantee of digital rights

Poland:

- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000) / The Act of 10 May 2018 on the Protection of Personal Data (Journal of Laws of 2018, item 1000),
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560) / The Act of 5 July 2018 on the National Cybersecurity System (Journal of Laws of 2018, item 1560)

Greece:

Law no. 4624: Hellenic Data Protection Authority (HDP), measures for implementing Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions

Malta:

- The Maltese Data Protection Act, 2018 (chapter 586 of the Laws of Malta)
- Maltese laws dealing with various aspects of cybersecurity include: the Criminal Code, which deals with cybercrime in the chapter entitled 'Of Computer Misuse'; the Processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation 440.01); and the Electronic Communications Networks and Services (General) Regulations

Germany:

The German "Bundesdatenschutzgesetz" (abbreviation: BDSG - the German Federal Data Protection Act) supplements and specifies the General Data Protection Regulation (GDPR) in those areas, that are left to the national regulations of the EU member states. These include, among others, the processing of employee data, video surveillance (relevant for the pilot project 3b), the appointment of data protection officers or supervisory authorities. The Federal Data Protection Act has been introduced on January 1, 1978, and the current version has been in force since May 25, 2018. This law is applied in both public and non-public entities in Germany. The European GDPR is currently also applied in Germany. It must be emphasized here, that the use of artificial intelligence for generalized surveillance or manipulation of the population is completely prohibited, as is so-called social scoring, in which people are evaluated based on their social behavior.

In the case of other countries, there have not been identified any specific national regulations that could have implications on pilot domains.

3.2 Legal regulations related to pilot domains

3.2.1 Port automation (Pilot 1)

The port automation pilot is basically a remote-controlled machine operation with machine to machine interchange of operational data where only the operator id will be used to identify the crane and truck driver for safety and performance analysis reasons.

Given the fact that some personal data, such as the employee id number and accordingly the driver's name that is linked to that number, will be used, the pilot is subject to the EU GDPR regulation. Due to the fact that the port automation pilot will take place in the port of Malta, this pilot is also subject to the Maltese GDPR regulation Chapter 586 of the Laws of Malta.

Other regulations are directly related to the wireless remote control and must follow the general machinery directives:

- EN 13557 + A2 Cranes. Controls and control stations
- EN 60204-32 Safety of machinery - Electrical equipment of machines - part 32: Requirements for hoisting machines.
- EN ISO 13849-1 Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design
- EN 1746 Safety of machinery. Guidance for the drafting of the noise clauses of safety standards
- EN ISO 4871 Acoustics – Declaration and verification of noise emission values of machinery and equipment.
- ISO 12100 Safety of machinery. General principles for safety of machinery. general principles for design, risk assessment and risk reduction.

Finally, additional regulations that should be taken into account in the ASSIST-IoT Port Automation Pilot are those associated with the safety, security and sustainability of container terminals. In particular, the following rules apply:

- Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work.
- European Parliament and Council Directive 2001/96/EC of 16 January 2001 on establishing harmonised requirements and procedures for the safe loading and unloading of bulk carriers.
- European Parliament and Council Directive 2010/65/EU of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States in electronic format and to ensure their transmission via a single window
- European Parliament and Council Directive 2005/65/EC of 26 October 2005 on enhancing port security.
- European Parliament and Council Directive 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
- EN ISO 1400:2015 of 14 September 2015 on Environmental management systems – Requirements with guidance for use

3.2.2 Smart Safety of Workers (Pilot 2)

A wide variety of Community measures in the field of safety and health at work has been adopted based on Article 153 of the Treaty on the Functioning of the European Union. European directives are legally binding and have to be transposed into national law by Member States. European directives set out minimum requirements and fundamental principles, such as the principle of prevention and risk assessment, as well as the responsibilities of employers and employees. A series of European guidelines aims to facilitate the implementation of European directives as well as European standards which are adopted by European standardisation organisations.

As set out by principle 10 of the European Pillar of Social Rights, workers have the right to a high level of protection of their health and safety at work. Occupational health and safety is based on a solid legal framework, the main ones being:

- Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work
- Council Directive 89/656/EEC of 30 November 1989 on the minimum health and safety requirements for the use by workers of personal protective equipment at the workplace (third individual directive within the meaning of Article 16 (1) of Directive 89/391/EEC)
- Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC
- Council Directive 89/654/EEC of 30 November 1989 concerning the minimum safety and health requirements for the workplace (first individual directive within the meaning of Article 16(1) of Directive 89/391/EEC)
- Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)
- Directive 89/654/EEC of 30 November 1989 concerning the minimum safety and health requirements for the workplace (first individual directive within the meaning of Article 16(1) of Directive 89/391/EEC).
- Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)

- Directive 92/58/EEC of 24 June 1992 on the minimum requirements for the provision of safety and/or health signs at work (ninth individual Directive within the meaning of Article 16 (1) of Directive 89/391/EEC).
- Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24).

In addition, there are hazards-related directives; the most important ones related to the scope of the project are:

- Directive 2002/44/EC of the European Parliament and of the Council of 25 June 2002 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (vibration) (sixteenth individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)
- Directive 2013/59/Euratom - protection against ionising radiation of 5 December 2013 laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation, and repealing Directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom and 2003/122/Euratom
- Directive 2013/35/EU of the European Parliament and of the Council of 26 June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (20th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) and repealing Directive 2004/40/EC. *Off J Eur Union* 2013, L 179/1, 1–21
- International Commission on Non-Ionizing Radiation Protection (ICNIRP). Guidelines for limiting exposure to time-varying electric, Magnetic, and electromagnetic fields (up to 300 GHz). *Health Phys* 1998, 74(4), 494–522. 452
- International Commission on Non-Ionizing Radiation Protection (ICNIRP). Guidelines for limiting exposure to electromagnetic fields (100 kHz to 300 GHz). *Health Phys* 2020, 118(5), 483-524. DOI: 10.1097/HP.0000000000001210
- Directive 2006/25/EC of the European Parliament and of the Council of 5 April 2006 on the minimum health and safety requirements regarding the exposure of the workers to risks arising from physical agents (artificial optical radiation) (19th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC).
- Directive 2003/10/EC of the European Parliament and of the Council of 6 February 2003 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (noise) (Seventeenth individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC).

Pilot 2 will be implemented in Poland. For this reason, additional legal regulations based on national documents are applicable. These include the following documents:

- Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. 1974 Nr 24 poz. 141) / The Act of 26 June 1974 the Labour Code. (Journal of Laws of 1974, No. 24, item 141)
The Labour Code is a normative act constituting a set of provisions regulating the rights and obligations covered by the employment relationship in relation to all employees, regardless of the legal basis of their employment and employers. The most important issues in the code concern: employment relationship, remuneration for work and other benefits, obligations of the employer and employee, working time, employment of young people, occupational health and safety, handling disputes over employment claims and responsibility for offenses against employee rights.
- Rozporządzenie Ministra Gospodarki i Pracy z dnia 27 lipca 2004 r. w sprawie szkolenia w dziedzinie bezpieczeństwa i higieny pracy / Regulation of the Minister of Economy and Labour of 27 July 2004 on training in the field of health and safety at work
The regulation concerns training that should be organised by the employer for employees. This includes introductory, periodic, and induction training.

- Rozporządzenie Ministra Infrastruktury z dnia 6 lutego 2003 r. w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych / Regulation of the Minister of Infrastructure of 6 February 2003 on occupational health and safety during construction works
The regulation deals with access control to construction sites and the enforcement of restrictions on danger zones.
- Rozporządzenie Ministra Infrastruktury z dnia 26 czerwca 2002 r. w sprawie dziennika budowy, montażu i rozbiórki, tablicy informacyjnej oraz ogłoszenia zawierającego dane dotyczące bezpieczeństwa pracy i ochrony zdrowia / Regulation of the Minister of Infrastructure of 26 June 2002 on the construction, assembly and demolition log, information board and announcement containing data on occupational safety and health protection
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów / Regulation of the Minister of the Interior and Administration of 7 June 2010 on fire protection of buildings, other structures and areas
- Rozporządzenie Ministra Rozwoju, Pracy i Technologii z dnia 18 lutego 2021 r. zmieniające rozporządzenie w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy / Regulation of the Minister of Development, Labour and Technology of 18 February 2021 amending the regulation on the maximum allowable concentrations and intensities of factors harmful to health in the work environment

3.2.3 Cohesive vehicle monitoring and diagnostics (Pilot 3)

Within the Cohesive vehicle monitoring and diagnostics pilot (pilot 3), we can distinguish two separate applications: fleet in-service emission verification and vehicle diagnostics (Pilot 3a) and vehicle exterior condition inspection and documentation (Pilot 3b). While general regulations identified for ASSIST-IoT pursuits (see section 3.1) relate to both Pilot 3a and Pilot 3b, there are several additional regulations that relate specifically to emissions and vehicle diagnostics. The main legislation corpus for emissions is the following:

EURO 6 Emission Regulation:

Regulation (EC) No 715/2007 — type-approval of light passenger and commercial vehicles with respect to emissions (Euro 5 and Euro 6) and access to vehicle repair and maintenance information

Worldwide harmonised Light-duty vehicles Test Procedures (WLTP) and Real driving emissions (RDE):

Regulation (EU) 2017/1151 — supplementing Regulation (EC) No 715/2007 on type-approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information

In addition, general legislation concerning vehicle safety can be found in the following documents. The first document is a huge collection of all the directives within the EU market for various vehicle components to obtain CE marking, while the second one better corresponds to Pilot 3A application.

Regulation (EU) 2018/858 — approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles

Regulation (EU) 2019/2144 — type approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users

The main regulation for the Pilot 3b project are the EU-GDPR provisions including the German extensions via the "Bundesdatenschutzgesetz". As the vehicles are automatically scanned during their pass through the scanner, all relevant personal direct (faces) or indirect (license plates) data must be protected according to the mentioned

rules. The general rules for data governance, cybersecurity and artificial intelligence are also here relevant and applied.

Obviously, the general product liability laws concerning automation system, electronic devices & machinery also apply for the planned scanner system(s), where are several aspects for the pilot project are considered as R&D components and not usual, commercially available products.

3.3 Selected standards relevant to ASSIST-IoT pursuits

Besides general regulations and directives, specific technical requirements for products, processes, services and test methods are often included in standards. Therefore, within the review of legal regulations that may have implications on the ASSIST-IoT pursuits, also the most relevant standards have been included. Considering the scope of the selected standards, they were divided into four subsections:

- Standards related to electronic devices and machinery – see section 3.3.1 (Table 1),
- Standards related to cybersecurity and data protection - see section 3.3.2 (Table 2),
- Standards related to 5G technology - see section 3.3.3 (Table 3),
- Standards related to OSH - see section 3.3.4 (Table 4).

3.3.1 Standards related to electronic devices and machinery

Table 1 Standards related to electronic devices and machinery

Topic	European standard
RFID	ISO/PWI TR 22100-4 and IEC/CD 63074:2017 concerning security aspects (RFID)
	European Telecommunications Standards Institute (ETSI) EN 302-208 V3.3.1 (2020-08). Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W and in the band 915 MHz to 921 MHz with power levels up to 4 W; Harmonised Standard for access to radio spectrum; ETSI: Sophia-Antipolis, France, 2016.
Electromagnetic compatibility	EN-IEC 61000-4-2 Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test
	EN-IEC 61000-4-3 Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test
	EN-IEC 61000-4-4 Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test
	EN-IEC 61000-4-5 Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test
	EN-IEC 61000-4-6 Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields
	EN-IEC 61000-4-8 Electromagnetic compatibility (EMC) - Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test
	EN-IEC 61000-6-1 Electromagnetic compatibility (EMC) - Part 6-1: Generic standards - Immunity standard for residential, commercial and light-industrial environments

Topic	European standard
	EN-IEC 61000-6-2 Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity standard for industrial environments
	EN-IEC 61000-6-3 Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for equipment in residential environments
	IEC 63203- 201 series Part 201-3: Electronic textile - Determination of electrical resistance of conductive textiles under simulated microclimate; Part 201-2. Electronic Textile. Measurement methods for basic properties of conductive fabric and insulation materials
Machinery	EN ISO 13849-1 Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design
	EN 1746 Safety of machinery. Guidance for the drafting of the noise clauses of safety standards
	EN ISO 4871 Acoustics – Declaration and verification of noise emission values of machinery and equipment
	ISO 12100 safety of machinery. general principles for design. risk assessment and risk reduction
	EN 13557 + A2 Cranes. Controls and control stations

3.3.2 Standards related to cybersecurity and data protection

Table 2 Standards related to cybersecurity and data protection

Topic	European standard
Cybersecurity and data protection	ISO/IEC 27006:2015(en) Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
	ISO/IEC TS 27006-2:2021(en) Requirements for bodies providing audit and certification of information security management systems — Part 2: Privacy information management systems
	ISO/IEC 27007:2020(en) Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing
	ISO/IEC 27010:2015(en) Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications
	ISO/IEC 27011:2016(en) Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations;
	ISO/IEC 27013:2015(en) Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
	ISO/IEC 27018:2019(en) Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	ETSI EN 303 645 « CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements

3.3.3 Standards related to 5G technology

Table 3 Standards related to 5G technology

Topic	European standard
European standards for 5G deployment	ETSI TR 121 915 V15.0.0 (2019-10): Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Recommendation of 5G Phase 1 deployment, Release 15 also specifies, among other Features: further enhancements on Critical Communications (including Ultra Reliable Low Latency Communication and Highly Reliable Low Latency Communication), Machine-Type of Communications (MTC) and Internet of Things (IoT), Vehicle-related Communications (V2X), Mission Critical (MC), and features related to WLAN and unlicensed spectrum. https://www.etsi.org/deliver/etsi_tr/121900_121999/121915/15.00.00_60/tr_121915v150000p.pdf
	ETSI TS 122 261 V15.7.0 (2019-03): 5G; Service requirements for next generation new services and markets https://www.etsi.org/deliver/etsi_TS/122200_122299/122261/15.07.00_60/ts_122261v150700p.pdf
	ETSI TS 22.185, LTE; Service requirements for V2X services; https://www.etsi.org/deliver/etsi_ts/122100_122199/122185/14.03.00_60/ts_122185v140300p.pdf
	ITU-R M.2150 (IMT-2020); ‘Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2020 (IMT-2020); https://www.itu.int/rec/R-REC-M.2150-0-202102-I/en
	3GPP TS 23.501 V17.0.0; Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2; (Release 17); https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144
Network Function Virtualisation	ETSI, NFV Release 4 Definition; https://docbox.etsi.org/ISG/NFV/Open/Other/ReleaseDocumentation/NFV(21)00025_NFV_Release_4_Definition_v0_3_0.pdf
Multi-access Edge computing	ETSI GR MEC 031; Multi-access Edge Computing (MEC) 5G Integration; https://www.etsi.org/deliver/etsi_gr/MEC/001_099/031/02.01.01_60/gr_MEC031v020101p.pdf
	ETSI GS MEC 003; Multi-access Edge Computing (MEC); Framework and Reference Architecture; https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/02.02.01_60/gs_MEC003v020201p.pdf
Standards for electromagnetic fields protection	ICNIRP (International Commission on Non-ionizing Radiation Protection), Guidelines for Limiting Exposure to Electromagnetic Fields (100kHz to 300GHz); https://www.icnirp.org/cms/upload/publications/ICNIRPrfgdl2020.pdf

3.3.4 Standards related to OSH

Table 4 Standards related to occupational safety and health

Topic	European standard
Occupational risk management	PN-N-18002:2011. Systemy zarządzania bezpieczeństwem i higieną pracy. Ogólne wytyczne do oceny ryzyka zawodowego (Occupational health and safety management systems. General guidelines for occupational risk assessment). PKN, Polish standard
Electromagnetic fields	PN-T-06580-3:2002. Ochrona pracy w polach i promieniowaniu elektromagnetycznym o częstotliwości od 0 Hz Część 3. Metody pomiaru i oceny pola na stanowisku pracy (Protection of work in fields and electromagnetic radiation with a frequency from 0 Hz to 300 GHz. Part 3. Methods of measuring and evaluating the field at the workplace). PKN, Polish standard PN-T-06260:1974 (PN-74/T-06260). Źródła promieniowania elektromagnetycznego. Znaki ostrzegawcze (Sources of electromagnetic radiation. Warning signs). PKN, Polish standard
Optical radiation	EN 14255-1:2005. Measurement and assessment of personal exposures to incoherent optical radiation Ultraviolet radiation emitted by artificial sources in the workplace EN 14255-2:2005. Measurement and assessment of personal exposures to incoherent optical radiation Visible and infrared radiation emitted by artificial sources in the workplace EN 1836:2005+A1:2007. Personal eye protection. Sun glare glasses and filters for general use. EN 172 - 1: 1994 Personal eye protection. Sun glare filters for industrial use
Noise	EN ISO 9612:2009. Acoustics - Guidelines for the measurement and assessment of noise exposure in the work environment. PN-N-01307:1994. Hałas – Dopuszczalne wartości hałasu w środowisku pracy – Wymagania dotyczące wykonywania pomiarów (Noise. Permissible values of noise in the workplace. Requirements relating to measurements). PKN, Polish standard EN ISO 4871:2009. Acoustics - Declaring and verifying the noise emission values of machines and devices. EN ISO 9612:2009. Acoustics - Determination of occupational noise exposure - Technical method. EN ISO 10052:2004/A1:2010. Acoustics — Field measurements of airborne and impact sound insulation and of service equipment sound — Survey method. EN ISO 11201:2010 Acoustics — Noise emitted by machinery and equipment — Determination of emission sound pressure levels at a work station and at other specified positions in an essentially free field over a reflecting plane with negligible environmental corrections.
Vibration	EN ISO 5349-1:2001. Mechanical vibration — Measurement and evaluation of human exposure to hand-transmitted vibration — Part 1: General requirements. EN ISO 5349-2:2001. Mechanical vibration — Measurement and evaluation of human exposure to hand-transmitted vibration — Part 2: Practical guidance for measurement at the workplace.
Work under electric voltage	EN 50528:2010. Insulating ladders for use on or near low voltage electrical installations

Topic	European standard
	<p>EN 60900:2012. Live working - Hand tools for use up to 1 000 V a.c. and 1 500 V d.c.</p> <p>EN 61557-6:2007. Electrical safety in low voltage distribution systems up to 1 000 V a.c. and 1 500 V d.c. - Equipment for testing, measuring or monitoring of protective measures - Part 6: Effectiveness of residual current devices (RCD) in TT, TN and IT systems.</p> <p>EN 61479:2001. Live working - Flexible conductor covers (line hoses) of insulating material.</p> <p>EN 61229:2001/A2:2003. Rigid protective covers for live working on a.c. installations.</p>
Workload, ergonomic and psychosocial risks	<p>EN 1005 Series:</p> <ul style="list-style-type: none"> - EN 1005-1:2001+A1:2008 Safety of machinery - Human physical performance – Part 1: Terms and definitions - EN 1005-2:2003+A 8 1:200 Safety of machinery - Human physical performance – Part 2: Manual handling of machinery and component parts of machinery - EN 1005-3:2002+A1:2008 Safety of machinery Safety of machinery - Human physical performance – Part 3: Recommended force limits for machinery operation - EN 1005-4:2005+A1:2008 Safety of machinery - Human physical performance – Part 4: Evaluation of working postures and movements in relation to machinery - EN 1005-5 Safety of machinery - Human physical performance – Part 5: Risk assessment for repetitive handling at high frequency
Protective helmets	<p>EN 397:2012+A1:2012 Industrial safety helmets</p> <p>EN 14052:2012+A1:2012 High performance industrial helmets</p>
Protective clothing	<p>EN ISO 13688:2013 Protective clothing - General requirements</p> <p>EN ISO 20471:2013+A1:2016 High visibility clothing - Test methods and requirements</p>
Protective glasses	EN 166:2001 Personal eye protection. Requirements
Equipment protecting against falls from a height	<p>EN 795:2012 Personal fall protection equipment - anchor devices</p> <p>EN 354:2010 Personal fall protection equipment. Lanyards</p> <p>EN 355:2002 Personal protective equipment against falls from a height. Energy absorbers</p> <p>EN 360:2002 Personal protective equipment against falls from a height. Retractable type fall arresters</p> <p>EN 353-1:2014 Personal fall protection equipment. Guided type fall arresters including an anchor line. Guided type fall arresters including a rigid anchor line</p> <p>EN 353-2:2002 Personal protective equipment against falls from a height. Guided type fall arresters including a flexible anchor line</p> <p>EN 361:2002 Personal protective equipment against falls from a height – Full body harnesses</p>

Topic	European standard
	EN 364:1992 Personal protective equipment against falls from a height – Test methods

4 Legal aspects related to the Data Management plane

According to the initial ASSIST-IoT architecture definition (Deliverable D3.5), the Data Management plane encompasses any processes, in which data are processed to deliver features concerning data interoperability, annotation, security, acquisition, provenance, aggregation, fusion, etc. Therefore, ensuring that all processes are performed in line with the existing laws and regulations, it is of the highest importance for the whole ASSIST-IoT pursuits. In relation to the Data Management plane, three main legal aspects have been identified that should be considered at the development phase: (1) safety; (2) data protection and privacy, and (3) cybersecurity. Thus, the aim of this section is to discuss those aspects providing the legal landscape for further consideration during the development works.

4.1 Safety

Ensuring safety in AI-driven applications is one of the biggest challenges as it requires the reliability and validity of the datasets used for the training purposes [1]. In order to perform its assumed functionality, AI needs to find a pattern in the training datasets. Small or limited (e.g. profiled) datasets, corrupted data or infected algorithms may lead to finding a wrong pattern between the input and the output, resulting in incorrect and unsafe recommendations [2]. When a case is not adequately represented by the data, the accuracy of the system will be compromised. According to Gerke et al. [1] “*machine learning system or human-trained algorithm will only be as trustworthy, effective, and fair as the data that it is trained with*”. Considering the ASSIST-IoT pilot domains, such AI-based errors may ultimately lead to property damage and high monetary losses (e.g. due to collision during remote RTG operation), but also to a harm to humans or even their death (e.g. in the case of wrong decision on evacuation route). Some examples of damage caused by AI use were reported by Gluyas and Day [3]: running over pedestrians by driverless cars, crashes and damage caused by a partially operated drone, wrongful medical treatment diagnosis.

4.2 Data protection and privacy

Several legal challenges for the Next Generation Internet of Things (NGIoT) reference architecture stem from a pilot-driven need to process personal data. According to Article 4(1) of the GDPR, the term “personal data” is defined as “any information relating to an identified or identifiable natural person (‘data subject’)”. Moreover, while within the Smart Safety of Workers pilot, workers’ physiological data are going to be processed. These data fall into a special category of personal data according to Article 4(15) and Article 9(1) of the GDPR, processing of which is prohibited. This limitation does not apply to cases where the data subject (e.g. worker) has given explicit consent for one or more specified purposes.

As already described in the Data Management Plan (Deliverable 2.2), the GDPR also specifies key principles related to personal data such as: (1) lawfulness, fairness and transparency; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality; and (7) accountability, as well as data subjects’ rights: (1) right to be informed; (2) right of access; (3) right to rectification; (4) right to erasure; (5) right to restriction processing; (6) right to data portability; (7) right to object; (8) right in relation to automated decision making and profiling.

The above mentioned provisions impose particular legal challenges to AI-based applications, as discussed by Rodrigues [4]. Among others, specifically in relation to privacy and data protection, she indicated, following Wachter and Mittelstadt [5], that “*individuals are granted little control and oversight over how their personal data is used to draw inferences about them*”. The complexity of methods used in big data analysis makes providing the transparency extremely challenging.

In order to meet GDPR requirements, recommendations include paying close attention by developers to ethical and regulatory restrictions at each stage of data processing supported by the informed consent for the use of AI,

as well as data anonymization [6], [7]. The measures taken to ensure personal data protection within the ASSIST-IoT are described in Ethics and Privacy Protection Manual (Deliverable 2.3).

4.3 Cybersecurity

Automation of decision making with the use of artificial intelligence means that a human is not involved in this process and catching eventual irregularities is dependent only on the provided algorithms. Limited or lack of appropriate measures for providing the system's cybersecurity may lead to significant errors and fatalities due to incorrect decisions made by an infected AI-based algorithm. Special attention to cybersecurity vulnerabilities in AI was paid by Comiter [8] who highlighted that while in the traditional cybersecurity vulnerability, the problem can be fixed or patched, in the case of AI attacks the problem is more in the algorithms and their reliance on data. Many AI cyberattacks result from gaining access to datasets or model details. Rodrigues [4] summarised several solutions that are available to address this issue such as: incorporating the cybersecurity vulnerabilities in the design process; involvement of the human analysts in making critical decisions; using risk management programmes; and software updates. In order to include the security in the development cycle of the ASSIST-IoT project, a DevSecOps methodology has been adopted. The DevSecOps characteristics and practices are also described in the Ethics and Privacy Protection Manual (Deliverable 2.3).

5 Implications of legal aspects on pilots

In order to guarantee the successful deployment of NGIoT reference architecture in the three human-centric pilots embraced in the project, i.e., port automation (pilot 1), smart safety of workers (pilot 2), and cohesive vehicle monitoring and diagnostics (pilot 3), the industrial and academic leaders of each pilot are responsible for ensuring the safety of operations and compliance with European and national law. Therefore, based on the review of existing legal regulations (see section 3), their implications on the ASSIST-IoT pilots were analysed. Given the above, the aim of this section is to identify the characteristic pilot-related regulatory constraints on the development and integration of the ASSIST-IoT project enablers, solutions and services, as well as their demonstration and validation. This section is divided into three subsections according to the defined ASSIST-IoT pilots.

5.1 Implications on Port Automation pilot

Pilot 1 is focused on automation and optimisation of the logistics processes during the planification stage and taking better decisions during real-time operations, by improving the availability of information (IoT, edge) and the way it is presented to the terminal staff. Several implications can be foreseen with respect to personal data protection, and cybersecurity, workers safety, and environmental sustainability.

5.1.1 Personal data protection, privacy, and cybersecurity

The GDPR regulation is already being taken into account in the daily operations over terminal's owned machines involving terminals workers and stevedores. Nevertheless ASSIST-IoT will introduce new privacy and authentication mechanisms in order to support the exchange of terminal's data with an external truck. In particular, regarding GDPR implications, it is considered that privacy control mechanisms of ASSIST-IoT should prevent sending the external truck driver's personal data (i.e., their id or name) to the terminal's IT systems and machinery, which only needs an internal authorisation of the company.

Regarding M2M authentication, the involved CHEs in the loading/unloading process, both the Trucks (either internal Terminal Tractors, either external truck) and RTG cranes should authenticate each other, then confirm their work instructions and if everything is fine - exchange operational data. Since two machines are expected to autonomously cooperate, it is important to define what M2M communication channel will be used. In order not to surpass coverage limitations, a near field technology such as Bluetooth should be used. This also implies that the authentication certificates should also be embedded within the machines involved in the process, and not going to an external cloud database system.

All the aforementioned challenges will for sure follow the EU and Maltese GDPR legislations, as well as 2010/65/EU, 2005/65/EC, 2016/1148 EU security directives for ports.

5.1.2 Workers safety

Demands to increase productivity, energy efficiency and machine autonomy increases complexity of machine control and safety systems in port terminals. Machines can have various control modes and different levels of automation. New adaptive safety concepts are studied and developed to enable operational flexibility and advanced human-machine co-operation as well as to increase machine performance by intelligent safety solutions in different operating modes.

ASSIST-IoT will introduce new adaptive and flexible safety concepts in port crane applications, which will have impact on machine and system suppliers as well as port terminal planning and management. In particular, latency control of remote operation will affect the operational performance of the machine, but also workers safety that are closer to the physical infrastructure. To do so, for instance, safety mechanisms should be put in place at higher remote operation latencies in which the maximum speed of the equipment should be lower to warrant the safety and the control of the equipment and the workers. Since ASSIST-IoT will provide graphical information about latency values, the remote crane operator will be able to first slowdown machinery movements, and if needed, finally force and stoppage of the crane. This slowdown will follow the different safety directives identified for port machinery (EN 13557, EN 60204-32, EN ISO 13849-1, ISO 12100), as well as for health of workers (89/391/EEC, 2001/96/EC).

5.1.3 Environmental sustainability

The reduction of carbon emissions is not only a major challenge for the logistics sector, but also from national and European institutions. In particular, the EU has set a target of reducing greenhouse gas emissions by 80-95% by 2050 compared to 1990. Terminal operators have taken this responsibility to reduce carbon emissions seriously through the development of a common methodology for calculation carbon emissions. In particular, container terminals use the “number of boxes entering and leaving the terminal” as the common denominator to estimate gas emissions. The methodology is utilised by dividing the total terminal emissions by the total number of containers entering and exiting a port in a year. This gives the total figure for a terminals total emissions per container handled (kgCO₂e/box). Thanks to the expected operational efficiencies increase provided by ASSIST-IoT technologies, the number of containers handled per year in the terminal will be increased, and consequently reduced the total emissions per container of Malta.

Furthermore, the use of “E” yard equipment (e.g., electricity-powered remote RTGs) of ASSIST-IoT will allow Malta Freeport to switch from traditional diesel-powered vehicles to electric vehicles. By using “E” yard equipment, MFT can take concrete steps to reduce consumption while also ensuring a high level of operational efficiency. These enhancements will be compliant with the EN ISO 1400:2015, and EN ISO 4871.

5.2 Implications on Smart Safety of Workers pilot

The aim of pilot 2 is to increase safety of workers at the construction site thanks to the ASSIS-IoT use. However, the implementation of new technologies such as artificial intelligence and NGIoT in the area of occupational safety and health, also imposes some legal constraints that should be considered in order to guarantee workers’ rights and safety. The main identified areas of legal restrictions include: personal data protection and privacy, general provisions for safety and health at work on the construction site, essential health and safety requirements for personal protective equipment (PPE), and ethics.

5.2.1 Personal data protection and privacy

While implementing the ASSIST-IoT project, the demonstration and validation activities within pilot 2 will be performed at the construction site provided by Mostostal Warszawa SA, one of the ASSIST-IoT consortium partners. Mostostal Warszawa SA pays special attention to the protection of personal data. Currently, the processing of personal data takes place on the basis of the GDPR regulations. More information about the personal data protection procedure existing in Mostostal Warszawa SA is available at: <https://www.mostostal.waw.pl/en/company/personal-data-protection>. However, the implementation of AI-based technologies into the work environment will mean that the existing procedures will require an update.

The use of AI is tightly connected with automated decision making and limited algorithmic transparency that demands particular attention in order to meet the GDPR requirements. Given that workers' physiological data and location will be processed in the Smart Safety of Workers pilot, this pilot domain is particularly challenging. Therefore, several studies analysed possible solutions to legal and human rights issues related to AI use. Undoubtedly, including special legal requirements to the Data Management plane is a necessity (see section 4), however, due to the automated decision-making process, lack of user acceptance will also completely block the implementation of the AI-based technologies in the work environment due to the GDPR requirements. Therefore, raising awareness [4] and building trust that workers' processed data will not be used against them is crucial. This can be achieved by providing relevant education to the users (in this case – workers) with technology demonstration. Besides updating the content of the consent for processing personal data, trainings should be provided to workers with a clear explanation which exactly personal data are processed, what the aim of the processing is, how the data are processed, how they are stored and secured.

Within the ASSIST-IoT, the monitoring and protection of construction workers' personal health and safety will be provided. However, in order to ensure workers' privacy, those data cannot be accessed by the employer. Moreover, special procedures for incidental findings should be implemented. The collected health data should be a basis for further processing in order to detect abnormalities that are threatening workers' health and safety. Only a need for emergency and rescue should be notified. However, in order to ensure OSH supervision of subcontractors at the construction site, workers' authorisation is also needed. This information (Table 5) should be available to the employer in order to verify whether no authorised entry has occurred.

Table 5 Example of information on a subcontractor's employee

Company	Name
Personal data	Name and Surname
OSH training	Expiry date
Adaptation training for construction works	Date
Medical tests (admission to work, work at height)	Expiry date
Special permissions	Name and expiry date
Manager	Name and Surname

5.2.2 General provisions for safety and health at work on the construction site

The European Framework Directive on Safety and Health at Work (Council Directive 89/391/EEC) adopted in 1989 guarantees minimum safety and health requirements throughout Europe. It imposes an obligation on employers to take the measures necessary for the safety and health protection of workers, including the prevention of occupational risks and the provision of information and training, as well as the provision of the necessary organisation and means. The employer should follow the general principles of prevention, in which avoiding risks comes first, while giving collective and individual protective measures, as well as appropriate instructions to workers come last. Therefore, the implementation of the ASSIST-IoT in the work environment, does not mean that the employer is exempt from the obligation to avoid the risk in the first place.

Considering the ASSIST-IoT pursuits, as well as European (international level), Polish (national level) and Mostostal Warszawa SA (company level) legal regulations in the field of both occupational safety and health and construction works, the most important provisions have been summarised with an indication of the “question marks” that need to be checked in order to ensure workers' safety, as well as the safety for conducting demonstration and validation activities.

Protective barriers

A fall of a person from even a small height usually results in death or permanent disability. Accident statistics confirm that the risk of falls from a height prevails in the construction industry.

To be checked:

- Are all workstations at height secured with safety barriers?
- Is the main barrier at a height of min. 1.1 m?
- Have safety zones around the works carried out at height been designated, fenced off and marked?

Protection of excavations

Working in excavations is particularly dangerous. Unprotected walls of excavations deeper than 1 m pose a real risk of backfilling that may slide to the ground. There are many ways to protect the walls of excavations, which guarantee safe conditions for the people working in them. When preparing works in excavations, it is necessary to select a method of securing the walls against landslides and to designate, mark and fence dangerous zones where there is a risk of falling into the excavation.

To be checked:

- Are there any protective barriers close to the excavations?

Protection of power lines

Electric cables of overhead power lines running over the area of construction works may pose serious threats. Accidents most often occur during unloading works, when it is necessary to raise the vehicle's load box. In addition, the passage of large-size vehicles under overhead power lines without keeping the minimum distances from them may lead to electric shock.

To be checked:

- Do overhead power lines run over the area of the construction works?

Protection against electric shock

An electric shock is one of the most dangerous hazards that can occur on a construction site. When organising and conducting works on electrical power devices and installations (Figure 1), it is necessary to ensure appropriate and effective protection against electric shock. Connections of electric cables with mechanical devices or tools, as well as the cables themselves must be protected against mechanical damage.

To be checked:

- Do the persons authorised to operate electrical devices and installations have the required authorisations?
- Are construction switchboards secured against unauthorised access?



Figure 1 A view of the electrical power installation

Traffic of vehicles at the construction site

Vehicle traffic on the construction site poses a serious threat to the surrounding environment. Most often, it is associated with the possibility of running over or hitting people standing behind a reversing vehicle or construction machine. Even efficient and properly installed rear-view mirrors in vehicles and road machines do not eliminate the so-called "blind spot" outside the driver's observation area. That is why, it is so important to give clear signals by vehicles or construction machines retreating on the construction site to warn bystanders or other road users.

To be checked:

- Do all vehicles performing a reversing maneuver signal it with an acoustic or acoustic- light signal?

Health and safety annex to the contract

Subcontractors may perform work for the general contractor only on the basis of a previously signed contract. The contract should contain work safety requirements that must be met by the subcontractor when preparing and carrying out works in accordance with the scope specified in the contract. Work safety requirements include the obligations and rights of the subcontractor, as well as the consequences of non-compliance with them.

To be checked:

- Has the subcontractor received an appendix on health and safety requirements with the contract?
- Has the subcontractor appointed a contact person with the general contractor who is responsible for health and safety matters?

Safety instructions

Any construction work should be carefully planned. Safety instructions are the documents confirming the preparation for the implementation of construction tasks. On their basis, workstations should be prepared, machines, equipment and tools should be selected, and people should be trained to perform their assigned tasks. Safety instructions should contain precise information on the hazards that may occur and the methods of their elimination or reduction to an acceptable level.

To be checked:

- Have safety instructions been developed and accepted for the planned works?

Information training

All new recruits to work at construction sites undergo health and safety information training. This applies to both in-house and subcontractors' employees.

To be checked:

- Have all people starting work on the construction site completed health and safety information training?

Danger zones

A danger zone (Figure 2) is a place at the construction site, where there is a threat to human life or health.

Balustrades should be placed around the excavations at a height of 1.1 m above the ground and at a distance of not less than 1 m from the edge of the trench.

The danger zone where objects fall from height must not be less than 1/10 of the height.

Any work involving the risk of falling to the ground from a height above 1m is work at height.

The danger zone for a fall from height is at least 2 meters from the edge.

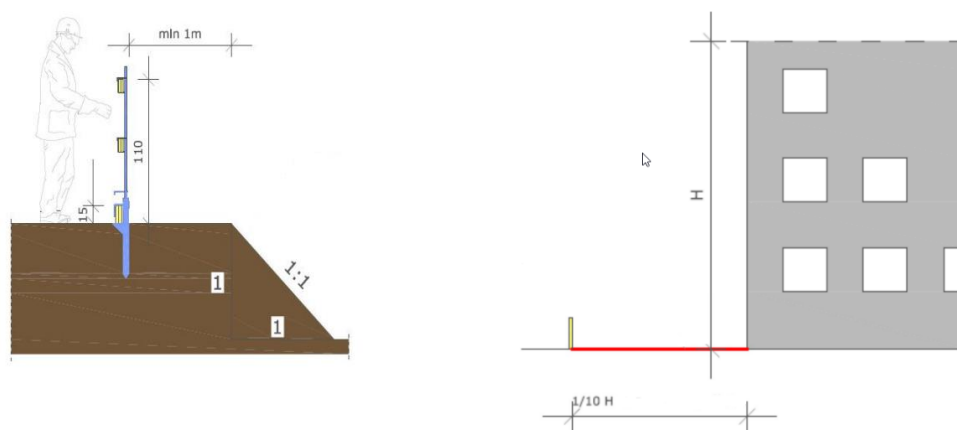


Figure 2 Visualisation of dangerous zones

The ASSIST-IoT pursuits should be coherent with the above mentioned general OSH provisions. Thanks to the ASSIST-IoT enablers, solutions and services, we will achieve benefits in terms of improving safety and health at the construction site. However, using artificial intelligence for this purpose raises also several challenges regarding legal aspects. Besides those described in Section 4, the liability for errors caused by AI is also an issue, as the deployment of AI technologies can cause damage to persons and property [4]. The involvement of multiple parties in the development of an AI-based system makes this liability difficult to determine. Rachum-Twaig [9] followed by Rodrigues [4] addresses this need through supplementary rules including a monitoring duty, built-in emergency breaks, and ongoing support and patching duties. In 2020 the European Commission published a report [10] that indicates the key issues in relation to the safety and liability of AI-based systems. It highlights the need to ensure the same level of protection for victims of AI technologies as for victims of traditional technologies, while maintaining the balance with the needs of technological innovation. It suggests certain adjustments to Product Liability Directive and national liability regimes on a targeted, risk-based approach.

5.2.3 PPE essential health and safety requirements

Considering the scope of ASSIST-IoT, personal protective equipment (PPE), being the carrier for wearable technologies, will play a particular role in the project. The main legal regulations related to the use of PPE, crucial for the ASSIST-IoT pursuits, are the following: Directive 89/656/EEC and Regulation (EU) 2016/425.

The Directive 89/656/EEC lays down the requirements for the use of PPE by workers at the workplace. PPE must be used when risks cannot be avoided or sufficiently limited by technical means of collective protection or procedures of work organisation. The equipment must comply with the relevant Community legislation on design and manufacture with respect to safety and health. All PPE must be suitable for the risks involved, without itself leading to any increased risk, correspond to existing conditions at the workplace, take account of ergonomic requirements and the worker's state of health, fit the wearer correctly after any necessary adjustments. The employer must provide the appropriate equipment free of charge and must ensure that it is in good technical and hygienic condition. Where the presence of more than one risk makes it necessary for a worker to wear simultaneously more than one item of PPE, such equipment must be compatible. Before choosing PPE, the employer is required to assess whether the PPE he intends to use satisfies the requirements of this Directive. Member States shall ensure that general rules are established for the use of PPE and/or covering cases and situations where the employer must provide such equipment. There must be prior consultation with employers' and workers' organisations. The employer shall organise training and demonstrate the use of PPE. Workers shall be informed of all measures to be taken. Consultation and participation shall take place in the matters covered by this Directive. In relation to the ASSIST-IoT pursuits, the Directive concerns the use of PPE such as: equipment protecting against falls from height, protective clothing, eye and face protectors, protective helmets to be used in the demonstration and validation activities in the project.

The Regulation (EU) 2016/425 lays down the requirements for the design and manufacture of PPE which is to be made available on the market, in order to ensure protection of the health and safety of users and establish rules on the free movement of PPE in the Union. PPE means: (a) equipment designed and manufactured to be worn or held by a person for protection against one or more risks to that person's health or safety; (b) interchangeable components for equipment referred to in point (a) which are essential for its protective function; (c) connexion systems for equipment referred to in point (a) that are not held or worn by a person, that are designed to connect that equipment to an external device or to a reliable anchorage point, that are not designed to be permanently fixed and that do not require fastening works before use. The Regulation applies to both specially prepared equipment and standard PPE purchased on the European market. The requirements of the Regulation also apply to equipment that will cooperate with PPE during tests, e.g. fall arrest detectors.

The following PPE is required for each construction site:

Protective helmet

A protective helmet (Figure 3) is the basic, personal protection against head injuries of people who work in exposure to risks related mainly to the fall of materials or other objects from above. In addition, the protective helmet eliminates or significantly protects against the effects of head hits against various elements or the ground in the event of a worker falling.

To be checked:

- Does everyone on the construction site have and use protective helmets as intended?
- Do the protective helmets have the CE mark and have the current expiry date?
- Do workers have chinstraps fastened to prevent the helmet from falling off the head?



Figure 3 Protective helmet

High visibility vest

A high visibility vest (Figure 4) is an element of the construction worker's clothing, ensuring its visibility in all conditions, regardless of the time of day.

To be checked:

- Does every worker and any other person on the construction site wear a warning vest?



Figure 4 High visibility vest

Protective footwear

A significant number of injuries suffered by construction site workers affect the lower limbs, especially the feet. These include sprains, fractures and wounds caused by sharp elements puncturing the sole of the shoe. The most common causes of foot injuries include nails left in dismantled wooden elements, e.g. formwork or railing barriers. In order to prevent this, work stations should be systematically arranged. In addition, the use of protective footwear (Figure 5) with anti-puncture inserts and a reinforced toe cap significantly reduces the risk of injury and other injuries to the feet, and the design of the shoe prevents the foot from twisting.

To be checked:

- Does everyone staying on the construction site use safe footwear of at least S3 class - with a reinforced toe cap and an anti-puncture insole?



Figure 5 Protective footwear

Even the driver of each vehicle entering the construction site should be equipped with a protective helmet, high visibility vest and protective footwear. Their use is obligatory when leaving the vehicle cabin.

To be checked:

- Does the driver have protective helmet, high visibility vest and protective footwear?

In the case of PPE of category II (including risks that relate neither to minimal ones covered by category I, nor to the risks covered by category III) and category III (including risks that may cause very serious consequences such as death or irreversible damage to health), they should have valid certificates of EU-type examination issued by a notified body. Moreover, without a permission from the notified body, any change in the PPE cannot be made. PPE with integrated additional elements (electronic devices, components, etc.) should be considered as a whole and submitted to the notified body for EU-type examination. PPE should be compatible with each other. Additional components cannot worsen the protective properties of PPE. If we interfere with the construction of PPE, for example by implementing electronic components, PPE should still meet the requirements of Regulation 2016/425 in terms of design and ergonomics principles (point 1.1.1 Annex II), as well as the Innocuousness (point 1.2.1, 1.2.1.1, 1.2.1.2 and 1.2.1.3), Comfort and effectiveness (point 1.3.1, 1.3.2). Specific requirements for particular kinds of PPE are included in standards harmonised with EU Regulation 2016/425:

- in the case of protective helmets: taking into account the scope of ASSIST-IoT and any other scopes industrial safety helmets should meet the requirements specified in EN 397:2012+A1:2012,
- in the case of safety glasses: Safety glasses should meet the requirements specified in EN 166: 2001.
- in the case of safety harnesses they should meet the requirements specified in EN 361:2002 and EN 358:2018.
- in the case of high visibility protective clothing: requirements of EN ISO 13688:2013 and EN ISO 20471:2013+A1:2016 should be met.
- in the case of fall arrest detector it should meet the requirements specified in EN 362:2004. The requirements concern some aspects of construction, materials, static strength and corrosion resistance.

5.2.4 Ethics

Within the ASSIST-IoT project, pilot sites ethics strategy, as well as ethical risk management and mitigation strategy have been developed (Deliverable 2.3 – Ethics and privacy protection manual), which should be respected in relation to all human subjects involved in the ASSIST-IoT. The ASSIST-IoT will comply with ethical principles and relevant national, European Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols.

From a legal point of view, research projects must comply with relevant national laws of the country where the research will be carried out. In turn, the national law of each country must fulfil the requirements of any international laws/treaties to which the countries concerned have subscribed. Furthermore, the standard-setting instruments are, therefore, classified according to their legally non-binding or binding character.

At the European level, biomedical research is governed by the Convention on Human Rights and Biomedicine and its Additional Protocol concerning Biomedical Research – these are binding in the States where they have been ratified. All research involving human beings should be conducted according to ethical principles described in the Council of Europe Convention on Human Rights and Biomedicine [11]. Domestic law / national level is related to guidelines published by Research Ethics Committees (RECs) [12]. RECs are multidisciplinary, independent groups of individuals appointed to review biomedical research protocols involving human beings to help ensure in particular that the dignity, fundamental rights, safety, and well-being of research participants are duly respected and protected. Their scope as a local, regional or national REC is defined by the appointing authorities.

Demonstration and validation activities within the pilot will involve the participation of human subjects who will be monitored and/or guided by a variety of technologies that may have an impact on their behaviour and performance in their work environment. All research involving human beings should be conducted according to the ethical principles described in the Council of Europe Convention on Human Rights and Biomedicine, which are universally recognised. Particular attention will be paid to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection. Human participation in research will be voluntary, and their consent will be expressed voluntarily in a specific, informed and unambiguous way and they will retain the right to withdraw at any time.

During demonstration and validation activities in WP7, human subjects will be equipped with smart technologies (including wearable health sensors and other devices e.g. with tracking function) that will monitor their health parameters. Sensitive data will be collected. To fulfill and implement pilots, information exchange and processing of personal data will be required between entities involved in the project and pilots. The general principles concerning personal data protection in relation to the smart environments, can be summarised as follows:

- users whose data are being collected should be aware that their data are being collected;
- data collected and stored in memory of IoT devices should be used only for the management of smart environment and for no other purposes;
- personal data collected, processed and transmitted by IoT devices should not be disclosed or shared with third parties without explicit permission of the users; and
- personal data collected should be kept safe and secure from potential abuse, theft, or loss.

The rights of all involved persons are guaranteed, inter alia, by documents such as The Charter of Fundamental Rights of the European Union providing for the respect for private and family life (Art. 7) and the protection of personal data (Art. 8) as well as the GDPR. The consent of the research participants to use the data collected from the research will be required. Processing of such datasets will be performed in accordance with H2020 and EU regulations [13]. Risk management issues and mitigations strategies concerning occupational and health hazards arising in the pilot will be conducted according to national OSH legislation described in Section 3.

5.3 Implications on Cohesive Vehicle Monitoring and Diagnostics pilot

The cohesive vehicle monitoring and diagnostic pilot is affected mainly by three legal aspects: protection of personal data, emission regulations and safety requirements, which will be described in this chapter.

5.3.1 Personal data protection

5.3.1.1 GDPR sensitive points related to the driver of connected vehicles

As in all other areas related to personal data within the EU legislation, the General Data Protection Regulation (GDPR) must be applied to the automotive pilot (pilot 3A). The European Data Protection Board (EDPB) guidelines [14] review the legal requirements on processing personal data in the context of connected vehicles. The applicable regulations are listed as:

- General data protection regulation (2016/679).
- “ePrivacy” Directive (2002/58/EC, as revised by 2009/136/EC).

The European Data Protection Supervisor highlights the following issues concerning data protection for connected cars [15]: lack of transparency, excessive data collection (including behavioural data), data retention, lack of user’s control over the data, lack of purpose limitation, and collection or inference of sensitive information.

While most aspects are generic and comparable to the other pilots (see sections 5.1 - 5.2), some are unique to the vehicle perimeter and will be discussed in detail.

In this context, the amount of sensors in the vehicle perimeter has increased exponentially in the last decades. Systems such as electronic Anti-lock braking (ABS) have become standard since the 1970s even in budget vehicles, driving the need to incorporate more and more sensors. As an example for the electronic ABS, wheel speed sensors are needed to measure the rotation speed of every wheel. While in the beginning wheel speed sensors were directly connected to the ABS, in modern vehicles this information is used by several electronic vehicle modules with the help of bus systems like the CAN bus. Data protection aspects come into play once modules need to store this information or especially if this information has to be transferred to the outside of the vehicle. As mentioned above, the wheel speed information is just an example – due to extended sensing capabilities modern vehicles are capable to paint a complete picture of every driving situation and driver use case. While sensors in early vehicles focused mainly on driving functionality, like the aforementioned ABS, modern vehicles offer much broader human-centric functionalities. Linking a personal mobile phone to the vehicle has become a standard in recent years, mixing vehicle and private data while offering parallel access to the mobile cloud. This, of course, triggers the need for a very strict personal data protection policy in the vehicle, ensuring that third parties are only able to access data if they are complying with the GDPR regulations and, where required by the law, if the driver has explicitly given consent.

Within the ASSIST-IoT automotive pilot, mainly propulsion system related data are processed, however also these data contain significant privacy aspects that need to be considered and protected. Therefore, the ASSIST-IoT architecture has to ensure two important principles:

- 1) Privacy-related data must be anonymised if possible. This can be done by handling emission-related data without information which can help to identify the driver, like the vehicle identification number (VIN), if possible. This principle especially applies to data which have to be stored in the cloud for later intensive processing or documentation purposes. However, it has to be noted that certain information must include private data, e.g. the information that a software update was successful on a certain vehicle.
- 2) Data which cannot be anonymised have to be encapsulated and protected to guarantee privacy. This can be achieved with the help of edge computing, as data can remain within the safe environment of the vehicle instead of transferring privacy-related information into the cloud.

It has to be noted that these fundamental principles apply only to later usage in series production and might have to be neglected especially during the early phase of the pilot development.

Privacy-related data in the vehicle perimeter can be divided into two main categories:

1) Data which can be used to identify the driver

Within the scope of the in-service emission and enhanced diagnostic pilot, only very limited data can be used to identify the driver. This mainly applies to the vehicle information number (VIN), which is unique for each vehicle. This of course implies that the VIN can only identify the vehicle, however this information opens the door to indirect identification of the driver. Within the context of the diagnostic and emission part of the automotive pilot, no biometric data are gathered or processed.

2) Data which affect privacy once the driver is identified

Most vehicle-related data can be considered irrelevant while presented alone. However, in the context of driver identification, a large amount of vehicle data incorporates privacy aspects which need to be protected. Two examples for data within this context are:

Location related data – Data like GPS are needed for emission geofencing, i.e. to reduce emissions temporarily in an urban environment. However, these data also enable tracking of the driver, which is an unwanted side effect.

Vehicle acceleration / deceleration / velocity – Vehicle acceleration has a direct impact on exhaust emissions. Also, a higher velocity results in higher driving emissions, due to increasing wind resistance at higher vehicle velocity. Therefore, this information is relevant to understand the emissions a vehicle generates. On the other hand, this information is critical, e.g. it contains detailed data on driving habits. In this sense, EDPB recalls that the initial consent of the driver on the GDPR will never legitimise further processing, as consent is only given in a specific context and therefore is automatically invalid outside of this context. Specifically, two relevant examples are pointed out:

- Telemetry data, collected during the use of the vehicle for servicing purposes must not be disclosed to motor insurance companies without the user's consent. Hence, it is not allowed to offer systematic analysis of driving behaviour for creating driver profiles affecting insurance policies.
- Data collected by connected vehicles may be processed by law enforcement authorities (e.g. to detect speeding) only when specific conditions in the law enforcement directive are fulfilled (as covered in art.10 of the GDPR)

The edge-cloud approach of the ASSIT-IoT can be levered to strictly meet such GDPR requirements. Specifically, and within the context of the pilot, sensitive data such as detailed location and driving profile may be kept in the far edge node, and not propagated to the cloud service. While this is not the only valid approach, it will allow a complete and by-design fulfilment of the data protection sensitive points.

5.3.1.2 GDPR sensitive points related to the driver of scanned vehicles

Within the context of the vehicle condition monitoring (pilot 3B), the vehicles are 360°- scanned as they pass through the scanner. Thus, the faces of the persons sitting in the vehicles are being potentially captured and the license plates of these vehicles are also gathered. Whilst the former are primary biometric data, the latter are indirect personal data, as they could be used in conjunction with additional information to indirectly identify persons who may have driven or were present in the scanned vehicle. For both types of personal data, several actions must be made to fulfil the legal aspects during the project.

Within the vehicle condition monitoring pilot (pilot 3B) the gathered, high-resolution, coloured images are used in two ways: 1. they provide the basis to create the necessary annotations for the Artificial Intelligent (AI-) algorithmic training, and 2. they are processed by the generated AI-engines for the automated surface inspection of the scanned vehicles. For both steps all the images containing human faces and vehicle license plates must be anonymised for visualisation and archiving purposes. This means, that they must be automatically detected and afterwards "pixelated".

For the pilot activities using the digital scanner at the TwoTronic premises, no particular measures must be taken with respect to the above aspects. All drivers and other persons sitting in the scanned vehicles will be

informed about and asked for their explicit permission for using their personal data for the pilot project needs before the vehicle scans. However, it is considered as a better practice to also include this scenario to the general personal data protection actions foreseen for the general case, where vehicle images are gathered from dedicated pilot installations participating in the pilot 3B.

This general case of pilot scanners in real operation at auto houses and car dealers also includes the generation of the AI-training data for the AI-based inspection. The associated AI-training needs thousands of annotations to generate enough amount of training instances. For these needs, the pilot activities include the usage of additional physical scanners situated in different locations with high vehicle traffic. In these locations any customer may drive his vehicle to the auto house dealership and pass through the scanner without a prior agreement about potential usage of his personal data. TwoTronic is collaborating with a few major automotive Original Equipment Manufacturers (OEMs), in whose premises some scanners are already installed and are ready to provide the hundreds of thousands of pictures, needed for the AI-training to allow for useful recall and precision performances of the resulting AI-engines. For these data, both the faces of all persons sitting in the cars (Figure 6) as well as their license plates (Figure 7) must be anonymised for further usage according to the existing laws concerning the personal data protection. The *anonymisation* process is conducted with the help of the AI-techniques. In this way no additional legal issues need to be considered for the further data treatment, e.g., in the case of storage duration of person-related videos (an acquisition frequency with more than 4 pictures per second is considered a video) in Europe, depending on the country, all the associated pictures must be deleted after 2-4 months. Also, the scanned vehicle images are displayed to the customer consultants of the automotive houses without showing the real faces of their customers, who brought their cars for inspection or repair. In this digitalisation process both, the consultant and the end user are inspecting the vehicle conditions by looking through the scanned images without explicit show of license plates content and face display. Similarly, the scanned pictures are remotely reviewed by the annotation- and the inspection- team via secure network connections, without biometrical data or indirect personal data. However, this process requires a minimal computing power at the edge nodes as well as appropriate network bandwidth with remote operator capabilities to handle the above operations.



Figure 6 Anonymised driver face to conform with personal data protection rules



Figure 7 Anonymised license plate to conform with personal data protection rules

To ensure the formal and correct exchange of images and data with the various scanners located in different auto houses for the needs of the pilot 3B, we must also consider several rules, typically obeying the exchange of critical data between European organisations. Data protection officers, several data interchange procedures including safety and archiving concepts, separate managers responsible for the data integrity and regulatory compliance for all co-working locations must be assigned and defined for the pilot project needs.

5.3.2 Emissions

Regulations regarding emissions worldwide have a long history. Along with the obvious goal to reduce emissions, each update has always been one of the major drivers for the technological evolution of the automotive propulsion systems and one of the main reasons for Pilot 3a, which is trying to identify innovative concepts in the vehicle emissions and enhanced (emission) diagnostics perimeter. While regional differences exist, three major action priorities may be identified from a general perspective:

- 1) The search for low emission technologies. For that, worldwide legislations have applied a progressive and persistent decrease in the limit of the regulated emissions, combined with the inclusion of additional species over the years (e.g. particulate number for diesel engines in Euro 5b and for gasoline engines in Euro 6). As shown in the graph on the left side of Figure 8, the EU regulated limits for diesel engines have been reduced by more than 90% for NO_x and 97% for particulate matter from Euro 2 to Euro 6d. Additionally, CO₂ emissions have been regulated at the fleet level for a few years.

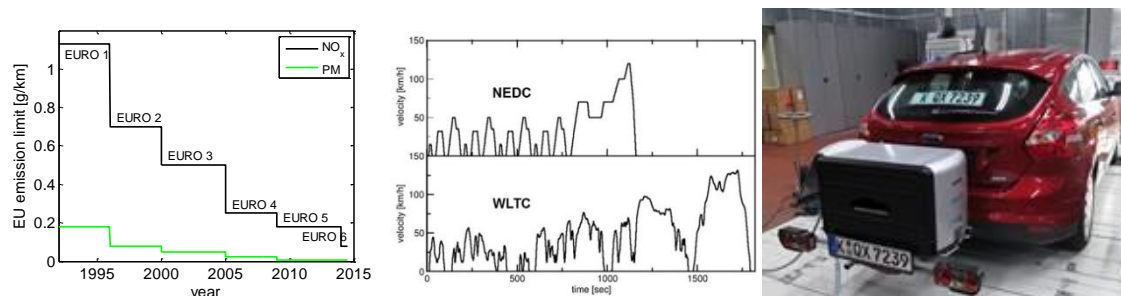


Figure 8 Evolution of the legislated emission limit for EU diesel light vehicles (left); NEDC and WLTC certification cycles (centre) and vehicle with PEMS system (right)

- 2) Ensuring that the emissions in real life operating conditions are consistent with the legislated values. Initial efforts were based on the increase of the representativeness of the certification cycle for real-life operation. As a consequence, old cycles as the New European Driving Cycle (NEDC) (top-central plot in Figure 8), originally designed for comparing emissions and consumption between different models,

have been replaced by more representative cycles such as the World Harmonised Light Vehicle Test Cycle (WLTC) (bottom-central plot). This trend has resulted in the later introduction of real driving emission (RDE) verification using portable emissions measurement systems (PEMS), where the vehicle is tested in real life conditions. In this case, the driving itself is unknown, yet the order and the street characteristics are known (urban, rural district and highway sections are included).

- 3) Ensuring that the emissions level does not vary over the service life. Here again, a couple of mechanisms have been employed. On the one hand, on-board diagnostics target the identification of faults impacting vehicle emission level. Since most engine subsystems can affect the engine emission output, this means most subsystems must be monitored. As a result, the On-Board-Diagnostics (OBD) layer has grown over the years and its advancement and calibration represents a significant part of the control system development. On the other hand, in-service conformity (ISC) mechanism is set to test a sample of vehicles in operation. A negative outcome of the ISC testing procedure forces corrective actions from the OEM in order to restore the fleet emission level.

As of now, within the European Union the Euro 6 emission regulation is in place and consequently car manufacturers have adapted their production to meet the given emission targets. However, the automotive emission and enhanced diagnostic pilot will focus on future Post-EU 6 regulations, which are currently under discussion and have not yet been finalised. Thus, any work within the emission part of the automotive pilot is based on assumptions only.

Vehicle and fleet emission levels should be kept within the legal limits throughout the vehicle life. While the ISC mechanism offers a verification of this through periodic testing of a limited sample of the fleet, the proposed connected diagnostics system offers a more universal approach – taking a larger portion of vehicles into account and considering real-life use of the fleet. How a cost effective, efficient, yet sufficiently precise method of fleet data acquisition could look like, which at the same time is less dependent on the ISC test procedures, remains an open question. A potential but consequent solution to address these demands could be to:

- a) Focus on fleet level emissions rather than single vehicle emissions, since emission level will vary depending on the individual circumstances of a given vehicle.
- b) Increase fleet wide emission sensing capabilities, using additional sensors when considered for a part of the fleet.
- c) Use statistical methods to prove that the entire fleet meets the ISC requirements within the desired confidence interval.

It is not yet clear how these ideas will be incorporated into the Post-EU 6 regulations once they are made public. However, due to its flexibility, the ASSIST-IoT infrastructure can be adapted with little effort, even if new, so far unexpected, ideas are brought up by the legislator during the current legislative procedure.

5.3.3 Safety

From a legal perspective, no specific legal requirements regarding firmware versions and update procedures have been identified. However, due to the paramount effect of the control software on the propulsive system behaviour, some aspects are to be considered since they could drive legal implications.

In the context of the ASSIST-IoT pilot, the project specifically covers the update of software calibrations for the emissions part of the pilot or adding enhanced diagnostic functionality into a given software framework on the edge. The updated emission calibration can be distributed after a full testing and release process successfully completed on the OEM side, making this process comparable to current release actions where modules are updated while the vehicle is in the garage. A more innovative approach to be implemented is to add a new level of calibration flexibility, either by using the AI/ML to provide unique optimal calibrations for each vehicle or by changing the calibration on the fly, for example with the help of geofencing technologies if the vehicle enters an urban area with stricter emission thresholds. In addition, innovative software functionality will be added within the enhanced diagnostic part of the pilot, ideally without the necessity to run a complete software release, which is a costly and time-consuming process. Below are the main aspects which need to be considered in this regard:

- Updated emission calibrations – it has been a reality for several years that some cities restrict access for older high emission vehicle. While so far these vehicles have had to stay outside of these sensitive inner urban areas, a more flexible use of emission calibrations could be useful in this context. As mentioned above, the geofencing technologies could be used to switch between two propulsion system calibrations, in order to fulfil strict emission thresholds in urban areas, while offering full vehicle performance according to less strict regulations in rural areas.
- Unique emission calibrations with the AI or Machine Learning (ML) assistance – currently only fixed calibrations are released which are designed for a whole vehicle fleet and only minor adjustments to production spread are possible. From emission perspective, it might be beneficial if this aspect is used to a larger potential in the future, because not only unavoidable production spread is a variable over the life of a vehicle. A vehicle, which is used in the southern Europe is likely to experience higher average outside temperatures compared to a vehicle in the northern Europe, so an adjusted propulsion system calibration could take this into account. Also, the personal driving behaviour could be used to improve emissions, if patterns are identified with the AI/ML assistance. However, this idea drives the need for a more flexible handling of calibrations, for example by releasing a safe and secure corridor of values instead of a fixed set of predefined values.
- Adding new software parts on the edge – in order to allow a flexible, yet safe and secure way to add enhanced diagnostics, it has to be ensured that these functions are separated from the safety critical parts of the Powertrain Control Module (PCM), for example with the help of software containers. This significantly differs from the current release process, because as a consequence not every software part is known before the release. Therefore, an adapted release process has to focus rather on secure software interfaces rather than the software itself.

For all of the above mentioned changes it is essential to ensure, that software updates must be performed in a secure manner. In order to do this, the code integrity must be verified, and any update process has to take place in safe situations only. That means that firmware updates must be done when the vehicle is parked as otherwise drivability could be compromised. For the case of minor software modifications (e.g. automated optimisation of the calibration values while the vehicle is in operation), mechanisms are to be set in order to ensure that drivability is not affected.

6 Legal guidance from the European and national regulatory bodies and authorities

Within sections 3 ÷ 5, legal aspects arising from the currently binding regulations are discussed. However, in order to prevent a situation in which the ASSIST-IoT enablers, solutions and services do not meet legal requirements when the project is finished, proposals for EU regulations related to the ASSIST-IoT pursuits have been also identified (section 6.1). Moreover, European and national regulatory bodies and authorities have been identified and contacted in order to provide ASSIST-IoT with legal guidance, especially in relation to personal data protection and requirements resulting from the GDPR (section 6.2).

6.1 Published proposals for EU regulations

A review of the regulations related to the ASSIST-IoT pursuits indicated that three relevant proposals for EU regulations have been already published:

- **in relation to the privacy:**
Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications),
- **in relation to data governance:**

Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act),

- **in relation to artificial intelligence:**

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts.

Considering the status of those regulations, it is necessary to follow their legislation process during the ASSIST-IoT project execution in order to be aware when they come into force.

6.2 Identified regulatory bodies and authorities

For the purpose of legal guidance, regulatory bodies and authorities relevant for the pilot domains have been identified and reached out to by means of official letters. A list of selected bodies is presented in Table 6.

Table 6 A list of regulatory bodies and authorities contacted for legal guidance in pilot domains

Regulatory body/authority	Name and Surname	Responsibility in terms of generating policy	Pilot domain
Directorate-General for Maritime Affairs and Fisheries European Commission 1049 Bruxelles/Brussel Belgium	Charlina Vitcheva DIRECTOR-GENERAL	Policy area of fisheries, the Law of the Sea and Maritime Affairs	Pilot 1
Directorate-General for Employment, Social Affairs and Inclusion European Commission 1049 Bruxelles/Brussel Belgium	Joost Korte DIRECTOR-GENERAL	Policy on employment and social affairs, education and training	Pilot 2
Directorate-General for Mobility and Transport European Commission 1049 Brussels Belgium	Henrik Hololei DIRECTOR-GENERAL	Policy on transport	Pilot 3
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs European Commission 1049 Bruxelles/Brussel Belgium	Kerstin Jorna DIRECTOR-GENERAL	Policy on the protection and enforcement of industrial property rights, coordinating the EU position and negotiations in the international intellectual property rights (IPR) system, and assisting innovators on how to effectively use IP rights	All pilots

Each official letter included a brief presentation of the ASSIST-IoT project and particular pilot according to the competences, identified legal challenges and a list of European regulations that seemed the most relevant for our purposes. Copies of the letters are included in the Appendix. In order to receive legal guidance, several legal challenges have been distinguished.

Legal challenges in relation to Pilot 1:

- avoiding incidental findings of driver's personal data while interchanging data with external trucks,
- ensuring meeting safety requirements of machines during remote control taking into account the latency,
- ensuring cybersecurity in order to prevent errors and fatalities caused by cyberattacks.

Legal challenges in relation to Pilot 2:

- ensuring protection of workers' personal data and algorithmic transparency in order to prevent adverse effects of AI use on workers,
- ensuring the right to privacy when processing workers' health data,
- ensuring cybersecurity in order to prevent errors and fatalities caused by cyberattacks,
- providing wearable electronics coherent with essential health and safety requirements,
- liability for errors caused by AI (e.g. in the case of poor navigation decisions during evacuations).

Legal challenges in relation to Pilot 3:

- challenges concerning data protection for connected cars, data retention, purpose limitation and safe handling of sensitive information,
- ensuring safe and secure way of software updates.

Within the activities aimed at establishing connection with regulatory bodies and authorities, special attention was also paid to reaching out to those involved in personal data protection, artificial intelligence and cybersecurity. A list of those regulatory bodies is presented in Table 7.

Table 7 A list of regulatory bodies and authorities contacted for legal guidance in personal data protection, cybersecurity and artificial intelligence

Regulatory body/authority	Name and Surname	Competences related to the ASSIST-IoT pursuits
European Data Protection Supervisor Rue Montoyer 30, B-1000 Brussels Belgium	Wojciech Wiewiórowski European Data Protection Supervisor	Personal data protection
European Union Agency for Cybersecurity Agamemnonos 14, Chalandri 15231, Attiki, Greece	Jean Baptiste Demaison Chair of the Management Board	Cybersecurity

Regulatory body/authority	Name and Surname	Competences related to the ASSIST-IoT pursuits
Directorate-General for Communications Networks, Content and Technology European Commission 1049 Bruxelles/Brussel Belgium	Roberto Viola DIRECTOR-GENERAL	Digital economy and society Research and innovation Business and industry Culture and media

Legal challenges in relation to personal data protection, cybersecurity and artificial intelligence:

- preventing the lack of transparency, excessive data collection (including behavioural data), data retention, lack of user control over data, lack of purpose limitation, and collection or inference of sensitive information,
- avoiding incidental findings of driver's personal data while interchanging data with external trucks,
- ensuring protection of workers' personal data and algorithmic transparency in order to prevent adverse effects of AI use on workers, as well as the right to privacy when processing workers' health data.
- ensuring the security of workers' personal data in order to prevent the data leakage that may lead to adverse effects on workers,
- preventing errors and fatalities caused by cyberattacks, especially in the case of fully automated decision-making,
- preventing false AI predictions due to cyberattacks manipulating the learning system and/or data,
- liability for errors caused by AI (e.g. in the case of poor navigation decisions during evacuations).

Moreover, the above mentioned challenges have been also addressed to national regulatory bodies and authorities. A list of national regulatory bodies is in Table 8.

Table 8 A list of national regulatory bodies and authorities

Regulatory body/authority	Country	Topic
Commission Nationale de l'Informatique et des Libertés	France	Data privacy
Agence Nationale de la Sécurité des Systèmes d'Information	France	Data security
Agencia Española de Protección de datos	Spain	Data protection
Hellenic Data Protection Authority	Greece	Personal Data Protection
Hellenic Institute for Occupational Health and Safety	Greece	OSH
Personal Data Protection Office	Poland	Personal Data Protection
Cyber Security Department, Digital Affairs – Chancellery of the Prime Minister	Poland	Cybersecurity
Office of the Data Protection Ombudsman	Finland	Personal Data Protection
Dutch Data Protection Authority	Netherlands	Personal Data Protection
Federal Commissioner for Data Protection and Freedom of Information	Germany	Personal Data Protection

Regulatory body/authority	Country	Topic
Office of the Information and Data Protection Commissioner	Malta	Personal Data Protection

7 Conclusions

This deliverable contains the legal and regulatory constraints analysis and specification with a special focus on pilot domains, as well as aspects of personal data protection, privacy, cybersecurity especially while using AI technologies. Those aspects are common for all ASSIST-IoT pursuits.

Based on the analysis performed for the deliverable, some general conclusions can be formulated:

- There are plenty of regulations, mainly at the European level, that should be considered within the ASSIST-IoT. However, most of them are well known and practiced among the partners according to the competences.
- ASSIST-IoT pursuits will create some legal challenges that are mainly related to the use of Artificial Intelligence in relation to safety and security, as well as privacy and requirements of GDPR.
- Reliability and validity of the datasets used for training purposes are crucial in terms of ensuring safety in the deployment of the ASSIST-IoT AI-based algorithms.
- Cybersecurity vulnerabilities may become a potential cause of incorrect decisions made by an infected AI-based algorithms. Adoption of the DevSecOps methodology in the ASSIST-IoT project is an appropriate measure to prevent this.
- AI-based algorithms transparency is one of the biggest challenges in terms of meeting GDPR requirements. Providing users with an oversight over how their personal data are used (e.g. during trainings or workshops) may be a key factor in technology acceptance.

It is expected that this report will be a valuable tool for developers in meeting specific pilot-oriented requirements. Deliverable 3.4 finalises activities performed within Task 3.4.

References

- [1] S. Gerke, T. Minssen, and G. Cohen, “Ethical and legal challenges of artificial intelligence-driven healthcare,” 2020, doi: 10.1016/B978-0-12-818438-7.00012-5.
- [2] S. Gerke, T. Minssen, H. Yu, and I. G. Cohen, “Ethical and legal issues of ingestible electronic sensors,” *Nat. Electron.* 2019 28, vol. 2, no. 8, pp. 329–334, Aug. 2019, doi: 10.1038/s41928-019-0290-6.
- [3] L. Gluyas and S. Day, “Who is liable when AI fails to perform?,” *C. Cameron McKenna Nabarro Olswang LLP*, p. 2, 2018, [Online]. Available: <https://cms.law/en/gbr/publication/artificial-intelligence-who-is-liable-when-ai-fails-to-perform>.
- [4] R. Rodrigues, “Legal and human rights issues of AI: Gaps, challenges and vulnerabilities,” *J. Responsible Technol.*, vol. 4, p. 100005, Dec. 2020, doi: 10.1016/J.JRT.2020.100005.
- [5] S. Wachter and B. Mittelstadt, “A Right to Reasonable Inferences,” *Columbia Bus. Law Rev.*, vol. 2019, no. 2, pp. 494–620–494–620, May 2019, doi: 10.7916/CBLR.V2019I2.3424.
- [6] M. J. Rigby, “Ethical dimensions of using artificial intelligence in health care,” *AMA J. Ethics*, vol. 21, no. 2, pp. 121–124, Feb. 2019, doi: 10.1001/AMAJETHICS.2019.121.
- [7] E. Vayena, A. Blasimme, and I. G. Cohen, “Machine learning in medicine: Addressing ethical challenges,” *PLOS Med.*, vol. 15, no. 11, p. e1002689, Nov. 2018, doi: 10.1371/JOURNAL.PMED.1002689.
- [8] M. Comiter, “Attacking Artificial Intelligence AI’s Security Vulnerability and What Policymakers Can Do About It,” 2019, Accessed: Oct. 24, 2021. [Online]. Available: www.belfercenter.org.
- [9] O. Rachum-Twaig, “Whose Robot Is It Anyway?: Liability for Artificial-Intelligence-Based Robots.” Feb. 21, 2019, Accessed: Oct. 24, 2021. [Online]. Available: <https://papers.ssrn.com/abstract=3339230>.
- [10] “REPORT ON THE SAFETY AND LIABILITY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE, THE INTERNET OF THINGS AND ROBOTICS,” doi: 10.1787/ab757416-en.
- [11] D. FW and A. D, “The Convention on Human Rights and Biomedicine of the Council of Europe,” *Kennedy Inst. Ethics J.*, vol. 7, no. 3, pp. 259–276, 1997, doi: 10.1353/KEN.1997.0023.
- [12] “Research Ethics Service and Research Ethics Committees - Health Research Authority.” <https://www.hra.nhs.uk/about-us/committees-and-services/res-and-recs/> (accessed Oct. 24, 2021).
- [13] “REGULATION (EU) No 1291/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC.”.
- [14] “Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications | European Data Protection Board.” https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-12020-processing-personal-data_en (accessed Oct. 24, 2021).
- [15] European Data Protection Supervisor., “EDPS TechDispatch : connected cars. Issue 3, 2019.”

A Official letters

European Union Agency for Cybersecurity**Agamemnonos 14,****Chalandri 15231, Attiki, Greece**

I am writing in relation to the EU-funded ASSIST-IoT project (GA no. 957258, project website: <https://assist-iot.eu/>). The project aims at designing, implementing and validating of an open, decentralised reference architecture, associated enablers, services and tools, for assisting human-centric applications in multiple verticals. The ASSIST-IoT solutions will be validated in three pilot domains, namely: (1) port automation, (2) smart safety of workers, (3) cohesive vehicle monitoring and diagnostics. While implementing the project, we would like to make sure that ASSIST-IoT pursuits are compliant with the existing and upcoming legal regulations, especially in the abovementioned pilot domains. With your expertise in mind, we kindly request your support and involvement in providing us with legal advice and guidance on the ASSIST-IoT project.

The main identified legal concerns are related to the use of NGIoT architecture and AI-based technologies for the purpose of:

- tracking of assets in terminal yard, automated operation of container handling equipment (including rubber-tired gantry (RTG)-truck identification, authentication and alignment) and RTG remote control with augmented reality support – pilot 1,
- prevention from dangerous work-related situations at the construction site (including safe navigation in the case of evacuation) and provision of relevant safety-related information to OSH inspectors, integration of smart devices with personal protective equipment in order to monitor individual exposures, as well as monitoring of physiological parameters and tracking the location of workers to detect anomalies and provide necessary first aid – pilot 2,
- fleet in-service emissions verification, vehicle diagnostics (i.e. non-conformance causes identification) and vehicle exterior conditions inspection and documentation – pilot 3.

Particular legal issues that draw our attention in connection with the above mentioned scope of pilots include:

- preventing errors and fatalities caused by cyberattacks, especially in the case of fully automated decision-making,
- ensuring the security of workers' personal data in order to prevent the data leakage that may lead to adverse effects on workers,
- preventing false AI predictions due to cyberattacks manipulating the learning system and/or data.

Accordingly, in relation to the scope of our pilots, we have identified the following regulations as the most important for the ASSIST-IoT pursuits in relation to personal data protection, privacy and cybersecurity:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and

communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

- 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

We would be very grateful if you could indicate whether any additional legal aspects or upcoming EU regulations should be taken into account during the ASSIST-IoT project. We would appreciate your response within 2 weeks of receiving this letter.

Yours faithfully,

On October 29th, 2021, at Valencia, Spain

Prof. Dr. **Carlos E. PALAU-SALVADOR**
ASSIST-IoT Project Coordinator

Dear Mr Wojciech Wiewiórowski
European Data Protection Supervisor
Rue Montoyer 30,
B-1000 Brussels, Belgium

I am writing in relation to the EU-funded ASSIST-IoT project (GA no. 957258, project website: <https://assist-iot.eu/>). The project aims at designing, implementing and validating of an open, decentralised reference architecture, associated enablers, services and tools, for assisting human-centric applications in multiple verticals. The ASSIST-IoT solutions will be validated in three pilot domains, namely: (1) port automation, (2) smart safety of workers, (3) cohesive vehicle monitoring and diagnostics. While implementing the project, we would like to make sure that ASSIST-IoT pursuits are compliant with the existing and upcoming legal regulations, especially in the abovementioned pilot domains. With your expertise in mind, we kindly request your support and involvement in providing us with legal advice and guidance on the ASSIST-IoT project.

The main identified legal concerns are related to the use of NGIoT architecture and AI-based technologies for the purpose of:

- tracking of assets in terminal yard, automated operation of container handling equipment (including rubber-tired gantry (RTG)-truck identification, authentication and alignment) and RTG remote control with augmented reality support – pilot 1,
- prevention from dangerous work-related situations at the construction site (including safe navigation in the case of evacuation) and provision of relevant safety-related information to OSH inspectors, integration of smart devices with personal protective equipment in order to monitor individual exposures, as well as monitoring of physiological parameters and tracking the location of workers to detect anomalies and provide necessary first aid – pilot 2,
- fleet in-service emissions verification, vehicle diagnostics (i.e. non-conformance causes identification) and vehicle exterior conditions inspection and documentation – pilot 3.

Particular legal issues that draw our attention in connection with the above mentioned scope of pilots include:

- preventing the lack of transparency, excessive data collection (including behavioural data), data retention, lack of user control over data, lack of purpose limitation, and collection or inference of sensitive information,
- avoiding incidental findings of driver's personal data while interchanging data with external trucks,
- ensuring protection of workers' personal data and algorithmic transparency in order to prevent adverse effects of AI use on workers, as well as the right to privacy when processing workers' health data.

Accordingly, in relation to the scope of our pilots, we have identified the following regulations as the most important for the ASSIST-IoT pursuits in relation to personal data protection, privacy and cybersecurity:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
- 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

We would be very grateful if you could indicate whether any additional legal aspects or upcoming EU regulations should be taken into account during the ASSIST-IoT project. We would appreciate your response within 2 weeks of receiving this letter.

Yours faithfully,

On October 29th, 2021, at Valencia, Spain

Prof. Dr. **Carlos E. PALAU-SALVADOR**
ASSIST-IoT Project Coordinator

Dear Ms Vitcheva

DIRECTOR-GENERAL

Directorate-General for Maritime Affairs and Fisheries

European Commission

1049 Bruxelles/Brussel

Belgium

I am writing in relation to the EU-funded ASSIST-IoT project (GA no. 957258, project website: <https://assist-iot.eu/>). The project aims at designing, implementing and validating of an open, decentralised reference architecture, associated enablers, services and tools, for assisting human-centric applications in multiple verticals. The ASSIST-IoT solutions will be validated in three pilot domains, namely: (1) port automation, (2) smart safety of workers, (3) cohesive vehicle monitoring and diagnostics. While implementing the project, we would like to make sure that ASSIST-IoT pursuits are compliant with the existing and upcoming legal regulations, especially in the abovementioned pilot domains. With your expertise in mind, we kindly request your support and involvement in providing us with legal advice and guidance on the ASSIST-IoT project.

For the port automation pilot, the main identified legal concerns are related to the use of NGIoT architecture and AI-based technologies for the purpose of tracking assets in terminal yard, automated container handling equipment operation (including rubber-tired gantry (RTG)-truck identification, authentication and alignment) and RTG remote control with augmented reality support. Particular legal issues that draw our attention in connection with the port automation pilot include:

- avoiding incidental findings of driver's personal data while interchanging data with external trucks,
- ensuring meeting safety requirements of machines during remote control taking into account the latency,
- ensuring cybersecurity in order to prevent errors and fatalities caused by cyberattacks.

Accordingly, in relation to the scope of port automation pilot, we have identified the following regulations as the most important for the ASSIST-IoT pursuits:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
- 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
- Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

We would be very grateful if you could indicate whether any additional legal aspects or upcoming EU regulations should be taken into account during the ASSIST-IoT project. We would appreciate your response within 2 weeks of receiving this letter.

Yours faithfully,

On October 29th, 2021, at Valencia, Spain

Prof. Dr. Carlos E. PALAU-SALVADOR
ASSIST-IoT Project Coordinator

Dear Mr Korte

DIRECTOR-GENERAL

Directorate-General for Employment, Social Affairs and Inclusion

European Commission

1049 Bruxelles/Brussel

Belgium

I am writing in relation to the EU-funded ASSIST-IoT project (GA no. 957258, project website: <https://assist-iot.eu/>). The project aims at designing, implementing and validating of an open, decentralised reference architecture, associated enablers, services and tools, for assisting human-centric applications in multiple verticals. The ASSIST-IoT solutions will be validated in three pilot domains, namely: (1) port automation, (2) smart safety of workers, (3) cohesive vehicle monitoring and diagnostics. While implementing the project, we would like to make sure that ASSIST-IoT pursuits are compliant with the existing and upcoming legal regulations, especially in the abovementioned pilot domains. With your expertise in mind, we kindly request your support and involvement in providing us with legal advice and guidance on the ASSIST-IoT project.

For the smart safety of workers pilot, the main identified legal concerns are related to the use of NGIoT architecture and AI-based technologies for the purpose of prevention from dangerous work-related situations at the construction site (including safe navigation in the case of evacuation) and provision of relevant safety-related information to OSH inspectors, integration of smart devices with personal protective equipment in order to monitor individual exposures, as well as monitoring of physiological parameters and tracking the location of workers to detect anomalies and provide necessary first aid. Particular legal issues that draw our attention in connection with the smart safety of workers pilot include:

- ensuring protection of workers' personal data and algorithmic transparency in order to prevent adverse effects of AI use on workers,
- ensuring the right to privacy when processing workers' health data,
- ensuring cybersecurity in order to prevent errors and fatalities caused by cyberattacks,
- providing wearable electronics coherent with essential health and safety requirements,
- liability for errors caused by AI (e.g. in the case of poor navigation decisions during evacuations).

Accordingly, in relation to the scope of smart safety of workers pilot, we have identified the following regulations as the most important for the ASSIST-IoT pursuits:

- in relation to personal data protection, privacy and cybersecurity:
 - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
 - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
- 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
- in relation to occupational safety and health:
 - Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work
 - Council Directive 89/656/EEC of 30 November 1989 on the minimum health and safety requirements for the use by workers of personal protective equipment at the workplace (third individual directive within the meaning of Article 16 (1) of Directive 89/391/EEC)
 - Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC
 - Council Directive 89/654/EEC of 30 November 1989 concerning the minimum safety and health requirements for the workplace (first individual directive within the meaning of Article 16(1) of Directive 89/391/EEC)
 - Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)
 - Directive 2013/35/EU of the European Parliament and of the Council of 26 June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (20th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) and repealing Directive 2004/40/EC
- in relation to machinery and electrical devices:
 - Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC
 - Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits
 - Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility
 - Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the member states relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
 - Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC



UNIVERSITAT
POLITÀCNICA
DE VALÈNCIA

We would be very grateful if you could indicate whether any additional legal aspects or upcoming EU regulations should be taken into account during the ASSIST-IoT project. We would appreciate your response within 2 weeks of receiving this letter.

Yours faithfully,

On October 29th, 2021, at Valencia, Spain

Prof. Dr. **Carlos E. PALAU-SALVADOR**
ASSIST-IoT Project Coordinator

Dear Mr Henrik Hololei
DIRECTOR-GENERAL
Directorate-General for Mobility and Transport
European Commission
1049 Brussels
Belgium

I am writing in relation to the EU-funded ASSIST-IoT project (GA no. 957258, project website: <https://assist-iot.eu/>). The project aims at designing, implementing and validating of an open, decentralised reference architecture, associated enablers, services and tools, for assisting human-centric applications in multiple verticals. The ASSIST-IoT solutions will be validated in three pilot domains, namely: (1) port automation, (2) smart safety of workers, (3) cohesive vehicle monitoring and diagnostics. While implementing the project, we would like to make sure that ASSIST-IoT pursuits are compliant with the existing and upcoming legal regulations, especially in the abovementioned pilot domains. With your expertise in mind, we kindly request your support and involvement in providing us with legal advice and guidance on the ASSIST-IoT project.

For the cohesive vehicle monitoring and diagnostics pilot, the main identified legal concerns are related to the use of NGIoT architecture and AI-based technologies for the purpose of fleet in-service emissions verification, vehicle diagnostics (i.e. non-conformance causes identification) and vehicle exterior conditions inspection and documentation. Particular legal issues that draw our attention in connection with the cohesive vehicle monitoring and diagnostics pilot include:

- challenges concerning data protection for connected cars, data retention, purpose limitation and safe handling of sensitive information
- ensuring safe and secure way of software updates.

Accordingly, in relation to the scope of the cohesive vehicle monitoring and diagnostics pilot, we have identified the following regulations as the most important for the ASSIST-IoT pursuits:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
- 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
- Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information
- Commission Regulation (EU) 2017/1151 of 1 June 2017 supplementing Regulation (EC) No 715/2007 of the European Parliament and of the Council on type-approval of motor vehicles

with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, amending Directive 2007/46/EC of the European Parliament and of the Council, Commission Regulation (EC) No 692/2008 and Commission Regulation (EU) No 1230/2012 and repealing Commission Regulation (EC) No 692/2008

- Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC
- Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166

We would be very grateful if you could indicate whether any additional legal aspects or upcoming EU regulations should be taken into account during the ASSIST-IoT project. We would appreciate your response within 2 weeks of receiving this letter.

Yours faithfully,

On October 29th, 2021, at Valencia, Spain

Prof. Dr. **Carlos E. PALAU-SALVADOR**
ASSIST-IoT Project Coordinator

Dear Ms Florika Fink-Hooijer

DIRECTOR-GENERAL

Directorate-General for Environment

European Commission

1049 Bruxelles/Brussel

Belgium

I am writing in relation to the EU-funded ASSIST-IoT project (GA no. 957258, project website: <https://assist-iot.eu/>). The project aims at designing, implementing and validating of an open, decentralised reference architecture, associated enablers, services and tools, for assisting human-centric applications in multiple verticals. The ASSIST-IoT solutions will be validated in three pilot domains, namely: (1) port automation, (2) smart safety of workers, (3) cohesive vehicle monitoring and diagnostics. While implementing the project, we would like to make sure that ASSIST-IoT pursuits are compliant with the existing and upcoming legal regulations, especially in the abovementioned pilot domains. With your expertise in mind, we kindly request your support and involvement in providing us with legal advice and guidance on the ASSIST-IoT project.

For the cohesive vehicle monitoring and diagnostics pilot, the main identified legal concerns are related to the use of NGIoT architecture and AI-based technologies for the purpose of fleet in-service emissions verification, vehicle diagnostics (i.e. non-conformance causes identification) and vehicle exterior conditions inspection and documentation. Particular legal issues that draw our attention in connection with cohesive vehicle monitoring and diagnostics pilot include:

- challenges concerning data protection for connected cars, data retention, purpose limitation and safe handling of sensitive information
- ensuring safe and secure way of software updates.

Accordingly, in relation to the scope of cohesive vehicle monitoring and diagnostics pilot, we have identified the following regulations as the most important for the ASSIST-IoT pursuits:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
- 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
- Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information
- Commission Regulation (EU) 2017/1151 of 1 June 2017 supplementing Regulation (EC) No 715/2007 of the European Parliament and of the Council on type-approval of motor vehicles

with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, amending Directive 2007/46/EC of the European Parliament and of the Council, Commission Regulation (EC) No 692/2008 and Commission Regulation (EU) No 1230/2012 and repealing Commission Regulation (EC) No 692/2008

- Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC
- Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166

We would be very grateful if you could indicate whether any additional legal aspects or upcoming EU regulations should be taken into account during the ASSIST-IoT project. We would appreciate your response within 2 weeks of receiving this letter.

Yours faithfully,

On October 29th, 2021, at Valencia, Spain

Prof. Dr. **Carlos E. PALAU-SALVADOR**
ASSIST-IoT Project Coordinator

Dear Ms Kerstin Jorna

DIRECTOR-GENERAL

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

European Commission

1049 Bruxelles/Brussel

Belgium

I am writing in relation to the EU-funded ASSIST-IoT project (GA no. 957258, project website: <https://assist-iot.eu/>). The project aims at designing, implementing and validating of an open, decentralised reference architecture, associated enablers, services and tools, for assisting human-centric applications in multiple verticals. The ASSIST-IoT solutions will be validated in three pilot domains, namely: (1) port automation, (2) smart safety of workers, (3) cohesive vehicle monitoring and diagnostics. While implementing the project, we would like to make sure that ASSIST-IoT pursuits are compliant with the existing and upcoming legal regulations, especially in the abovementioned pilot domains. With your expertise in mind, we kindly request your support and involvement in providing us with legal advice and guidance on the ASSIST-IoT project.

The main identified legal concerns are related to the use of NGIoT architecture and AI-based technologies for the purpose of:

- tracking of assets in terminal yard, automated operation of container handling equipment (including rubber-tired gantry (RTG)-truck identification, authentication and alignment) and RTG remote control with augmented reality support – pilot 1: port automation,
- prevention from dangerous work-related situations at the construction site (including safe navigation in the case of evacuation) and provision of relevant safety-related information to OSH inspectors, integration of smart devices with personal protective equipment in order to monitor individual exposures, as well as monitoring of physiological parameters and tracking the location of workers to detect anomalies and provide necessary first aid – pilot 2: smart safety of workers,
- fleet in-service emissions verification, vehicle diagnostics (i.e. non-conformance causes identification) and vehicle exterior conditions inspection and documentation – pilot 3: cohesive vehicle monitoring and diagnosis.

Particular legal issues that draw our attention in relation to above mentioned scope of pilots include:

- regarding privacy and personal data protection:
 - avoiding incidental findings of driver's personal data while interchanging data with external trucks,
 - ensuring protection of workers' personal data and algorithmic transparency in order to prevent from the adverse effects of a use of AI on workers, as well as right to privacy while processing workers' health data,
 - challenges concerning data protection for connected cars, data retention, purpose limitation and safe handling of sensitive information,
- ensuring cybersecurity in order to prevent errors and fatalities caused by cyberattacks.
- meeting safety and security requirements for:
 - machines during remote control taking into account the latency,
 - wearable electronics at work environment,
 - software updates in connected cars.

- liability for errors caused by AI (e.g., in the case of wrong decisions in navigation during the evacuation).

Accordingly, in relation to the scope of our pilots, we have identified the following regulations as the most important for the ASSIST-IoT pursuits:

- in relation to personal data protection, privacy and cybersecurity:
 - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),
 - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications),
 - Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013,
 - 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,
- in relation to occupational safety and health:
 - Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work,
 - Council Directive 89/656/EEC of 30 November 1989 on the minimum health and safety requirements for the use by workers of personal protective equipment at the workplace (third individual directive within the meaning of Article 16 (1) of Directive 89/391/EEC),
 - Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC
 - Council Directive 89/654/EEC of 30 November 1989 concerning the minimum safety and health requirements for the workplace (first individual directive within the meaning of Article 16(1) of Directive 89/391/EEC),
 - Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC),
 - Directive 2013/35/EU of the European Parliament and of the Council of 26 June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (20th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) and repealing Directive 2004/40/EC,

- in relation to machinery and electrical devices:
 - Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC,
 - Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of laws of Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits,
 - Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility,
 - Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the member states relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC,
 - Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC,
- in relation to motor vehicles and emissions:
 - Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information,
 - Commission Regulation (EU) 2017/1151 of 1 June 2017 supplementing Regulation (EC) No 715/2007 of the European Parliament and of the Council on type-approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, amending Directive 2007/46/EC of the European Parliament and of the Council, Commission Regulation (EC) No 692/2008 and Commission Regulation (EU) No 1230/2012 and repealing Commission Regulation (EC) No 692/2008,
 - Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC,
 - Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166.



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

We would be very grateful if you could indicate whether any additional legal aspects or upcoming EU regulations should be taken into account during the ASSIST-IoT project. We would appreciate your response within 2 weeks of receiving this letter.

Yours faithfully,

On October 29th, 2021, at Valencia, Spain

Prof. Dr. Carlos E. PALAU-SALVADOR
ASSIST-IoT Project Coordinator