

interiot

INTEROPERABILITY
OF HETEROGENEOUS
IOT PLATFORMS.

D2.5

Legal and regulatory requirements analysis
and specification

December 2016

INTER-IoT

INTER-IoT aim is to design, implement and test a framework that will allow interoperability among different Internet of Things (IoT) platforms.

Most current existing IoT developments are based on “closed-loop” concepts, focusing on a specific purpose and being isolated from the rest of the world. Integration between heterogeneous elements is usually done at device or network level, and is just limited to data gathering. Our belief is that a multi-layered approach integrating different IoT devices, networks, platforms, services and applications will allow a global continuum of data, infrastructures and services that will enhance different IoT scenarios. Moreover, reuse and integration of existing and future IoT systems will be facilitated, creating a de facto global ecosystem of interoperable IoT platforms.

In the absence of global IoT standards, the INTER-IoT results will allow any company to design and develop new IoT devices or services, leveraging on the existing ecosystem, and bring them to market as fast as possible.

INTER-IoT has been financed by the Horizon 2020 initiative of the European Commission, contract 687283.

INTER-IoT

Legal and regulatory requirements analysis and specification

Version: Final

Security: Public

December 29. 2016

The INTER-IoT project has been financed by the Horizon 2020 initiative of the European Commission, contract 687283



Disclaimer

This document contains material, which is the copyright of certain INTER-IoT consortium parties, and may not be reproduced or copied without permission.

The information contained in this document is the proprietary confidential information of the INTER-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.

Executive Summary

The aim of the legal and regulatory requirements documentation is to provide an analysis of the legislation needed for the design and implementation of the different products of INTER-IoT¹, defined in the proposal: INTER-LAYER, INTER-FW, INTER-METH, INTER-LogP, and INTER-Health.

The document was created using inputs from regulatory bodies as well as data protection authorities at a national and the EU level to ensure the involvement of authorities for legal guidance for the project. In particular, we have approached national data protection authorities, national ministries, and cloud focused task forces and other bodies associated with the European Commission.

This deliverable groups all the identified legal decisions, directives and acts that are going to be taken into consideration when approaching the design of the INTER-IoT solutions. The consortium have analysed the legal constraints at a European level and the national laws that have transposed the national legislation. It should be borne in mind that the use of a Directive obliges national legislative bodies to transpose the provisions in question into their own national legislation. Therefore, each partner has carried out and in depth research in its Member State to identify the specific legal constraints at a national level. This work has been done with the guidance of national regulators and other legal authorities.

On the other hand, this deliverable includes the legal and regulatory constraints for the different application domains of port transport and logistics and mobile health. In particular, port logistics laws and regulations are being presented as well as several legal conditions for medical devices, certification and control procedures intended to verify that the medical devices offer patients, users, and third parties, a high level of protection and that they attain the performances assigned to them by their manufacturer and they set a distinction between a device itself and its accessory or accessories.

Finally, the INTER-IoT consortium members have decided to include different IoT good practices and recommendations from European organisations such as the IoT EPI, AIOTI or the European Research Cluster (IERC) on the Internet of Things.

¹ <http://www.inter-iot.eu>

List of Authors

Organisation	Authors	Main organisations' contributions
VPF	Miguel Llop, Pablo Giménez, Alexandre Sánchez, M ^a Luisa Escamilla, Eduardo Olmeda	Initial version Methodology National regulations Conclusion Quality review
NOATUM	Francisco Blanquer	Transport and logistic regulations
AFT	Moncef Semichi, Sarah Koneke, Kimvy Bui	European regulations
ASL TO 5	Margherita Gulino, Claudio Maggi, Angelina Della Torre, Domenica Pata, Monica Minutolo, Anna Aldrighetti, Bartolomeo Avataneo	Health regulations
UPV	Carlos E. Palau, Eneko Olivares, Regel González	Contribution to national and European regulations Final review and editing
All		Search national regulations

Change control datasheet

Version	Changes	Chapters	Pages
0.1	Creation, index and introduction	All	16
0.2	Methodology	2	19
0.3	European directives	3	26
0.4	National regulations	3	37
0.5	Transport and logistic regulation	3	43
0.6	Health regulations	3	47
0.7	Good practices	4	56
0.8	Conclusions	5	57
1.0	Final version	All	59
1.1	Internal review 1	All	59
1.2	Internal review 2	All	59
1.3	Final version to upload	All	68

Contents

- Executive Summary 3
- List of Authors 4
- Change control datasheet 5
- Contents..... 6
- List of Figures..... 7
- List of Tables..... 7
- Acronyms 8
- 1 Introduction 9
 - 1.1 Internet of Things 9
 - 1.2 IoT interoperability.....10
 - 1.3 Scope of the INTER-IoT project12
 - 1.4 Scope of the document15
- 2 Methodology.....17
 - 2.1 Identification17
- 3 Legal aspects in interoperability and IoT20
 - 3.1 European legislation.....20
 - 3.2 Legislation in the countries of the project.....28
- 4 Legislation in application domains43
 - 4.1 Transport and port logistics43
 - 4.2 eHealth.....49
- 5 IoT good practices and recommendations53
 - 5.1 Digital Single Market (DSM) of European Union.....53
 - 5.2 Article 29 Data Protection Working Party.....53
 - 5.3 Alliance for Internet of Things Innovation (AIOTI)54
 - 5.4 IERC-European Research Cluster on the Internet of Things56
 - 5.5 IoT European Platform Initiative (IoT-EPI)58
 - 5.6 ENISA59
 - 5.7 The European GNSS Agency.....60
 - 5.8 The European Telecommunications Standards Institute (ETSI)62
 - 5.9 OneM2M63
 - 5.10 ISO - International Organization for Standardization.....64
- 6 Conclusions.....65

List of Figures

Figure 1: IoT Installed Base and Revenues in EU 28 2013-2018.....10

Figure 2: INTER-IoT approach abstract schema.....13

Figure 3: Abstract schema of the INTER-FW.....14

Figure 4. IoT Legal Framework [Source: Valenciaport Foundation]18

Figure 5: Working Groups AIOTI55

Figure 6: Innovation IoT projects H202058

List of Tables

Table 1. Example of regulation19

Table 2. International Legislation.....21

Table 3. International Legislation on Logistics and Transport44

Table 4. National Legislation on eHealth51

Table 5. WP29 last publications54

Table 6. AIOTI and EC last publications56

Table 7. IERC last publications.....57

Table 8. ENISA last publications60

Table 9. GSA last publications.....61

Table 10. Latest published ETSI standards on internet of things62

Acronyms

AIOTI	Alliance for Internet of Things Innovation
BIP	Best Ideas and Projects
EC	European Commission
IERC	European Research Cluster on the Internet of Things
INTER-LAYER	INTER-IoT Layer integration tools
INTER-FW	INTER-IoT Interoperable IoT Framework
INTER-METH	INTER-IoT Engineering Methodology
INTER-LogP	INTER-IoT Platform for Transport and Logistics
INTER-Health	INTER-IoT Platform for Health monitoring
INTER-META-ARCH	INTER-IoT Architectural meta-model for IoT interoperable platforms
INTER-META-DATA	INTER-IoT Metadata-model for IoT interoperable semantics
INTER-API	INTER-IoT Programming library
INTER-CASE	INTER-IoT Computer Aided Software Engineering tool for integration
IoT	Internet of Things
ITU	International Communications Union
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
M2M	Machine to Machine
W3C	World Wide Web Consortium
ETSI	European Telecommunications Standards Institute
DSM	Digital Single Market
AIOTI	Alliance for Internet of Things Innovation
IoT-EPI	IoT European Platform Initiative
ENISA	European Union Agency for Network and Information Security
NIS	network and information security
ICT	Information and Communication Technology

1 Introduction

1.1 Internet of Things

The connection of intelligent devices, equipped with a growing number of electronic sensors and/or actuators, via the Internet, is known as the 'Internet of Things' (IoT). With the IoT, every physical and virtual object can be connected to other objects and to the Internet, creating a fabric of connectivity between things and between humans and things. The IoT is now widely recognised as the next step of disruptive digital innovation.

The International Communications Union (ITU) and the European Research Cluster on the Internet of Things (IERC) provide the following definition: IoT is a dynamic global network infrastructure, with self-configuring capabilities based on standard and interoperable communication protocols, where physical and virtual "things" have identities, physical attributes and virtual personalities and use intelligent interfaces. All of them are seamlessly integrated into the information network.

The design of the Internet and specifically the extension of the Internet to the IoT, rely on the convergence of the infrastructure with software and services. A common practice is required to think/design cross solutions between software and infrastructure in order to provide integrated solutions for some of the complex problems arising in current and future systems. In the IoT environment this convergence is evident, and the continuous evolution generates more and more smart connected objects and platforms that are embedded with sensors and their respective associated services, in some cases considering virtualization.

IoT is the network or overlay associations between smart connected objects (physical and virtual), that are able to exchange information by using an agreed method (including protocols) and a data scheme. As IoT deployments are increasing, there is growing interest in standardisation, alliances and homogenization. All these developments are giving a strong push to the IoT domain to be considered as one of the most promising emerging technologies. As an example, Gartner (one of the world's leading information technology research and advisory company) estimates that the number of web-connected devices will reach 25 billion by 2020. In other words, more devices, appliances, cars, artefacts, and accessories will be connected and will communicate with each other, and with other objects, thus bringing amplified connectivity and better supply chain visibility. The applications of the IoT are numerous i.e. every object could be transformed into a smart object that sends several valuable pieces of information to other devices. As an example, in transportation and logistics in ports, IoT could be applied to shipping containers, container-handling equipment, container trucks, and even, to container ships that move them around the globe.

According to the European Commission (EC), IoT represents the next step towards the digitisation of our society and economy, where objects and people are interconnected through communication networks, and report about their status and/or the surrounding environment. Furthermore, IoT can also benefit the European economy generating economic growth and employment; according to a recent European Commission study revenues in the EU28 will increase from more than €307 billion in 2013 to more than €1,181 billion in 2020 (as shown in Figure 1).

IoT is an emerging area that not only requires development of infrastructure but also deployment of new services capable of supporting multiple, scalable and interoperable applications. Today, the focus is on cloud deployments, virtualizations, and the elimination of silos solutions, thus avoiding the creation of application-domain specific developments, with AIOI and EC pressing in this direction. IoT has evolved from sensor networks and wireless sensor networks to a clearer definition referring to objects and the virtual representations of these objects on the Internet and associated infrastructures. It defines how the physical things and virtual objects will be connected through the Internet and their interaction. It also defines how they communicate with other systems and platforms, in order to expose their capabilities and functionalities in terms of services and accessibility through open APIs and frameworks. IoT is not only linking connected devices through the Internet; it is also web-enabled data exchange in order to enable systems with more capacities to become smart and accessible, creating webs of objects and allowing integration of data, services and components.

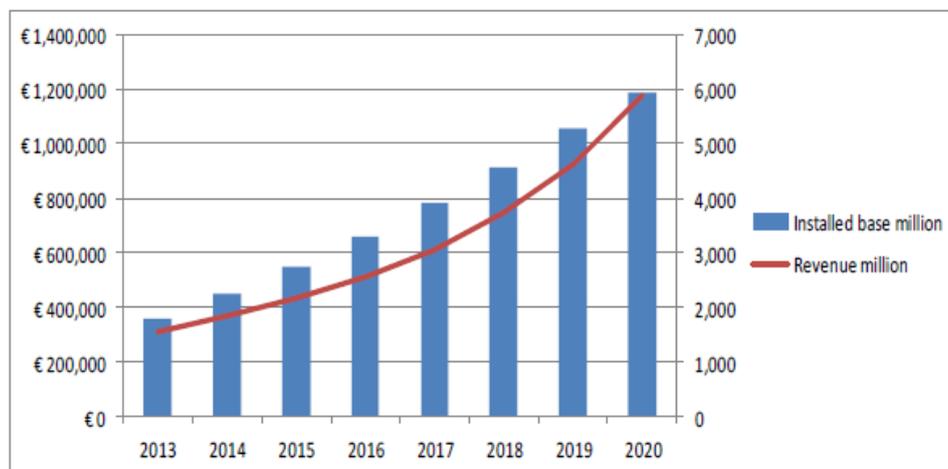


Figure 1: IoT Installed Base and Revenues in EU 28 2013-2018

There are several challenges associated with IoT and its evolution, but one major issue is related with interoperability. IoT is mainly supported by continuous progress in wireless sensor and actuator networks and by manufacturing low cost and energy efficient hardware for sensor and device communications. However, the main challenge for expanding generic IoT solutions to a global scale are the heterogeneity of underlying devices, different communication standards and interoperability issues in various layers. Layer interoperability issues range from communication and seamless integration of devices up to interoperability of data generated by the IoT resources. By addressing these issues, INTER-IoT aims at providing solutions that are application domain agnostic, with the further goals of avoiding technological and application siloes.

1.2 IoT interoperability

Many projects have dealt and/or are dealing with the development of IoT architectures in diversified application domains. However, the conceptual realization of IoT is far from achieving a full deployment of converged IoT services and technology. Widespread development of vertically-oriented closed systems, architectures and application areas has generated a fragmentation that needs to be overcome. The lack of interoperability causes major technological and business issues such as impossibility to plug non-interoperable IoT

devices into heterogeneous IoT platforms, impossibility to develop IoT applications exploiting multiple platforms in homogeneous and/or cross domains, slowness of IoT technology introduction at a large-scale, discouragement in adopting IoT technology, increased cost, scarce reusability of technical solutions and user dissatisfaction. Current research in IoT is focused on providing integrated solutions primarily on the feature that enables convergence or what is known as Interoperability.

Interoperability is a property referring to the ability of systems and organizations to work together. The overall challenge of achieving interoperability of heterogeneous IoT platforms is to deliver an IoT extended into a web of platforms for connected devices and objects. They will support smart environments, businesses, services and people with dynamic and adaptive configuration capabilities. Interoperability of heterogeneous IoT platforms will be the way to achieve the potential benefits derived from a scenario where everything is linked; interoperability between several heterogeneous platforms is of utmost importance.

Interoperability can be generalized as the feature for providing seamless exchange of information to, for example, customize services automatically or simply exchanging information in a way that other systems can use it for improving performance, enabling and creating services, controlling operations and processing information. This type of scenarios requires increased interoperability in service management operations. The INTER-IoT project, aware of this fact, aims to provide an interoperable open IoT framework (with associated engineering tools and methodology) for seamless integration of heterogeneous IoT platforms available in the same or different application domains.

INTER-IoT will provide all the building blocks needed to achieve interoperability, including a framework, methodology and associated APIs and tool-boxes. Ensuring that interoperability will be kept as the different products and architectures may evolve in the market. The benefits of INTER-IoT will be:

- At the **device level**, seamless inclusion of novel IoT devices and their interoperation with already existing, even heterogeneous ones. This will allow fast growth of smart objects ecosystems.
- At the **networking level**, seamless support for smart objects mobility and information routing. This will allow design and implementation of fully connected ecosystems.
- At the **middleware level**, seamless service discovery and management system for smart objects and their basic services. This will allow global exploitation of smart objects in large (even extreme) scale (multi-platform) IoT systems.
- At the **application service level**, reuse and exchange (import/export) of heterogeneous services between different IoT platforms.
- At the **data and semantics level**, common interpretation of data and information based on global shared ontology in order to achieve semantic interoperability.
- At the **integrated IoT platform level**, rapid prototyping of cross-platform IoT applications.
- At the **business level**, faster introduction of IoT technology and applications across multiple application domains.

By using the aforementioned approach, IoT platform heterogeneity will be turned from a crucial problem to a great advantage, as there will be no need to wait for a unique standard for an

interoperable IoT. Instead, interoperable IoT, even on a very large scale, will be created through a bottom-up approach.

1.3 Scope of the INTER-IoT project

INTER-IoT project aims at the design, implementation and experimentation of an open cross-layer framework, an associated methodology and tools to enable voluntary interoperability among heterogeneous Internet of Things (IoT) platforms. The proposal will allow effective and efficient development of adaptive, smart IoT applications and services, atop different heterogeneous IoT platforms, spanning single and/or multiple application domains. The project and associated approach has been defined to be use case-driven. Thus, it will be implemented and tested in three realistic large-scale pilots:

- Port of Valencia transportation and logistics involving heterogeneous platforms with ~400 smart objects.
- An Italian National Health Centre for mobile health involving ~200 patients, equipped with body sensor networks, wearable sensors and mobile smart devices.
- A cross-domain pilot involving IoT platforms from both application domains will be deployed and tested in the premises of the Port of Valencia.

Furthermore, the project will analyse usability of the provided solutions from the perspective of IoT platform creators, IoT platform owners, IoT application programmers and users investigating business perspectives and creating new business models. The most important benefits expected for third parties are related with the new features and components that will be released by the consortium: Methodologies, tools, protocols and APIs that will be released as open items available to develop new applications and services. The variety and cross availability of the results could be used to build and integrate services and platforms at different layers according to the needs of the stakeholders and developers. The availability of more and new data will stimulate the creation of new opportunities and products, always in the scope of open interoperability.

Open interoperability relies on the promise of enabling vendors and developers to interact and interoperate, without interfering with anyone's ability to compete by delivering a superior product and experience. In the absence of global IoT standards, INTER-IoT will support and make it easy for companies to design IoT devices, smart objects, or services, thus drastically decreasing time to market. With this approach, we create new IoT interoperable ecosystems.

The INTER-IoT approach is general-purpose and may be applied to any application domain and across domains in which there is a need to interconnect IoT systems already deployed or add new ones. INTER-IoT will be based on three main building blocks:

- Methods and tools for providing interoperability among and across layers of IoT platforms (INTER-LAYER);
- Global framework (INTER-FW) for programming and managing interoperable IoT platforms; and
- Engineering Methodology (INTER-METH) based on a CASE tool for IoT platforms integration and interconnection.

Project results will be specifically tested in the two independent application domains that will lead to two independent products, namely: INTER-LogP and INTER-Health. Thus, as an outcome of the project, INTER-IoT will provide five products that could be introduced in the market for a wider implementation and exploitation. The market analysis and stakeholders will be based in the existence of these five products, and the interest generated by the stakeholders.

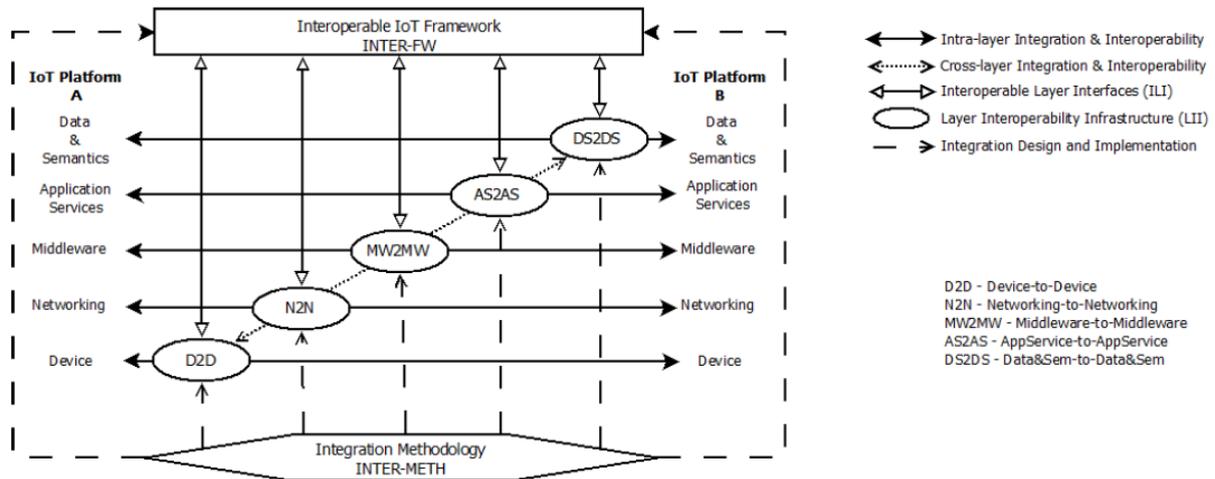


Figure 2: INTER-IoT approach abstract schema

INTER-LAYER

INTER-IoT uses a layer-oriented approach to fully exploit specific functionalities of each layer (device, networking, middleware, application services, data & semantics) (see Figure 2). Although the development of a layer-oriented approach is a research challenge, as compared to a global approach, it has a higher potential to deliver tight bidirectional integration among heterogeneous IoT platforms, notably guaranteeing independence, thus providing higher performance, modularity and reliability and, what is extremely important, more control on functional and non-functional requirements. In addition, the data and semantics level provides a global shared ontology and methods in order to achieve IoT platform semantic interoperability.

INTER-LAYER includes the design of device-to-device interaction based on multiprotocol/access mechanisms, the design of software defined interoperable modules for mobility and routing, the development of an open service discovery and management framework for smart objects, the design and implementation of smart IoT application service gateway and virtualization and the definition of a common ontology for IoT platform semantic interoperability.

INTER-FW

The Interoperability IoT Framework (INTER-FW) aims at providing global and open platform-level interoperability among heterogeneous IoT platforms coupled through specifically developed Layer Interoperability Infrastructures (LIIs) and Interoperability Layer Interfaces (ILI). INTER-FW will rely on an architectural meta-model for IoT interoperable platforms, on a metadata-model for IoT interoperable semantics and it will provide a programming API and tools allowing global-level management of the integrated IoT platforms.

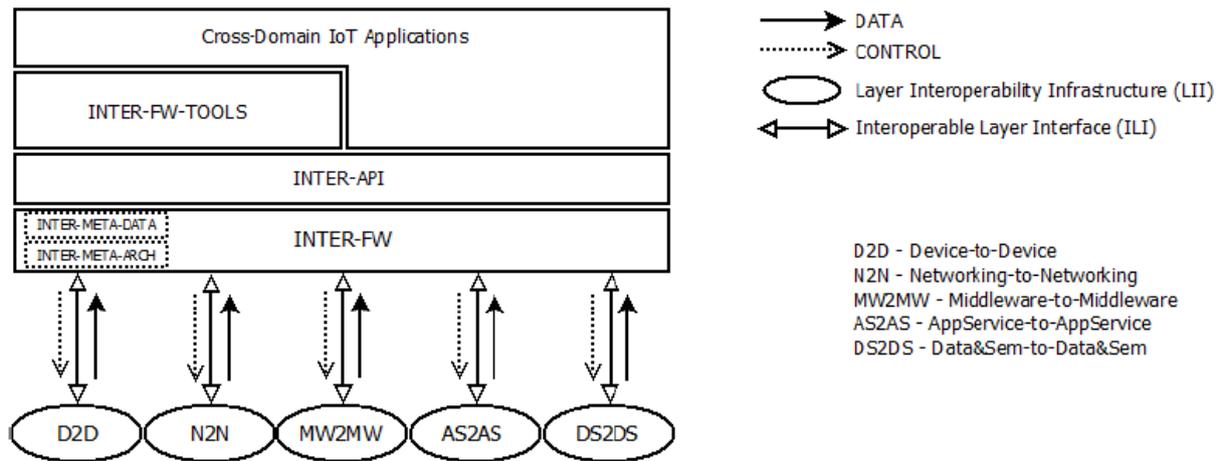


Figure 3: Abstract schema of the INTER-FW

Figure 3 shows the abstract schema of the INTER-FW. INTER-FW will advance the state-of-the-art by providing a general and effective method for inter-platform interoperability, addressing at a global level: real-timeless, reliability, security, privacy and trust. In particular, INTER-FW will thoroughly address privacy and security-related risks and challenges resulting from the use of IoT devices.

INTER-METH

The engineering methodology INTER-METH aims at defining a systematic methodology supporting the integration process of heterogeneous IoT platforms to obtain interoperability among them so allowing implementation and deployment of IoT applications at the top of them. It is widely recognized that using an engineering methodology is fundamental in any engineering application domain (e.g. software engineering, codesign hardware/software, civil engineering, etc.). The manual and non-systematic application of complex techniques, methods and frameworks would very likely lead to an increase of the degree of errors during integration. INTER-METH is supported by a Computer Aided Software Engineering tool (CASE) for driving IoT platforms/systems integration (INTER-CASE).

INTER-IoT considers two application domains: transportation and logistics in a port environment and m-health. Around these two application domains, three use cases will be built and packaged as products of the project:

1. INTER-LogP for “Smart Port Transportation for Containers and Goods”;
2. INTER-Health for “Decentralized and Mobile Monitoring of Assisted Livings” and
3. INTER-DOMAIN in which IoT platforms from both application domains plus some additional ones will be integrated.

INTER-LogP

INTER-LogP use case illustrates the need to achieve seamlessly interoperability of different heterogeneous IoT platforms, oriented to port transport and logistics. The considered application domain identifies several physical transport entities (trucks, containers, semi-trailers, cranes, tractors and other container handling machines) owned by different companies. The possibility to capture in real

time sensor-based data coming from these physical moving assets and connecting them to transport and logistic infrastructures, is an opportunity to drive optimal real-time execution as well as automation of transport and logistics operations. The capture and sharing of real time sensor-based data across different organisations is today a big challenge as there is not any solution in the market able to attend this need and overcoming the complexity of implementing IoT solutions connecting different sensors, systems and products. Sensor-based technology is already being pushed by the transportation and logistics industry. However, what it is lacking is the ability to effectively capture and share the data relative to the movement of vehicles and goods and convert it into actionable insights capable of driving improvements across the supply chain. The lack of use of IoT oriented platforms and their interoperability is today a main obstacle.

For example, almost any person, truck, machine and equipment have been outfitted or it is relatively easy to do so with GPS devices and other sensors to capture information such as location, speed and idle time. With this information, companies have been able to compile and assess several indicators like delivery times, fuel consumption or emissions. However, these companies are not able to design and establish connections with platforms managed by other operators in the supply, logistics and transport chains. The global and interconnected nature of today's supply chains needs a greater collaboration among supply chain partners. The interoperability of heterogeneous IoT platforms can provide a framework for real-time multidirectional information sharing to help in creating true supply chain collaboration.

INTER-Health

INTER-Health scenario for Decentralized and Mobile Monitoring of Assisted Livings' Lifestyle aims at developing an integrated IoT system for monitoring humans' lifestyle in a decentralized way and in mobility, to prevent health issues mainly resulting from food and physical activity disorders. By exploiting the integrated system - INTER-Health - the patient's monitoring process can be decentralized from the healthcare centre to the monitored subjects' homes, and supported in mobility by using on-body physical activity monitors.

The INTER-DOMAIN solution has not yet been considered as an initial product to be offered since its requirements and domain is still unknown until the open call takes place. Only when third party entities with the clear goal of fostering the adoption of INTER-IoT developments are selected, the INTER-DOMAIN could be considered as a product to be offered to the market.

1.4 Scope of the document

An innovation such as the Internet of Things reaches a critical mass of adoption when its acceptance, trust and regulatory constraints are very well defined and executed. In fact, as a famous quote states, "trust takes years to build, seconds to break and forever to repair". This focus on legal issues and stability is essential for building trust, growing confidence and facilitating investment.

Being aware of how important is to build trust and protect individuals' rights, task 2.5 (T2.5) details legal and regulatory constraints in different countries that have to be considered when designing INTER-IoT solutions.

Additionally, legal aspects are examined by compiling national information on the project area and ensuring specifically that INTER-IoT propositions are compliant with the legal context,

especially in both application domains. This task defines the basic requirements that need to be incorporated into the subsequent, rather technical and operational activities. Furthermore, some legal guidance and advice has been taken into account from international and European regulatory bodies, data protection authorities and organizations.

Given that many IoT solutions involve the collection and use of vast quantities of data about individuals (e.g. personal health data) it is unsurprising that data privacy and security are key concerns for this consortium. Moreover, because IoT combines data from a variety of sources, this can result in additional security vulnerabilities if legal requirements are not carefully reviewed.

2 Methodology

The methodology that has been used as a reference for the tasks involved in Work Package 2 (WP2) is Volere. Volere has been used by thousands of organizations around the world in order to define, discover, communicate and manage all the necessary requirements for any type of system development (e.g. software, hardware, commodities, services, organizational, etc.) Volere can be applied in almost all kinds of development environments, with any other development methods or with most requirements tools and modelling techniques. To produce accurate and unambiguous requirements, the Volere methodology uses techniques that are based on experience from worldwide business analysis projects, and are continually improved.

One of the sections of the non-functional requirements, within the methodology Volere, is the identification of legal requirements. The legal requirements have the purpose of assuring compliance to applicable laws. This is why it is very important to collect complete analysis of legal requirements for IoT system and whether or not the system is under the jurisdiction of any law. In addition, INTER-IoT should comply international standards and agreements.

It is not always apparent that there are applicable standards because their existence is often taken for granted or in this case, the IoT is in constant change.

IoT is currently going through a significant phase of definition the code of practice, systems architecture and issues to consider.

2.1 Identification

This phase has been carried out collecting the information provided in the official sites of the main organisms at international, European and national level according to several topics related to IoT.

To facilitate further the identification, the legislation has been classified into the following topics:

- IoT and Smart Infrastructures
- Interoperability
- Security
- Data Protection/Privacy
- Cloud
- Trust Services
- Anonymization
- Tracking of goods and people

The national level has been completed with contributions from INTER-IoT partners who have reviewed the legislation from their respective countries. We have make an extra effort in the area of transport and logistics in Spain, as the pilot associated with INTER-LogP will be deployed in Valencia, and the same in the area of m-health as the pilot associated with INTER-Health will be deployed in Torino. The legislation and regulation will be reviewed in the INTER-

Domain use case as long as the project evaluates and accepts the third party from the open call.

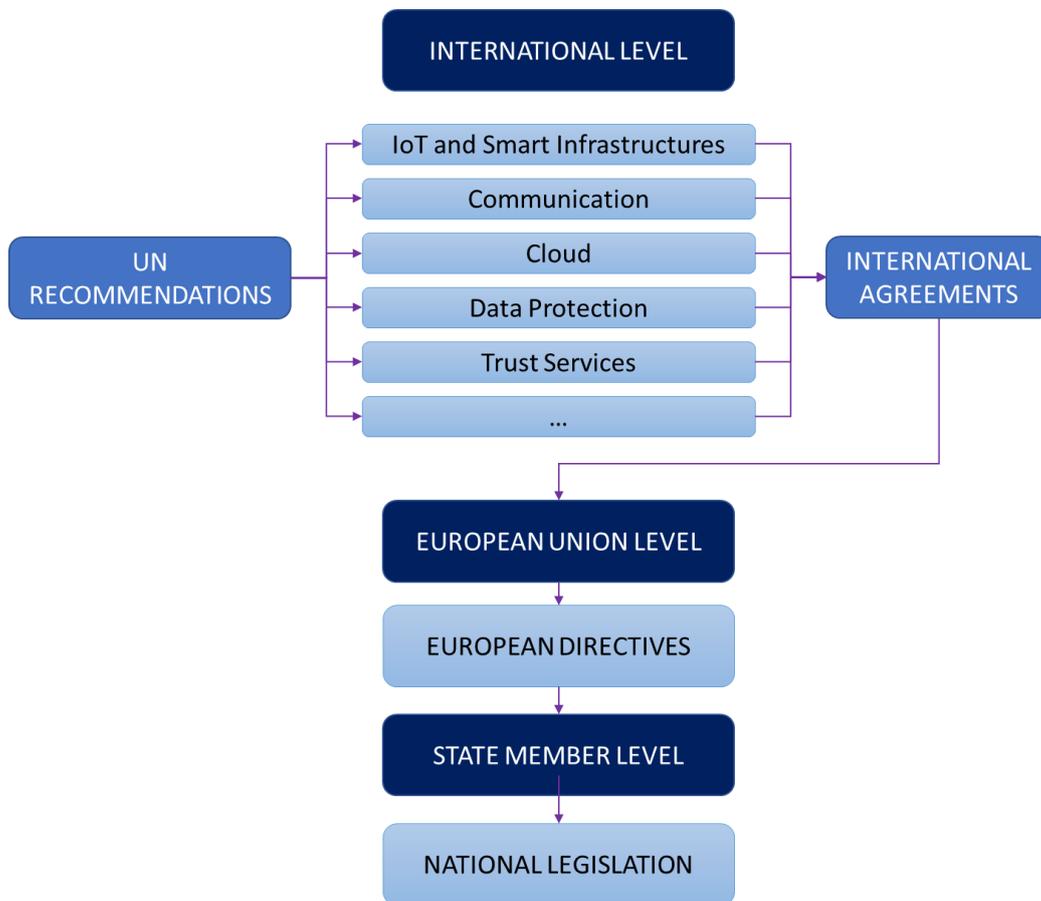


Figure 4. IoT Legal Framework [Source: Valenciaport Foundation]

In this section, the identification has been carried out with the aim to obtain a clear and accurate sight of the present legal and policy environment involving IoT. The analysis is developed at three levels: international, European and national. For this reason, the information is provided in tables, which are classified in the mentioned levels. Every table contains the following items:

- Scope of the law or policy: international, European and national (France, Italy Netherlands, Poland, Slovenia, Spain and United Kingdom).
- Identified topics.
- Title of the legal text and its year of adoption.
- Brief description of the law/policy.
- Adopted legislation in each INTER-IoT partner country according to the European or international legal system.

The transposition of a European directive can have three states: In force, in progress, and no participation.

Table 1. Example of regulation

EUROPEAN COMMUNITY		
According to	Legislation	Scope
TRUST SERVICES	<p>eIDAS regulation REGULATION (EU) No 910/2014 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC</p>	<p>The eSignature Directive established the legal framework at European level for electronic signatures and certification services. The aim is to make electronic signatures easier to use and help them become legally recognised within the Member States. The Directive does not favour any specific technology. A reliable system of electronic signatures that work across EU countries is vital for safe electronic commerce and efficient electronic delivery of public services to businesses and citizens.</p>

3 Legal aspects in interoperability and IoT

IoT in general, as well as interoperability of IoT in particular - especially when health and logistics issues are at hand - lay at the intersection of different regulatory thematic fields as they need to be - from a regulatory standpoint - tackled notably with regard to (market) competition, privacy, security, safety and training perspectives. These multiple facets of IoT perhaps explain why, some countries have imposed rules on stakeholders even before the EU started to regulate IoT - related activities.

Since the beginning of the current millennium, for coherence and harmonisation's sake, the EU has started producing rules to make sure the implementation of the European Single Market. The EU Single Market shall guarantee a satisfactory protection to all those involved in producing, using and processing IoT in every economic activity.

This section will first concentrate on describing the relevant EU legislation before briefly presenting the relevant national legislation that complete the European sets of rules that IoT-related activities need to comply with or take into account.

3.1 European legislation

The Inter-IoT project research has led consortium members to find European legislation addresses in detail six different dimensions:

- Trust services
- Data protection
- Interoperability
- Network security
- Logistics
- e-Health

The EU's commitment to promote an efficient single market in which IoT products are set to evolve, while ensuring sufficient protection for communications systems as well as for users themselves, becomes a tangible reality through these regulations and directives.

Table 2. International Legislation

According to	Legislation	Scope
Trust Services	eIDAS regulation REGULATION (EU) No 910/2014 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ²	The eSignature Directive established the legal framework at European level for electronic signatures and certification services. The aim is to make electronic signatures easier to use and help them become legally recognised within the Member States. The Directive does not favour any specific technology. A reliable system of electronic signatures that work across EU countries is vital for safe electronic commerce and efficient electronic delivery of public services to businesses and citizens.
Data Protection	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ³	Directive 95/46/EC is the reference text, at European level, on the protection of personal data. It sets up a regulatory framework, which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To achieve this goal, the Directive sets strict limits on the collection and use of personal data and demands that each Member State sets up an independent national body responsible for the supervision of any activity linked to the processing of personal data.
Data Protection	2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard	In order to facilitate data flows from the Community, it is desirable for data controllers to be able to perform data transfers globally under a single set of data protection rules. In the absence of global data protection standards, standard contractual clauses provide an important tool allowing the transfer of personal data from all Member States under a common set of rules.

² http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

³ <http://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:31995L0046>

	contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271)Text with EEA relevance ⁴	
Data Protection	Regulation (EU) No 611/2013 of the European Commission of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications ⁵	Directive 2002/58/EC provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Union. It sets out specific rules for the notification of data security breaches by telecommunications providers and internet service providers under Directive 2002/58/EC (the “ePrivacy Directive”) as transposed into Irish law via SI 336 of 2011.
Network Security	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 ⁶	The NIS Directive is the main piece of legislation of the “2013 EU Cybersecurity Strategy”. It aims at ensuring a high common level of network and information security (“NIS”) across the EU and in particular requires operators of critical infrastructures and digital service providers to adopt appropriate steps to manage security risks and to report serious incidents to the competent national authorities.
Data Protection	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal	Information is exchanged through public electronic communication services such as the internet and mobile and landline telephony and via their accompanying networks. These services and networks require specific rules and safeguards to ensure the users’ right to privacy and confidentiality.

⁴ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915>

⁵ <http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32013R0611>

⁶ <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148>

	data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ⁷	
Data Protection	Regulation (EC) No 45/2001 of the European Parliament and of the council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ⁸	<p>This European Union law sets out to ensure that citizens' fundamental rights and freedoms, in particular the right to privacy with respect to the processing of personal data by EU institutions and bodies, is respected.</p> <p>This regulation provides for the establishment of an EDPS (European Data Protection Supervisor), the authority responsible for monitoring the application of the data protection rules by EU institutions and bodies. Citizens can lodge complaints directly with the EDPS if they consider their data protection rights under the regulation have not been respected.</p>
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) ⁹	<p>The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.</p> <p>The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect fundamental rights and freedoms, particularly the right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and</p>

⁷ <http://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:32002L0058>

⁸ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001R0045>

⁹ <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>

		the convergence of the economies within the internal market, and finally to the well-being of natural persons.
Data Protection	Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ¹⁰	<p>The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16 of the Treaty on the Functioning of the European Union (TFEU) recognize everyone's right to the protection of personal data concerning him or her.</p> <p>The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Directive is intended to contribute to the accomplishment of an area of freedom, security and justice.</p>
Interoperability	Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network ¹¹	Differences between national technical specifications used for tenders have led to fragmentation of the market and systems and make industrial cooperation at Community level more difficult. European industry is particularly affected, as considerable efforts have to be made to adapt products to national markets. The creation of the Single European Sky requires the interoperability of all national systems.
Interoperability	Regulation (EU) No 328/2012 of 17 April 2012 amending Regulation (EC) No 62/2006 concerning the technical specification for interoperability relating to the	Each technical specification for interoperability (TSI) should indicate the strategy for implementing the TSI and the stages to be completed in order to make a gradual transition from the existing situation to the final situation in which compliance with the TSIs shall be the norm. The strategy to implement the telematic applications for freight services (TAF) TSI should not only rely

¹⁰ <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L0680>

¹¹ <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32004R0552>

	telematic applications for freight subsystem of the trans-European conventional rail system ¹²	on compliance of subsystems with the TSI but it should also be based on a coordinated implementation.
Network Security	Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) ¹³	To accompany the opening up of the telecommunications market to competition, the European Union (EU) has adopted a regulatory framework with regard to electronic communications in line with technological progress and market requirements.
Interoperability	Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services , 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services ¹⁴	The EU regulatory framework for electronic communications networks and services should be reformed in order to complete the internal market for electronic communications by strengthening the Community mechanism for regulating operators with significant market power in the key markets. This is complemented by Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office. The reform also includes the definition of an efficient and coordinated spectrum management strategy so as to achieve a single European information space and the reinforcement of provisions for users with disabilities in order to obtain an inclusive information society.
Interoperability	Directive 2002/19/EC of the European Parliament and of the	This directive harmonises the way in which EU countries regulate access to, and interconnection of, electronic communications networks and associated

¹² <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R0328>

¹³ <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32002L0021>

¹⁴ <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32009L0140>

	Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) ¹⁵	facilities. It establishes a regulatory framework for the relationships between suppliers of networks and services that will result in sustainable competition and interoperability of electronic communications services. Along with Directive 2009/140/EC, Directive 2009/136/EC and Reg. 121/2009
e-Health	Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices , Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market ¹⁶	Software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, is a medical device. However, software for general purposes when used in a healthcare setting is not a medical device. Particular care should be taken to ensure that the reprocessing of medical devices does not endanger patients' safety or health. It is therefore necessary to provide clarification on the definition of the term 'single use', as well as to make provision for uniform labelling and instructions for use.
Logistics	Directive 90/269/EEC of 29 May 1990 on the minimum health and safety requirements for the manual handling of loads where there is a risk particularly of back injury to workers ¹⁷	The aim of the Directive is to ensure that workers in the European Union are protected against the risks involved in the manual handling of loads and establishes the requirement for contractors to provide adequate handling equipment to manipulate loads and avoid health risks.

¹⁵ <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0019>

¹⁶ <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32007L0047>

¹⁷ <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A31990L0269>

Logistics	Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security ¹⁸	This regulation adopts the ISPS code including several of the recommendations given in its Part B. The main objective of this regulation is to introduce and implement Community measures to enhance maritime security in face of threats of intentional unlawful acts. The regulation deals with several issues regarding with the use of security and safety equipment for different purposes like intrusion-detection and surveillance, both for vessels and port facilities and the identification of vulnerabilities.
------------------	--	--

¹⁸ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004R0725>

3.2 Legislation in the countries of the project

This section analyses how the previous European directives and regulations have been transposed to the different countries that are part of the consortium. The list below provides a list of national laws implementing each European legislation. We have kept the description and name of the law in the original language in order to allow better tracking, those available online have been referenced. However in order to provide a better understanding we have added some comments to the different laws and regulations in English.

In some countries the EU regulations are directly transposed and there is no specific national law, as they enter in force automatically. This is a constant view adopted by the European Court of Justice. Other countries have either anticipated EU legislation or have found it necessary to set out some rules for greater market efficiency purposes.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data	
Spain	Real Decreto n° 156/96 de 02/02/1996, por el que se modifica el Estatuto de la Agencia de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, para designar a la Agencia de Protección de Datos como representante español en el grupo de protección de personas previsto en la Directiva 95/46/CE, de 24 de octubre BOE n° 37 de 12/02/1996 Página 4939 (Marginal 2991) ¹⁹
Italy	Legge del 06/10/1998 n. 344, differimento del termine per l'esercizio della delega prevista dalla legge 31 dicembre 1996, n. 676, in materia di trattamento dei dati personali ²⁰
France	Loi n° 2004/801 du 6/8/2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78 - 17 du 6/1/1978 relative à l'informatique, aux fichiers et aux libertés. ²¹
UK	The Data Protection Act 1998 ²² Data Protection Act 2004
Slovenia	Kazenski zakonik - uradno prečiščeno besedilo ²³ Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov ²⁴ Zakon o Informacijskem pooblaščenju ²⁵ Zakon o spremembah in dopolnitvah Zakona o varstvu osebnih podatkov ²⁶
Poland	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (z późniejszymi zmianami) ²⁷

¹⁹ Spanish Law designating the Spanish Data Protection Agency as representative in the people protection group foreseen by Directive 95/46/CE <https://www.boe.es/boe/dias/1996/02/12/pdfs/A04939-04939.pdf>

²⁰ Italian Law deferral of the deadline for the exercise of the associated delegation concerning the processing of personal data <http://www.privacy.it/legge1998344.html>

²¹ French Law on the protection of individuals with regard to the processing of personal data and amending the French Law related to information technology, files and freedoms <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676>

²² <http://www.legislation.gov.uk/ukpga/1998/29/contents>

²³ Slovenian Penal Code <http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4149>

²⁴ Slovenian Laws on the methodology of keeping the register of personal data collection

²⁵ Slovenian Law concerning Information Commissioner

²⁶ Slovenian Law amending the Law on Protection of Personal Data

²⁷ Polish Law of Data Protection <http://isip.sejm.gov.pl/DetailsServlet?id=WDU19971330883>

Netherlands	Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens ref: Staatsblad nr 302 van 2000 ²⁸
	Wet van 6 november 2013 tot aanpassing van enige wetten op het terrein van het Ministerie van Veiligheid en Justitie teneinde een aantal zelfstandige bestuursorganen onder de werking van de Kaderwet zelfstandige bestuursorganen te brengen ²⁹

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)

Spain	Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones BOE n° 264 de 4/11/2003 p. 38890 ³⁰ REAL DECRETO 2296/2004, de 10 de diciembre, por el que se aprueba el Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración ³¹ Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios ³²
Italy	Decreto legislativo 30/6/2003, n. 196-Codice in materia di protezione dei dati personali. GURI n° 174 del 29/7/2003 p. 11 ³³
France	Loi n° 575 du 21/6/2004 pour la confiance dans l'économie numérique ³⁴ Loi n° 669 du 9/7/2004 relative aux communications électroniques et aux services de communication audiovisuelle ³⁵ Loi n° 2004/801 du 6/8/2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78 - 17 du 6/1/1978 relative à l'informatique, aux fichiers et aux libertés ³⁶
UK	The Privacy and Electronic Communications (EC Directive) Regulations 2003 SI 2003 No. 2426 ³⁷ Article 5.1: the Regulation of Investigatory Powers Act 2000 and Article 5.2 : the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000 No. 2699 ³⁸

²⁸ Dutch Law containing rules on the protection of personal data <https://zoek.officielebekendmakingen.nl/stb-2000-302.html>

²⁹ Dutch Law to amend some laws of the Ministry of Security and Justice to bring a number of independent administrative bodies within the scope of the Framework Law

³⁰ Spanish General Law of Telecommunications <https://www.boe.es/boe/dias/2003/11/04/pdfs/A38890-38924.pdf>

³¹ Spanish Law on regulation of markets of electronic communications, and their networks access and numbering

³² Spanish Law regulating the conditions for the provision of electronic communications services, a universal service and the protection of users

³³ Italian Law for the regulation of the Protection of Personal Data <http://www.camera.it/parlam/leggi/deleghe/03196dl.htm>

³⁴ French Law on trust of the digital economy <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164>

³⁵ French Law relating to the electronic communications and to the services of media communications

³⁶ French Law on the protection of individuals with regard to the processing of personal data and amending to a law relating to data processing, files and freedoms

³⁷ <http://www.legislation.gov.uk/ukxi/2003/2426/contents/made>

³⁸ <http://www.legislation.gov.uk/ukxi/2000/2699/contents/made>

	Transposition Note relating to UK Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 ³⁹
Slovenia	Kazenski zakonik Republike Slovenije ⁴⁰ Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah ⁴¹ Zakon o elektronskih komunikacijah ⁴²
Poland	Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną ⁴³ Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne ⁴⁴ Ustawa z dnia 29 grudnia 2005 r. o przekształceniach i zmianach w podziale zadań i kompetencji organów państwowych właściwych w sprawach łączności, radiofonii i telewizji ⁴⁵ Ustawa z dnia 24 kwietnia 2009 r. o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw ⁴⁶
Netherlands	Wet van 22 april 2004 tot wijziging van de Telecommunicatiewet en enkele andere wetten in verband met de implementatie van een nieuw Europees geharmoniseerd regelgevingskader voor elektronische communicatienetwerken en -diensten en de nieuwe dienstenrichtlijn van de Commissie van de Europese Gemeenschappen ⁴⁷ Regeling universele dienstverlening en eindgebruikersbelangen ⁴⁸ Besluit van 7 mei 2004, houdende regels met betrekking tot universele dienstverlening en eindgebruikersbelangen (Besluit universele dienstverlening en eindgebruikersbelangen) ⁴⁹

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

Spain	Not yet implemented
Italy	Not yet implemented
France	Not yet implemented
UK	Not yet implemented
Slovenia	Not yet implemented
Poland	Not yet implemented

³⁹ <http://www.legislation.gov.uk/ukxi/2011/1301/contents/made>

⁴⁰ Slovenian Penal Code

⁴¹ Amendments of the Slovenian Law on Electronic Communications <https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=5111>

⁴² Slovenian Law on electronic communications

⁴³ Polish Law on electronic services <http://isap.sejm.gov.pl/DetailsServlet?id=wdu20021441204>

⁴⁴ Polish Law on telecommunications

⁴⁵ Polish Law relating to the transformations and changes in the division of tasks and powers of the competent state bodies in communications and broadcasting

⁴⁶ Amendments of the Polish Law of telecommunication

⁴⁷ Dutch Law to amend the Telecommunications Law and some other laws in connection with the implementation of a new European regulatory framework for electronic communications networks and services, and the new services of the Commission of the European Communities <http://www.wetboek-online.nl/wet/Wet%20implementatie%20Europees%20regelgevingskader%20voor%20de%20elektronische%20communicatiesector%202002.html>

⁴⁸ Dutch Law on universal service and end-user interests

⁴⁹ Dutch Decision laying down rules on universal service and end-user interests

Netherlands	Not yet implemented
-------------	---------------------

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Spain	Modificaciones a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico ⁵⁰
Italy	Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Il presente regolamento si applica a decorrere dal 1 luglio 2016 ⁵¹
France	-
UK	The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 (2016 No.696) and section 7 of the Electronic Communications Act 2000 (c. 7) ⁵²
Slovenia	-
Poland	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej ⁵³
Netherlands	Besluit van de Minister van Economische Zaken van 29 juni 2016, nr. WJZ / 16094083, tot tijdelijke aanwijzing van een toezichthoudend orgaan, een nationaal orgaan voor informatieveiligheid en een gegevensbeschermingsautoriteit in de zin van verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L 257) ⁵⁴

Regulation (EU) No 611/2013 of the European Commission of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications

Spain	Ley 9/2014, de 9 de mayo, General de Telecomunicaciones ⁵⁵
Italy	Decreto legislativo 30/6/2003, n.196 - Codice in materia di protezione dei dati personali ⁵⁶

⁵⁰ Modification of the Spanish Law regarding the Society of Information and Electronic Commerce <https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>

⁵¹ Regulation (EU) No. 910/2014 of the European Parliament and of the Council in Italy regarding Electronic identification for electronic transactions that is foreseen by the European directive 1999/93/CE

⁵² https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545098/beis-16-15-electronic-signatures-guidance.pdf

⁵³ Polish Law regarding Trust Services and Electronic Identification

http://www.sejm.gov.pl/Sejm8.nsf/komunikat.xsp?documentId=7B5014049C02A2CAC125803E0039E6BF&symbol=KOMUNIKATY_KOMUNIKAT&SessionID=DBAF538BFC5E4083F07FA5B0E4ADC560B197A2B5

⁵⁴ Temporary appointment of a supervisory body in Netherlands, the national agency for information security and data protection authority within the meaning of Regulation (EU) No. 910/2014 of the European Parliament and the Council on electronic identification and trust services for electronic transactions in the internal market and repealing European Directive 1999/93 / EC (OJ 2014 L 257) <https://zoek.officielebekendmakingen.nl/stcrt-2016-34156.html>

⁵⁵ Spanish General Law on Telecommunications <https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950>

⁵⁶ Italian Code on Personal Data Protection <http://www.camera.it/parlam/leggi/deleghe/03196dl.htm>

France	-
UK	The data protection (processing of sensitive personal data) Order 2012 (No. 1978) ⁵⁷
Slovenia	-
Poland	Ustawa z dnia 16 lipca 2004 r. Prawo and EU Regulation No 611/2013 ⁵⁸
Netherlands	Wet van 18 juli 2009 tot wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatiegegevens) ⁵⁹

2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271)Text with EEA relevance

Spain	Modificaciones a la Ley orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal ⁶⁰
Italy	Trasferimento dei dati personali all'estero - Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso paesi terzi - 9 giugno 2005 ⁶¹
France	-
UK	Modifications to the Data protection Act 1998 ⁶²
Slovenia	Zakon o varstvu osebnih podatkov ⁶³
Poland	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (z późniejszymi zmianami) ⁶⁴
Netherlands	Wijziging van de Wet bescherming persoonsgegevens in verband met de vermindering van administratieve lasten en nalevingskosten, wijzigingen teneinde wetstechnische gebreken te herstellen en enige andere wijzigingen ⁶⁵

⁵⁷ <http://www.legislation.gov.uk/ukdsi/2012/9780111524299>

⁵⁸ Polish Law regarding EU regulation 611/2013 <http://isap.sejm.gov.pl/DetailsServlet?id=WDU20041711800>

⁵⁹ Dutch Law to amend the Telecommunications Law and the Law on Economic Offences related to the implementation of the European Directive 2006/24 / EC of the European Parliament and the Council of the European Union on the retention of data processed in connection with the provision of public electronic communication services, and amending Directive 2002/58 / EC (Law obligation to retain telecommunications data) <http://wetten.overheid.nl/BWBR0026191/2009-09-01>

⁶⁰ Amendments to the Spanish Law of Protection of Personal Data <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750>

⁶¹ Authorization in Italy to transfer abroad personal data, from the Italian State to third countries

<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1151949>

⁶² <http://www.legislation.gov.uk/ukpga/1998/29/contents>

⁶³ Slovenian Law on the protection of personal data <https://www.uradni-list.si/1/content?id=82668>

⁶⁴ Modification to the Polish Law of Protection of Personal Data in connection with the reduction of administrative burdens and compliance costs, changes in order to restore technical legal defects and any other changes <http://isap.sejm.gov.pl/DetailsServlet?id=WDU19971330883>

⁶⁵ Modification of the Dutch Data Protection Law in connection with the reduction of administrative burdens and compliance costs, changes in order to restore technical legal defects and any other change telecommunications data https://www.eerstekamer.nl/wetsvoorstel/31841_wijziging_wet_bescherming

Regulation (EC) No 45/2001 of the European Parliament and of the council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data	
Spain	Modificaciones a la Ley orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal ⁶⁶
Italy	Decreto legislativo 30/6/2003, n.196 - Codice in materia di protezione dei dati personali ⁶⁷
France	-
UK	The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 (No 2905) ⁶⁸
Slovenia	-
Poland	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (z późniejszymi zmianami) ⁶⁹
Netherlands	VERORDENING (EG) Nr. 45/2001 VAN HET EUROPEES PARLEMENT EN DE RAAD van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens ⁷⁰

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)	
Spain	Not yet implemented
Italy	Not yet implemented
France	Not yet implemented
UK	Not yet implemented
Slovenia	Not yet implemented
Poland	Not yet implemented
Netherlands	Not yet implemented

⁶⁶ Amendments to the Spanish Law of Protection of Personal Data <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750>

⁶⁷ Italian Law for the Protection of Personal Data <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750>

⁶⁸ http://www.legislation.gov.uk/uk/si/2002/2905/pdfs/ukSI_20022905_en.pdf

⁶⁹ Amendment to the Polish Law of Data Protection <http://isip.sejm.gov.pl/DetailsServlet?id=WDU19971330883>

⁷⁰ European Regulation on Netherlands (EC). 45/2001 of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data <http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=uriserv%3Al24222>

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Spain	Not yet implemented
Italy	Not yet implemented
France	Not yet implemented
UK	Not yet implemented
Slovenia	Not yet implemented
Poland	Not yet implemented
Netherlands	Not yet implemented

Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network

Repeal: Regulation (EC) No 1070/2009 of the European Parliament and of the Council of 21 October 2009 amending Regulations (EC) No 549/2004, (EC) No 550/2004, (EC) No 551/2004 and (EC) No 552/2004 in order to improve the performance and sustainability of the European aviation system

Spain	Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea ⁷¹
Italy	Regolamento (CE) n. 1070/2009 del Parlamento europeo e del Consiglio, del 21 ottobre 2009, recante modifica dei regolamenti (CE) n. 549/2004, (CE) n. 550/2004, (CE) n. 551/2004 e (CE) n. 552/2004 al fine di migliorare il funzionamento e la sostenibilità del sistema aeronautico europeo ⁷²
France	-
UK	The single European sky (National supervisory Authority) regulations 2004 (No. 1958) ⁷³
Slovenia	-
Poland	Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze (z późniejszymi zmianami) ⁷⁴
Netherlands	Wet van 27 september 2012, houdende goedkeuring van het op 2 december 2010 te Brussel tot stand gekomen Verdrag betreffende de oprichting van het Functioneel Luchtruimblok «Europe Central» tussen de Bondsrepubliek Duitsland, het Koninkrijk België, de Republiek Frankrijk, het Groothertogdom Luxemburg, het Koninkrijk der Nederlanden en de Zwitserse Bondsstaat (Trb. 2011, 27) en wijziging van de Wet luchtvaart ter uitvoering van verordening (EG) nr. 1070/2009 van het Europees

⁷¹ Spanish Law on the development of the Air Regulation and common operational provisions for air navigation services and procedures.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-6856

⁷² European Regulation present in Italy, (EC) No. 1070/2009, amending European Regulations (EC) No. 549/2004, (EC) No. 550/2004, (EC) No. 551/2004 and (EC) No. 552/2004 in order to improve the performance and sustainability of the European aviation system

⁷³ http://www.uklaws.org/statutory/instruments_32/doc32030.htm

⁷⁴ Amendment on Polish Law on Aviation <http://isap.sejm.gov.pl/DetailsServlet?id=WDU20021301112>

	Parlement en de Raad van de Europese Unie van 21 oktober 2009 tot wijziging van verordeningen (EG) nr. 549/2004, (EG) nr. 550/2004, (EG) nr. 551/2004 en (EG) nr. 552/2004 teneinde de prestaties en de duurzaamheid van het Europese luchtvaartstelsel te verbeteren (PbEU 2009 L 300) ⁷⁵
--	---

Regulation (EU) No 328/2012 of 17 April 2012 amending Regulation (EC) No 62/2006 concerning the technical specification for interoperability relating to the telematic applications for freight subsystem of the trans-European conventional rail system Text with EEA relevance	
Spain	Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y se modifica el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea ⁷⁶
Italy	REGOLAMENTO (UE) N. 328/2012 DELLA COMMISSIONE del 17 aprile 2012 recante modifica del regolamento (CE) n. 62/2006 relativo alla specifica tecnica di interoperabilità per il sottosistema Applicazioni telematiche per il trasporto merci del sistema ferroviario transeuropeo convenzionale ⁷⁷
France	-
UK	-
Slovenia	-
Poland	Ustawa z dnia 28 marca 2003 r. o transporcie kolejowym (z późniejszymi zmianami) Rozporządzenie Ministra Infrastruktury i Budownictwa z dnia 25 lutego 2016 r. w sprawie interoperacyjności systemu kolei) ⁷⁸
Netherlands	VERORDENING (EU) Nr. 328/2012 VAN DE COMMISSIE van 17 april 2012 tot wijziging van Verordening (EG) nr. 62/2006 betreffende de technische specificaties voor interoperabiliteit inzake het subsysteem „Telematicatoepassingen voor goederenvervoer” van het conventionele trans-Europese spoorwegsysteem ⁷⁹

⁷⁵ Dutch convention concerning the establishment of the Functional Airspace Block "Europe Central" " between the Federal Republic of Germany, the Kingdom of Belgium, the French Republic, the Grand Duchy of Luxembourg, the Kingdom the Netherlands and the Swiss Confederation, and amendment of the Dutch Law on aviation pursuant to Regulation (EC) no. 1070/2009 of the European Parliament and of the Council of the European Union of 21 October 2009 amending regulations (EC) no. 549/2004, (EC) no. 550/2004, (EC) no. 551/2004 and (EC) No. 552/2004 in order to improve the performance and sustainability of the European aviation system (OJ 2009 L 300)C) no. 1070/2009

⁷⁶ Spanish Law on the Air Regulation and common operational provisions for air navigation services and procedures that amends the Spanish Law on Regulation of Aerial Circulation https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-6856

⁷⁷ European Regulation No. 62/2006 present in Italy concerning the technical specification for interoperability relating to the subsystems of telematics applications for European freight conventional rail system

⁷⁸ Amendment on the Polish Law on railway transport concerning the interoperability of the rail system.

<http://isap.sejm.gov.pl/DetailsServlet?id=WDU20030860789>

⁷⁹ European Regulation (EU). 328/2012 present in Netherlands amending European Regulation (EC) no. 62/2006 concerning the technical specification for interoperability relating to the subsystem "telematics applications for freight" of the trans-European rail system <http://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX%3A32012R0328>

Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities	
Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services	
Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services	
Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services	
Spain	<p>Ley 32 de 3/11/2003, General de Telecomunicaciones. BOE n° 264 de 4/11/2003 p. 38890 ⁸⁰</p> <p>REAL DECRETO 2296/2004, de 10 de diciembre, por el que se aprueba el Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración ⁸¹</p> <p>Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios ⁸²</p>
Italy	Decreto legislativo 1/8/2003, n. 259 - Codice delle comunicazioni elettroniche. GURI n° 214 del 15/9/2003 p. 3 ⁸³
France	<p>Loi n° 669 du 9/7/2004 relative aux communications électroniques et aux services de communication audiovisuelle ⁸⁴</p> <p>Décret n° 2004-1301 du 26 novembre 2004 relatif aux dispositions applicables aux opérateurs exerçant une influence significative sur un marché du secteur des communications électroniques en application des articles L.37-1 à L.38-3 du code des postes et des communications électroniques ⁸⁵</p> <p>Décret n° 2005-399 du 27/4/2005 modifiant la troisième partie (Décrets) du code des postes et des communications électroniques ⁸⁶</p> <p>Décret n° 2005/606 du 27/5/2005 relatif aux annuaires et aux services de renseignements et modifiant le code des postes et des communications électroniques ⁸⁷</p>

⁸⁰ General Spanish Law on Telecommunications <https://www.boe.es/boe/dias/2003/11/04/pdfs/A38890-38924.pdf>

⁸¹ Spanish Law on the regulation of the market of electronic communications, its network access and specific numbering

⁸² Spanish Law on the regulation on the conditions for the provision of electronic communications services, a universal service and user protection

⁸³ Italian Law on Electronic Communications ⁸³ <http://www.camera.it/parlam/leggi/deleghe/03259dl.htm>

⁸⁴ French Law on Electronic Communications and Audiovisual Communication Services

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000439399>

⁸⁵ French Law on the dispositions of operators exercising significant influence in markets in the electronic communications sector pursuant to Articles of the French Postal and Electronic Communications Code

https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=CA7D0F39AE58F23C6F4FC50A7D52D5B6.tpdila14v_1?cidTexte=JORFTEXT000000258070&dateTexte=29990101

⁸⁶ French Law amending the French Postal and Electronic Communication Code

https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=5CE015D2D3866D5AA0A52829B7E94D99.tpdila22v_2?cidTexte=JORFTEXT000000605864&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000000003371

⁸⁷ French Law on directories and information services that amends the French Postal and Electronic Communications Code

UK	<p>The Electronic Communications (Universal Service) Regulations 2003; SI n° 33 of 9/1/2003 ⁸⁸</p> <p>The Electronic Communications (Market Analysis) Regulations 2003; SI n° 330 of 19/2/2003 ⁸⁹</p> <p>The Wireless Telegraphy (Limitation of Number of Licences) Order 2003. SI n° 1902 of 17/7/2003 ⁹⁰</p>
Slovenia	<p>Pravilnik o načrtu oštevilčenja ⁹¹</p> <p>Splošni akt o določitviupoštevnihtrgov ⁹²</p> <p>Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (ZEKom-C) ⁹³</p> <p>Zakon o elektronskih komunikacijah ⁹⁴</p>
Poland	<p>Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego ⁹⁵</p> <p>Ustawa z dnia 24 kwietnia 2009 r. o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw ⁹⁶</p> <p>Ustawa z dnia 29 kwietnia 2010 r. o zmianie ustawy - Prawo telekomunikacyjne ⁹⁷</p> <p>Ustawa z dnia 15 kwietnia 2011 r. o zmianie ustawy - Prawo telekomunikacyjne ⁹⁸</p>
Netherlands	<p>Wet van 22 april 2004 tot wijziging van de Telecommunicatiewet en enkele andere wetten in verband met de implementatie van een nieuw Europees geharmoniseerd regelgevingskader voor elektronische communicatienetwerken en -diensten en de nieuwe dienstenrichtlijn van de Commissie van de Europese Gemeenschappen ⁹⁹</p> <p>Wijziging diverse ministeriële regelingen i.v.m. aanpassing aan de Telecommunicatiewet ¹⁰⁰</p> <p>Besluit van 7 mei 2004, houdende wijziging van enkele algemene maatregelen van bestuur in verband met aanpassingen aan de Telecommunicatiewet ¹⁰¹</p>

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services

Spain	Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones
-------	--

⁸⁸ http://www.legislation.gov.uk/uksi/2003/2426/pdfs/uksi_20032426_en.pdf

⁸⁹ http://www.legislation.gov.uk/uksi/2003/3125/pdfs/uksi_20033125_en.pdf

⁹⁰ http://www.legislation.gov.uk/uksi/2003/1902/pdfs/uksi_20031902_en.pdf

⁹¹ Slovenian Law regulating the numbering <http://www.pisrs.si/Pis.web/pregledPredpisa?id=PRAV5902>

⁹² Slovenian Law establishing the relevant markets http://www.pisrs.si/Pis.web/pregledPredpisa?id=AKT_503

⁹³ Slovenian Law amending the National Law on Electronic Communications (ZEKom-C)

<http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6086>

⁹⁴ Slovenian Law on Electronic Communications

⁹⁵ Polish Code of Administrative Procedure

⁹⁶ Amendment on Polish Law on Telecommunications

⁹⁷ Amendment on Polish Law on Telecommunications

⁹⁸ Amendment on Polish Law on Telecommunications https://uke.gov.pl/files/?id_plik=8805

⁹⁹ Amendment on the Dutch Telecommunications Law and some other laws in connection with the implementation of a new European harmonized regulatory framework for electronic communications networks and services

¹⁰⁰ Amendment of several Dutch regulations on Telecommunications

¹⁰¹ Amendment on certain orders in the Dutch council in connection with amendments on Dutch regulations on Telecommunication

	electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista ¹⁰²
Italy	<p>Consultazione pubblica riguardante modifica delle norme sulla portabilità del numero mobile a seguito del recepimento delle direttive europee 2009/136/CE e 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009, e modifica di alcune disposizioni riguardanti le penali, nonché misure temporanee urgenti di modifica della delibera n. 78/08/CIR. (Deliberazione n. 30/11/CR). ¹⁰³</p> <p>Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee - Legge Comunitaria 2010 ¹⁰⁴</p> <p>Modifiche al decreto legislativo 1° agosto 2003, n. 259, recante codice delle comunicazioni elettroniche in attuazione delle direttive 2009/140/CE, in materia di reti e servizi di comunicazione elettronica, e 2009/136/CE in materia di trattamento dei dati personali e tutela della vita privata ¹⁰⁵</p>
France	<p>Article 5 du décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » ¹⁰⁶</p> <p>Article 17 de la loi n°2011-302 du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques ¹⁰⁷</p> <p>Décret no 2012-488 du 13 avril 2012 modifiant les obligations des opérateurs de communications électroniques conformément au nouveau cadre réglementaire européen (rectificatif) ¹⁰⁸</p> <p>Décret no 2012-1266 du 15 novembre 2012 relatif au contrôle de la sécurité et de l'intégrité des installations, réseaux et services des opérateurs de communications électroniques ¹⁰⁹</p>
UK	<p>The Electronic Communications and Wireless Telegraphy Regulations 2011 ¹¹⁰</p> <p>The Communications Act 2006 (Amendment) Regulations 2011 ¹¹¹</p> <p>The Communications (Access) (Amendment) Regulations 2011 ¹¹²</p> <p>The Communications (Authorisation and Licensing) (Amendment) Regulations 2011¹¹³</p>
Slovenia	Zakon o digitalni radiodifuziji (ZDRad) ¹¹⁴

¹⁰² Spanish Law that transposes directives on electronic communications and on internal electricity and gas markets, and adopts measures to correct deviations due to mismatches between the costs and revenues of the electricity and gas sectors

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2012-4442

¹⁰³ Public consultation in Italy on changes to the rules on mobile number portability and amendment on dispositions on urgent and temporary criminal measures

¹⁰⁴ Italian Regulation concerning obligations deriving from the membership of Italia in EC

¹⁰⁵ Changes to Italian Law, that lay down the Code of electronic communications in the implementation of the 2009/140 / EC, in the field of electronic communications networks and services, and 2009/136 / EC concerning the processing of personal data and protection of privacy

¹⁰⁶ French Law establishing the figure of the National Agency for the Security of Information Systems

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212>

¹⁰⁷ French Law laying down dispositions for adapting French legislation to the European Union law in the field of health, work and electronic communications <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023751262&categorieLien=id>

¹⁰⁸ French Law that amends the obligations of electronic communications operators to be in accordance with the new European regulatory framework (corrigendum) <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025688775&categorieLien=id>

¹⁰⁹ French Law on the control of the security and integrity of the installations, networks and services of electronic communications operators <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026638421&categorieLien=id>

¹¹⁰ <http://www.legislation.gov.uk/uksi/2011/1210/contents/made>

¹¹¹ <http://www.legislation.gov.uk/uksi/2011/1211/contents/made>

¹¹² <http://www.legislation.gov.uk/uksi/2011/1212/contents/made>

¹¹³ <http://www.legislation.gov.uk/uksi/2011/2042/contents/made>

¹¹⁴ Slovenian Law on Digital Broadcasting

	Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (ZEKom-B) ¹¹⁵ Zakon o elektronskih komunikacijah ¹¹⁶ Zakon o spremembah in dopolnitvi Zakona o elektronskih komunikacijah ¹¹⁷
Poland	Rozporządzenie Ministra Infrastruktury z dnia 21 lipca 2008 r. w sprawie zakresu oferty ramowej o dostępie telekomunikacyjnym ¹¹⁸ Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami ¹¹⁹ Ustawa z dnia 16 listopada 2012 r. o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw ¹²⁰ Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 19 marca 2013 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług ¹²¹
Netherlands	Wet van 10 mei 2012 tot wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen ¹²² Besluit van 30 mei 2012 tot wijziging van het Besluit interoperabiliteit, het Besluit randapparaten en radioapparaten 2007, het Besluit universele dienstverlening en eindgebruikersbelangen, het Besluit vergoedingen Telecommunicatiewet, het Besluit voorwaardelijke toegang en het Frequentiebesluit, ter implementatie van de herziene telecommunicatierichtlijnen (Besluit implementatie herziene telecommunicatierichtlijnen) ¹²³

Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market

Spain	REAL DECRETO 1054/2002, de 11 de octubre, por el que se regula el proceso de evaluación para el registro, autorización y comercialización de biocidas ¹²⁴ Real Decreto 1591/2009, de 16 de octubre, por el que se regulan los productos sanitarios ¹²⁵ Real Decreto 1616/2009, de 26 de octubre, por el que se regulan los productos sanitarios implantables activos ¹²⁶
-------	---

¹¹⁵ Slovenian Law amending the Slovenian Law on Electronic Telecommunications (ZEKom-B)

¹¹⁶ Slovenian Law on Electronic Communications

¹¹⁷ Slovenian Law amending the National Law on Electronic Communications

¹¹⁸ Polish Law on the scope of the reference offer for telecommunication access regarding infrastructures

¹¹⁹ Polish Law on Real State

¹²⁰ Polish Law amending national Telecommunications Law

¹²¹ Polish Law on the model form to provide information about the breach of security or integrity of the network or telecommunications services

¹²² Dutch Law amending the national Telecommunications Law to implement revised telecommunications directives

¹²³ Dutch Law amending national laws on interoperability, on peripheral decision equipment and radio equipment, on universal service and retail interests, on Telecommunications fees, on conditional access and Frequency Decree

¹²⁴ Spanish Law on the regulation of biocides https://www.boe.es/diario_boe/txt.php?id=BOE-A-2002-19923

¹²⁵ Spanish Law on medical devices <https://www.boe.es/buscar/doc.php?id=BOE-A-2009-17606>

¹²⁶ Spanish Law on active implantable medical devices <https://www.boe.es/boe/dias/2009/11/06/pdfs/BOE-A-2009-17607.pdf>

Italy	<p>Modifiche ed integrazioni al decreto 20 febbraio 2007 recante "nuove modalità per gli adempimenti previsti per la registrazione dei dispositivi impiantabili attivi nonché per l'iscrizione nel Repertorio dei dispositivi medici" ¹²⁷</p> <p>Attuazione della direttiva 2007/47/CE che modifica le direttive 90/385/CEE per il ravvicinamento delle legislazioni degli stati membri relative ai dispositivi medici impiantabili attivi, 93/42/CE concernente i dispositivi medici e 98/8/CE relativa all'immissione sul mercato dei biocidi ¹²⁸</p>
France	<p>Décret no 2009-482 du 28 avril 2009 relatif aux conditions de mise sur le marché des dispositifs médicaux ¹²⁹</p> <p>Ordonnance no 2010-250 du 11 mars 2010 relative aux dispositifs médicaux ¹³⁰</p> <p>Arrêté du 15 mars 2010 fixant les conditions de mise en oeuvre des exigences essentielles applicables aux dispositifs médicaux, pris en application de l'article R. 5211-24 du code de la santé publique ¹³¹</p> <p>Arrêté du 15 mars 2010 fixant les modalités d'application des procédures de certification de la conformité définies aux articles R. 5211-39 à R. 5211-52, pris en application de l'article R. 5211-53 du code de la santé publique ¹³²</p>
UK	The Medical Devices (Amendment) Regulations 2008 ¹³³
Slovenia	<p>Zakon o biocidnih proizvodih (ZBioP) ¹³⁴</p> <p>Zakon o medicinskih pripomočkih (ZMedPri) ¹³⁵</p> <p>Pravilnik o medicinskih pripomočkih ¹³⁶</p>
Poland	<p>Ustawa z dnia 20 maja 2010 r. o wyrobach medycznych ¹³⁷</p> <p>Rozporządzenie Ministra Zdrowia z dnia 5 listopada 2010 r. w sprawie sposobu klasyfikowania wyrobów medycznych ¹³⁸</p> <p>Rozporządzenie Ministra Zdrowia z dnia 12 stycznia 2011 r. w sprawie wymagań zasadniczych oraz procedur oceny zgodności wyrobów medycznych ¹³⁹</p> <p>Rozporządzenie Ministra Zdrowia z dnia 31 marca 2011 r. w sprawie szczegółowych wymagań, jakie powinny spełniać jednostki ubiegające się o autoryzację celem notyfikacji w zakresie wyrobów, oraz sposobu sprawowania nadzoru i kontroli jednostek notyfikowanych ¹⁴⁰</p> <p>Ustawa z dnia 11 września 2015 r. o zmianie ustawy o wyrobach medycznych oraz niektórych innych ustaw ¹⁴¹</p>
Netherlands	Wet van 11 september 2008 tot aanpassing van de Wet op de medische hulpmiddelen aan richtlijn nr. 2007/47/EG van het Europees Parlement en de Raad van 5 september 2007 tot wijziging van Richtlijn 90/385/EEG van de Raad

¹²⁷Modifications on Italian Law concerning the registration of active implantable devices

¹²⁸Implementation the European Law 2007/47 /EC concerning active implantable medical devices, medical devices and the market of biocidal products

¹²⁹ French Law on the market of medical devices <https://www.legifrance.gouv.fr/eli/decret/2009/4/28/SJSP0828003D/jo>

¹³⁰ French Law on requirements of medical devices <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021961300>

¹³¹ French Law on the application of the conformity certification procedures concerning national Health Law

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021974462&categorieLien=id>

¹³² French Law on the certification procedures concerning Health Law

¹³³ <http://www.legislation.gov.uk/uksi/2008/2936/regulation/7/made#regulation-7-b>

¹³⁴ Slovenian Law on biocidal products

¹³⁵ Slovenian Law on Medical Devices

¹³⁶ Slovenian Laws on Medical Devices

¹³⁷ Polish Law on Medical Devices

¹³⁸ Polish Law on the classification method of medical devices

¹³⁹ Polish Law on the essential requirements and procedures for medical devices

¹⁴⁰ Polish Law on the requirements for product authorization, and how to supervise and control of notified bodies

¹⁴¹ Amendment on the Polish Law on medical devices

	<p>betreffende de onderlinge aanpassing van de wetgevingen van de lidstaten inzake actieve implanteerbare medische hulpmiddelen, Richtlijn 93/42/EEG van de Raad betreffende medische hulpmiddelen en Richtlijn 98/8/EG betreffende het op de markt brengen van biociden (PbEU L 247) ¹⁴²</p> <p>Besluit van 4 november 2008, houdende wijziging van het Besluit actieve implantaten en het Besluit medische hulpmiddelen ¹⁴³</p>
--	---

Directive 90/269/EEC of 29 May 1990 on the minimum health and safety requirements for the manual handling of loads where there is a risk particularly of back injury to workers

Spain	<p>Real Decreto número 487/97 de 14/04/1997, sobre disposiciones mínimas de seguridad y salud relativas a la manipulación manual de cargas que entrañe riesgos, en particular dorso lumbares, para los trabajadores BOE n° 97 de 23/04/1997 Página 12926 (Marginal 8670) ¹⁴⁴</p>
Italy	<p>Decreto legislativo del 19/09/1994 n. 626, attuazione delle direttive 89/391/CEE, 89/654/CEE, 89/655/CEE, 89/656/CEE, 90/269/CEE, 90/270/CEE, 90/394/CEE e 90/679/CEE riguardanti il miglioramento della sicurezza e della salute dei lavoratori sul luogo di lavoro Supplemento ordinario n. 141 alla Gazzetta Ufficiale - Serie generale - del 12/11/1994 n. 265 ¹⁴⁵</p> <p>Decreto legislativo del 19/03/1996 n. 242, modifiche ed integrazioni al decreto legislativo 19 settembre 1994, n. 626, recante attuazione di direttive comunitarie riguardanti il miglioramento della sicurezza e della salute dei lavoratori sul luogo di lavoro Supplemento ordinario n. 75 alla Gazzetta Ufficiale - Serie generale - del 06/05/1996 n. 104 ¹⁴⁶</p>
France	<p>Décret Numéro 91-451 du 14/05/1991 relatif à la prévention des risques liés au travail sur des équipements comportant des écrans de visualisation Journal Officiel du 16/05/1991, page 6497 ¹⁴⁷</p> <p>Décret n° 92-958 du 03/09/1992 relatif aux prescriptions minimales de sécurité et de santé concernant la manutention manuelle de charges comportant des risques, notamment dorso-lombaires, pour les travailleurs et transposant la directive (CEE) Numéro 90-269 du Conseil du 29/05/1990 Journal Officiel du 09/09/1992, page 12420 ¹⁴⁸</p> <p>Arrêté ministériel du 19/03/1993 fixant la liste des équipements de protection individuelle qui doivent faire l'objet des vérifications générales périodiques prévues à l'article R.233-42-2 du code du travail Journal Officiel du 28/03/1993, page 5354 ¹⁴⁹</p>

¹⁴² Dutch Law amending the national law on active implants and Medical Devices, and the European law on medical devices 2007/47 / EC.

¹⁴³ Amendment of the Dutch Law on active implantable medical devices

¹⁴⁴ Spanish Law on health and safety requirements for manual handling of load

https://www.boe.es/diario_boe/txt.php?id=BOE-A-1997-8670

¹⁴⁵ Italian Law on the implementation of the European Directives 89/391 / EEC, 89/654 / EEC, 89/655 / EEC, 89/656 / EEC, 90/269 / EEC, 90/270 / EEC, 90/394 / EEC and 90/679 / EEC concerning the improvement of workers' safety and health in the workplace

<http://www.mit.gov.it/mit/site.php?p=normativa&o=vd&id=321>

¹⁴⁶ Italian Law that amends national law for implementing the European Community directives on the improvement of safety and health conditions at the workplace

¹⁴⁷ French Law on the prevention of work-related hazards on equipment with display screens

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000537417&categorieLien=id>

¹⁴⁸ French Law on safety and health requirements for the manual handling of loads

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000178166>

¹⁴⁹ French Law concerning personal protective equipment <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000730566>

	Arrêté ministériel du 12/11/1993 modifiant l'arrêté du 19/11/1990 relatif aux solvants d'extraction utilisés dans la fabrication des denrées alimentaires ou de leurs ingrédients Journal Officiel du 17/12/1993, page 17581 ¹⁵⁰
UK	The Management of Health and Safety at Work Regulations 1992 S.I. n° 2051 of 1992 ¹⁵¹ The Manual Handling Operations Regulations 1992 S.I. n° 2793 of 1992 ¹⁵² The Management of Health and Safety at Work Regulations (Northern Ireland) 1992 Statutory Rules of Northern Ireland n° 459 of 1992 ¹⁵³
Slovenia	Pravilnik o zagotavljanju varnosti in zdravja pri ročnem premeščanju bremen ¹⁵⁴
Poland	Rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 30 maja 1996 r. w sprawie przeprowadzenia badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy ¹⁵⁵ Ustawa z dnia 23 maja 1991 r. o związkach zawodowych ¹⁵⁶ Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy ¹⁵⁷ Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 14 marca 2000 r. w sprawie bezpieczeństwa i higieny pracy przy ręcznych pracach transportowych ¹⁵⁸
Netherlands	Besluit van 27/01/1993, Staatsblad nummer 68 van 1993 ¹⁵⁹ Besluit van 10/12/1992, Staatsblad nummer 677 van 1995 ¹⁶⁰ Besluit houdende regels in het belang van de veiligheid, de gezondheid en het welzijn in verband met de arbeid (Arbeidsomstandighedenbesluit) van 15/01/1997, Staatsblad nummer 60 van 1997 ¹⁶¹ Besluit van de Staatssecretaris van Sociale Zaken en Werkgelegenheid, Directie Arbeidsomstandigheden, Arbo/AIS 9701436 tot vaststelling van beleidregels op het gebied van de Arbeidsomstandighedenwetgeving (Beleidsregels arbeidsomstandighedenwetgeving) van 27/06/1997, uitgegeven als supplement bij de Staatscourant van 27/06/1997 ¹⁶²

¹⁵⁰ French Law on extraction solvents for foodstuff production

¹⁵¹ <http://www.legislation.gov.uk/uksi/1992/2051/contents/made>

¹⁵² <http://www.legislation.gov.uk/uksi/1992/2793/contents/made>

¹⁵³ <http://www.legislation.gov.uk/nisr/2000/388/made>

¹⁵⁴ Slovenian Laws on safety and health requirements for manual handling of loads <https://www.uradni-list.si/1/content?id=57464>

¹⁵⁵ Polish Law on the medical examination, medical certificates and preventive health care for employees

¹⁵⁶ Polish Law regarding Trade Unions

¹⁵⁷ Polish Law on general safety and health at work

¹⁵⁸ Polish Law on occupational health and manual handling safety

¹⁵⁹ Dutch Law

¹⁶⁰ Dutch Law

¹⁶¹ Dutch Law on Working Conditions

¹⁶² Dutch Law establishing Policy Working Laws

4 Legislation in application domains

Legal aspects from the application domains of Transport and Logistics and eHealth are analysed in this section. The law and regulations studied in this document belong to local, national and international administrations. These regulations are focused on the legal aspects to arise when developing the pilots.

We consider that the two key national legislations for the different pilots are the Spanish and Italian ones. INTER-IoT will deploy the pilot associated with transport and logistics and m-health in these two countries respectively. Additionally, the INTER-Domain use case that will merge both pilots and will add other components (e.g. Smart city platform) will be deployed in Spain or in Italy.

On the other hand, if the open call brings a third party related with transport and logistics or with m-health. The National legislation in the country of the third party will need to be reviewed in order to cope with its own legislation. In any case, European legislation associated with IoT and the referenced application domains have been studied and analysed.

4.1 Transport and port logistics

In this section, transport and port logistics laws and regulation are being presented. The context of this law relate especially to the Spanish and Italian logistics sector as well as the European and international environment. An analysis of the law and regulation is required in order to develop the different pilots composing the Inter-LogP product. Laws concerning ports and safety are being analysed in this context.

In the national scope we have selected Spain and Italy because INTER-LogP pilot will be deployed in Valencia, and Italy, because some of the INTER-Domain pilots will be deployed in Italy so every activity have to comply with Italian and Spanish regulations. On the other hand we have reviewed the European legislation associated with transport and logistics and how it may affect IoT platform deployment and operation.

Table 3. International Legislation on Logistics and Transport

According to	Legislation	Scope
Logistics	Real Decreto Legislativo 2/2011 , Refunded text of Ports and Merchant Marine Law of Spain. ¹⁶³	Determining and classifying ports that are under competency of the State's general administration. Regulate the planning, construction, organization, managing, economic and financial politic of the mentioned. Regulate the services of the ports. Determining the Port Authorities general structure. Establish the normative framework of the Merchant Marine. Regulate Merchant Marine own administration.
Logistics	Legge 84/94 Riordino della legislazione in materia portuale ¹⁶⁴	The current Italian national port legislation (l.n. 84/1994) appears by now, from several perspectives, unsuitable to a modern idea of port, as "passage" of economic trades, element of a wider logistic chain. This article – starting from the exam of an interesting draft bill recently presented to the Italian Parliament – intends to underline the main critical aspects of the mentioned legislation (concerning, for example, the unclear role of the Port Authorities and the need of a real financial autonomy for these public bodies, the complexity of the port planning model, the not well-regulated connection between public and private interests; the lack of a sufficient logistics system, etc.), pointing out possible legal solutions able to increase competitiveness and effectiveness of Italian harbours system, which still shows a relevant deficit compared to the north Europe and Mediterranean ports.
Logistics	Real Decreto 58/1994 , guarantee of essential port services that are competency of Ports, Port Authorities and Stevedores societies ¹⁶⁵	This Royal Decree establishes and guarantees the capabilities of essential port services in strike situations that affect to the "Organización de Trabajos Portuarios" personnel, which are capable and in charge of the ports services.

¹⁶³ <https://www.boe.es/buscar/doc.php?id=BOE-A-2011-16467>

¹⁶⁴ http://www.assoporti.it/views/view_legge_84

¹⁶⁵ https://www.boe.es/diario_boe/txt.php?id=BOE-A-1994-1498

Logistics	International convention for the Safety of Life at Sea (SOLAS), 1974 ¹⁶⁶	The main objective of the SOLAS Convention is to specify minimum standards for the construction, equipment and operation of ships, compatible with their safety. Flag States are responsible for ensuring that ships under their flag comply with its requirements, and a number of certificates are prescribed in the Convention as proof that this has been done. Control provisions also allow Contracting Governments to inspect ships of other Contracting States if there are clear grounds for believing that the ship and its equipment do not substantially comply with the requirements of the Convention - this procedure is known as port State control. The current SOLAS Convention includes Articles setting out general obligations, amendment procedure and so on, followed by an Annex divided into 12 Chapters.
Logistics	Real decreto 393/1995 , de 1 de marzo, por el que se aprueba el Reglamento general de Practicaje, de conformidad con lo establecido en la Ley de Puertos del Estado y de la Marina Mercante ¹⁶⁷	Regulation of the port service of piloting and the regulation of the requirements that pilots need to fulfil so as to guarantee an adequate professional qualification, service order for maritime reasons and civil responsibility derived from such port service. As well as the sanctions and infractions that can be derived from supplying such service.
Logistics	Real Decreto 145/1989 , de 20 de enero, por el que se aprueba el Reglamento Nacional de Admisión, Manipulación y Almacenamiento de Mercancías Peligrosas en los Puertos ¹⁶⁸	As a result of the large increase in the transport of dangerous goods in the last decades, both the United Nations Organization and the International Maritime Organization (IMO) group of experts in these activities have carried out Various actions in order to provide the Administrations with instruments and guidelines to avoid or mitigate damages to people and goods and to regulate this important transport without risk to the ships and their crews. Among the standards recommended by IMO, which are applicable to ports, are those contained in the document "Safety in the Transport, Handling and Storage of Dangerous Goods in Port Areas", which is an index which recommends that it be developed in the form of Regulations in the ports of the different countries.

¹⁶⁶ [http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-\(SOLAS\),-1974.aspx](http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx)

¹⁶⁷ <https://www.boe.es/buscar/doc.php?id=BOE-A-2007-6237>

¹⁶⁸ https://www.boe.es/diario_boe/txt.php?id=BOE-A-1989-3496

Logistics	Ley 38/2015 , de 29 de septiembre, del sector ferroviario ¹⁶⁹	<p>The purpose of this law is the regulation, in the field of State competence, of railway infrastructures, safety in rail traffic and the provision of rail passenger and freight transport services and those Which are provided to railway undertakings in service facilities, including auxiliary and auxiliary facilities.</p> <p>The provisions of this law shall not apply to those modes of transportation that use cable or cables, tractors and carriers and do not have a fixed road, which shall be governed by its specific regulations</p>
Logistics	Ley 16/1987 , de 30 de julio, de Ordenación de los Transportes Terrestres ¹⁷⁰	<p>The road transport, considered as such that are carried out in motor vehicles or vehicle combinations that run without a fixed road, and without fixed means of energy collection, by all kinds of land, urban or long-distance , Of public character and, also, of the private character when the transport is public.</p> <p>The transport by rail, considering as such those that are realized by means of vehicles that circulate by a fixed rolling way that serves them of support and of guiding.</p> <p>The auxiliary and complementary activities of transport, considered as such, for the purposes of this law, those carried out by transport agencies, freight forwarders, logistics operators, warehousemen and passenger transport stations and centres Transport and logistics of goods by road or multimodal. Also, this consideration will be the lease of road vehicles without driver.</p> <p>Transports carried out by trolley buses, as well as those carried out in cable cars or other means in which traction is made by cable, and in which there is no fixed road, shall be subject to the provisions of the titles Preliminary and first of the present Law, being governed in the rest by its specific norms.</p> <p>However, the rules laid down in the third additional provision shall apply to cable transport.</p>
Logistics	Ley 29/2003 , de 8 de octubre, sobre mejora de las condiciones de	Modifies the law of Land Transport Ordinance so as to improve the conditions of competition and safety in the road transport market.

¹⁶⁹ <https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10440>

¹⁷⁰ <https://www.boe.es/buscar/act.php?id=BOE-A-1987-17803>

	competencia y seguridad en el mercado de transporte por carretera, por la que se modifica, parcialmente, la Ley 16/1987, de 30 de julio, de Ordenación de los Transportes Terrestres ¹⁷¹	
Logistics	Real Decreto 487/1997, de 14 de abril , sobre disposiciones mínimas de seguridad y salud relativas a la manipulación manual de cargas que entrañe riesgos, en particular dorso lumbares, para los trabajadores ¹⁷²	This Royal Decree establishes the minimum safety and health requirements for the manual handling of loads involving risks, particularly back pain, for workers. The provisions of Law 31/1995, of November 8, on Prevention of Occupational Risks, will be fully applied to the whole scope referred to in the previous section.
Logistics	DIRECTIVE 2003/59/CE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 July 2003 on the initial qualification and periodic training of drivers of certain road vehicles for the carriage of goods or passengers, amending Council Regulation (EEC) No 3820/85 and Council Directive 91/439/EEC and repealing Council Directive 76/914/EEC ¹⁷³	This directive imposes a system of compulsory initial qualification as well as periodic training (35 hours every 5 years) for all professional truck and coach drivers in Europe. In particular, the directive, in its Annex 1, provides that all professional drivers should be trained so as to avoid any improper use or tampering of a compulsory device always to be found on board a lorry: the digital tachograph.
Logistics	REGULATION (EC) No 561/2006 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March	This regulation provides the main social rules applicable to professional road transport. It notably includes, maximum driving and resting times (driving time: 9 hrs/day,

¹⁷¹ <https://www.boe.es/buscar/doc.php?id=BOE-A-2003-18681>

¹⁷² <https://www.boe.es/buscar/act.php?id=BOE-A-1997-8670>

¹⁷³ <http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32003L0059>

	2006 on the harmonization of certain social legislation relating to road transport and amending Council Regulations (EEC) No 3821/85 and (EC) No 2135/98 and repealing Council Regulation (EEC) No 3820/85 ¹⁷⁴	exceptionally 10 hrs/day, twice a week maximum; resting time: 9 hrs minimum/day + 1 break of 45 min. after 4.5 hrs. of driving). These rules must be taken into consideration by any IoT-based driving decision-making aid.
Logistics	Directive 2002/15/EC of the European Parliament and of the Council of 11 March 2002 on the organization of the working time of persons performing mobile road transport activities ¹⁷⁵	This directive provides compulsory rules on maximum working time (which goes beyond simply driving) as well as on minimum resting times (max. 60 hrs/week with an average 48 hrs. max in 4 consecutive months).

¹⁷⁴ <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32006R0561>

¹⁷⁵ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0015>

4.2 eHealth

Developments in mobile communication and its subsequent widespread in many field of application, has promoted the emergence of new services for medical monitoring and surveillance of citizens, called mobile Health, as dissemination of health-related information for prevention purposes, remote diagnosis and treatment of certain diseases, training of medical and health assistants, home care of patients and conduct research and studies using regularly updated databases.

The World Health Organization (WHO) defines mobile Health very broadly as “medical and public health practice supported by mobile devices such as mobile phones, patient monitoring devices, personal digital assistants (PDAs) and other wireless devices”

Despite the great possibility of development of mobile Health, in Europe is still in a very largely experimental phase and European legal landscape is too fragmented as it is largely dominated by individual State rules.

The technology is already present and used in many sectors, it is becoming increasingly common to be used to provide remote care to patients and from the point of view of quality of care provided both in a hospital or outpatient setting and at home our European health operators, as well as those in the electronic communications sector, suggest that one of the main reasons lies in insufficient rules and an inadequate national and European legal framework.

The development of mobile Health in Europe implies access to the European market by medical device manufacturers or distributors and European States must be able to exercise their control over the quality of medical devices circulating in Europe and ensure their safety and each European State has specific requirements with regard to protecting the health of its citizens.

Europeans have made an effort to harmonize their national laws, within the European Union and to adopt a body of common rules.

The national administrative, regulatory, and legal provisions sets conditions for medical devices, certification and control procedures intended to verify that the medical devices offer patients, users, and third parties, a high level of protection and that they attain the performances assigned to them by their manufacturer and they set a distinction between a device itself and its accessory or accessories.

A medical device is any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes. Medical devices shall be used following the instructions for its proper application and with the purpose intended by the manufacturer. A medical device does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but it may be assisted in its function by such means.

As a nutritional outpatient we follow ethics rule code, newly approved by the national law, adding chapters on technologies and innovation in the health field.

Following the updated Italian Medical Ethics Code approved in May 2014, every operator participates and collaborates with the health care organization in order to constantly improve the quality of services offered to subjects and in general to the community: The health care operator using internet of things' tools, ensures the acquisition of informed consent, the

protection of confidentiality and guarantees relevance of collected data and, within its outpatient competence, the safety of data. The healthcare operator, in the use of technologies and communication of clinical data, is pursuing the clinical appropriateness and make decisions in respect of any existing multidisciplinary contributions, ensuring the conscious participation of the subject. For the prevention and in general under any treatment or clinical surveillance, we refer to appropriateness, effectiveness and safety, respecting personal rights.

The development of mobile Health in Europe implies the ability to collect, retain, and transfer personal information which may be contain of subjects' private lives, that could affect their fundamental rights as written by Article 12 of the Universal Declaration of Human Rights, and more specifically in the European context, by the European Convention for the Protection of Human Rights.

Directive 2009/136/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector, sets a specific standard to any entity worldwide that wishes to store or access information stored in devices of users located in the European Economic Area.

The essential requirements of medical devices is to satisfy national standards, which themselves were adopted in accordance with harmonized European standards and data collected and processed for preventive medicine purposes, medical diagnostics, treatments or even management of healthcare services. The processing of sensitive data may be authorized under national laws, provided that such processing is performed by a healthcare practitioner subject to an obligation of professional confidentiality under national law (those information may only be collected after the interested parties have been informed).

In many European states, work done in pursuit of the public interest justifies collection and processing of personal health information, and folders created must be accurate, updated, and stored in conditions of guaranteed security. For a duration not longer than the necessary purpose for which said data has been collected, in the setting of procedures for evaluating care delivered by healthcare professionals, hospitals, or care-giving organizations.

We are waiting for the entry into force of Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data that repealing Directive 95/46/EC (general Regulation on data protection).

Table 4. National Legislation on eHealth

According to	Legislation	Scope
eHealth	Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices , Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market ¹⁷⁶	It is necessary to clarify that software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, is a medical device. Software for general purposes when used in a healthcare setting is not a medical device. Particular care should be taken to ensure that the reprocessing of medical devices does not endanger patients' safety or health. It is therefore necessary to provide clarification on the definition of the term 'single use', as well as to make provision for uniform labelling and instructions for use. Moreover, the Commission should engage in further analysis in order to see if additional measures are appropriate to ensure a high level of protection for patients.
Telemedicine	COMMUNICATION Brussels, 4.11.2008 ¹⁷⁷	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society.
Medical Devices	Green paper on m-health Brussels, 10.4.2014 ¹⁷⁸	The Commission is looking to support the implementation of m-Health in the EU.
eHealth	eHealth Action Plan 2012-2020 ¹⁷⁹	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Innovative healthcare for the 21st century.

¹⁷⁶ <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32007L0047>

¹⁷⁷ <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52008DC0689>

¹⁷⁸ <https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth>

¹⁷⁹ <https://ec.europa.eu/digital-single-market/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century>

eHealth	Direttiva 2007/47/Ce del Parlamento Europeo e del Consiglio ¹⁸⁰	Transposition of the EU regulation Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 for ensure that the reprocessing of medical devices does not endanger patients' safety or health.
eHealth	Decreto 20 febbraio 2007 Approvazione della Classificazione Nazionale dei dispositivi medici (CND) ¹⁸¹	Changes And Additions to the decree of 20 February 2007 on "New Mode for The Expected requirements for Registration of Active implantable devices as well as for inclusion in the Repertory of medical devices."
Medical Devices	Real Decreto 1591/2009 , de 16 de octubre, por el que se regulan los productos sanitarios ¹⁸²	This Royal Decree transposes Directive 2007/47 / EC of the European Parliament and of the Council of 5 September 2007 amending Council Directive 90/385 / EEC on the approximation of the laws, regulations and administrative Member States on active implantable medical devices, Council Directive 93/42 / EEC concerning medical devices and the Directive 98/8 / EC on the placing on the market of biocidal products, incorporating both directives in a single text.
eHealth	Ley 16/2003 , de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud ¹⁸³	Law 16/2003, of cohesion and quality of the National Health System (SNS), orders the Ministry of Health, Social Services and Equality (MSSSI) to develop health card systems and exchange of clinical information and electronic prescription In the SNS. Since the promulgation of the law, a series of lines of work have been developed in the SNS as a whole, under the coordination of the MSSSI, whose purpose is to respond to the health information needs of citizens when they move from an autonomous community to another and need assistance.
Medical Devices	Real Decreto 1616/2009 , de 26 de octubre, por el que se regulan los productos sanitarios implantables activos ¹⁸⁴	This Royal Decree aims to regulate active implantable medical devices and in particular: the health guarantees of the products and the essential requirements they must meet, procedures for the granting of licenses, or the requirements for the placing on the market and use of medical devices for a particular purpose.

¹⁸⁰ <http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32007L0047>

¹⁸¹ <http://gazzette.comune.jesi.an.it/2007/86/10.htm>

¹⁸² <https://www.boe.es/buscar/doc.php?id=BOE-A-2009-17606>

¹⁸³ <https://www.boe.es/buscar/act.php?id=BOE-A-2003-10715>

¹⁸⁴ https://www.boe.es/diario_boe/txt.php?id=BOE-A-2009-17607

5 IoT good practices and recommendations

5.1 Digital Single Market (DSM) of European Union

The European Commission acknowledges the need for focused research on Internet of Things (IoT). IoT has the potential to enhance Europe's competitiveness and is an important driver for the development of an information based economy and society.

For the past six years, the European Commission has been cooperating actively with Member States and third countries towards the development and future deployment of the IoT technology. The European Commission works on creating the European Single market for human-centred IoT and invests in fostering an innovative IoT ecosystem.

The future design of the Internet of Things applications will depend on the development of advanced platform architectures for smart objects, embedded intelligence, and smart networks. Most of today's IoT systems are mainly focused on sensors, whereas actuation and smart behaviour will be the key points in the future.

Novel interfaces combined with artificial intelligence and flexible self-organising platforms are promising areas. Smart agriculture, smart cities, smart industries as well as sustainable reverse logistics, smart water management and smart grids are strategic IoT areas for the EU.

The Digital Single Market (DSM) Strategy, adopted in May 2015, leads Europe a step further in accelerating developments on IoT. It underlines the need to avoid fragmentation and to foster interoperability for the technology to reach its potential. To fulfil these needs the European Commission is putting forward three concrete actions via the recent Digitising European Industry initiative:

- a single market for IoT
- a thriving IoT ecosystem
- a human-centred IoT approach

In order to support IoT innovation, Europe promotes the idea of open and easily accessible IoT platforms, with different initiatives like IERC in the past and currently AIOTI, and IoT-EPI. Additionally the website <http://www.open-platforms.eu> proposed to keep a catalogue of such open platforms, mainly in the area of IoT.

5.2 Article 29 Data Protection Working Party

This working party was set up under article 29 of Directive 05/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship).

The working party published the opinion 8/2014 on 16th September 2014 on Recent Development on the Internet of Things. This opinion stated that the expected benefits of IoT

must also respect the many privacy and security challenges which can be associated. Questions such as vulnerability of devices, data losses, infection by malware, unauthorized access to personal data, intrusive use of wearable devices, unlawful surveillance were exposed as risks that stakeholders in IoT must address to attract prospective end-users of the products or services.

The WP29 has decided to take the issue further by adopting this opinion. In this way, it intends to contribute to the uniform application of the legal data protection framework in the IoT as well as to the development of a high level of protection with regard to the protection of personal data in the EU. Compliance with this framework is key to meeting the legal, technical but also, since it relies on the qualification of data protection as a fundamental human right, the societal challenges described above.

Table 5. WP29 last publications

Table 5. WP29 last publications	
Opinion 8/2014 on the on Recent Developments on the Internet of Things	Published on September 16, 2014
This opinion identifies the main data protection risks that lie within the ecosystem of the IoT before providing guidance on how the EU legal framework should be applied in this context. The Working Party supports the incorporation of the highest possible guarantees for individual users at the heart of the projects by relevant stakeholders. In particular, users must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific. To help them meet this end, the Working Party designed a comprehensive set of practical recommendations addressed to the different stakeholders concerned (device manufacturers, application developers, social platforms, further data recipients, data platforms and standardisation bodies) to help them implement privacy and data protection in their products and services.	AIOTI WG4

5.3 Alliance for Internet of Things Innovation (AIOTI)

The Alliance for Internet of Things Innovation (AIOTI)¹⁸⁵ was initiated by the European Commission on the 26th of March 2015 at the Net Futures 2015 Conference, with the aim to strengthen the dialogue and interaction among Internet of Things (IoT) players in Europe, and to contribute to the creation of a dynamic European IoT ecosystem to speed up the take up of IoT.

AIOTI builds on the work of the IoT European Research Cluster (IERC) and expands activities towards innovation within and across industries. This also offers an opportunity to discuss legal obstacles to further IoT take up, and to forge consensus.

¹⁸⁵ <http://www.aioti.org/>

Other objectives of the Alliance include:

- fostering experimentation, replication, and deployment of IoT and supporting convergence and interoperability of IoT standards;
- gathering evidence on market obstacles for IoT deployment;
- mapping and bridging global, EU, and member states' IoT innovation activities.

With 500 active members and more than 1500 high level experts, members of the Alliance include key IoT industrial players - large companies, successful SMEs and dynamic start-ups - as well as well-known European research centres, universities, associations and public bodies.

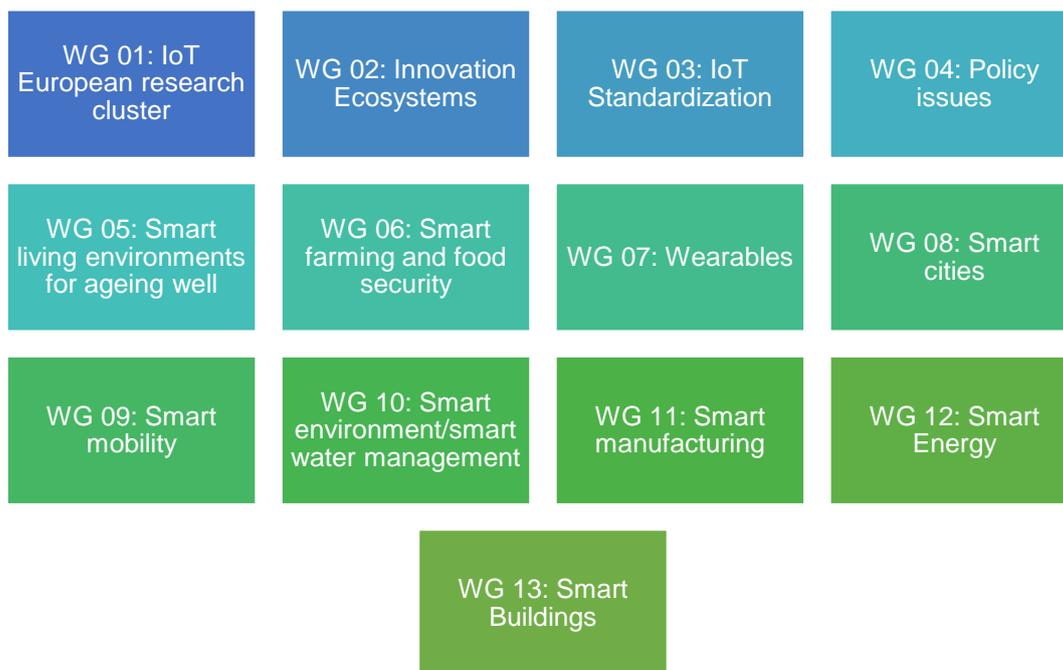


Figure 5: Working Groups AIOTI

Most of the AIOTI activities are carried out through Working Groups, which focus on well-defined areas of development. These include vertical Working Groups in research and innovation, policy issues and proposed standards, as well as horizontal, cross-disciplinary activities focused on hot topics in the field.

At the 3rd General Assembly of the AIOTI initiative, which took place on the 30th of May in Berlin, the members decided to work on transforming the Alliance into a legal entity. The AIOTI converted to a European association based in Brussels on 22 September 2016.

The legal entity maintains a close partnership with the European Commission on policy recommendations and on building the strategy for the research and innovation agenda for the future IoT funding programme.

AIOTI published in October 2015 a policy document (working group 4) which highlighted a number of issues and recommendations on the areas of privacy, security, liability and net neutrality. The AIOTI policy paper took the outcome of the IoT policy review initiated by the European Commission, concluded in May 2013. Both documents are taken into account in the project.

Table 6. AIOTI and EC last publications

AIOTI and EC last publications	
AIOTI WG4 Policy paper	Published on October 15, 2015
This document represents the initial output of the Policy group, WG4 of AIOTI and highlights a number of key issues related to privacy, security, liability and net neutrality. In so doing, this group also makes a number of recommendations to further inform both the policy debate and the activities of the Horizon 2020 Large Scale Pilots due to commence in 2016. They also make reference to other relevant stakeholders that are carrying out important activity in this field and which should be linked to the work of this WG.	AIOTI WG4
Europe's policy options for a dynamic and trustworthy development of the Internet of Things	Published on May 31, 2013
This report commissioned by the European Commission aims to inform the development of a consistent European policy stance capable of fostering a dynamic and trustworthy IoT that helps meet key European challenges.	

5.4 IERC-European Research Cluster on the Internet of Things

The aim of European Research Cluster (IERC)¹⁸⁶ on the Internet of Things was to address the large potential for IoT-based capabilities in Europe and to coordinate the convergence of ongoing activities, especially the IoT projects funded by the 7th European research framework program (FP7) and H2020.

The EU-funded projects are: UNIFY-IoT, BIG IoT, VICINITY, INTER-IoT, symbloTe, TAGITSMART, bloTope, AGILE, Be-IoT, WAZIUP, FESTIVAL, BeInCPPS, ESPRESSO, WISE IoT, FIESTA-IoT, iKaaS, ProaSense, MANTIS, ARMOUR, BIG IoT, VICINITY, INTER-IoT, symbloTe, TAGITSMART, bloTope, AGILE, Be-IoT, CLOUT, VITAL, SOCIOTAL, RERUM, COSMOS, CITY PULSE, ALMANAC, SMARTIE, SMART-ACTION, FITMAN, ASPIRE, CASCADAS, CONFIDENCE, CuteLoop, DACAR, EPoSS, EU-IFM, EURIDICE, GRIFS, HYDRA, IMS2020, Indisputable Key, iSURF, LEAPFROG, PEARS Feasibility, PrimeLife, RACE networkRFID, SMART, StoLPaN, SToP, TraSer, WALTER, IOT-A, INTREPID, IOT@Work, ELLIOT, SPRINT, NEFFICS, IOT-I, CASAGRAS2.

Wherefore, IERC has involved experts working in industry, research, and academia to provide their vision on IoT research challenges, enabling technologies and the key applications, which are expected to arise from the current vision of the IoT.

The aim of bringing together EU-funded projects is to define a common vision and the IoT technology and development research challenges at the European level in the view of global development. For IERC, the rationale for IoT is to address the large potential for IoT-based

¹⁸⁶ <http://www.internet-of-things-research.eu/>

capabilities in Europe - coordinate/encourage the convergence of ongoing work on the most important issues - to build a broadly based consensus on the ways to realise IoT in Europe.

IERC also seeks to facilitate the knowledge sharing at the global level and will encourage and exchange best practices and new business models that are emerging in different parts of the world. In this way, measures accompanying research and innovation efforts are considered to assess the impact of the Internet of Things at the global and industrial level, as well as at the organisational level.

Linking IERC activities with the activities of the IoT Expert Group in order to minimise overlaps and maximize synergies and contributing to the overall IoT objectives, the main objectives of the IERC are to:

The main objectives of the IERC were to:

- Establish a cooperation platform and develop a research vision for IoT activities in Europe and become a major entry and contact point for IoT research in the world.
- Define an international strategy for cooperation in the area of IoT research and innovation and have an overview of the research and innovation priorities at the global level.
- Coordinate the cooperation activities with other EC Clusters and ICT projects.
- Coordinate and align the SRIA agenda at the European level with the developments at the global level.
- Organise debates/workshops leading to a better understanding of IoT and Future Internet, 5G, cloud technology, and adoption.

Additionally, the IERC is actively involved in ITU-T Study Group 13, which leads the work of the International Telecommunications Union (ITU) on standards for next generation networks (NGN) and future networks and has been part of the team which has formulated the important definitions about Internet of Things.

In following table there are last publications IERC.

Table 7. IERC last publications

IoT Digital Value Chain Connecting Research, Innovation and Deployment	IERC Cluster SRIA 2016.
Building the Hyperconnected Society - IoT Research and Innovation Value Chains, Ecosystems and Markets	IERC Cluster Book 2015.
Internet of Things beyond the Hype: Research, Innovation and Deployment	IERC Cluster SRIA 2016.
IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps	IERC Position Paper 2015
IoT Governance, Privacy and Security Issues	IERC Position Paper 2015
Position Paper on Standardization for IoT technologies	IERC Position Paper 2015
EU-China Joint White Paper on Internet-of-Things Identification	IERC Position Paper 2015

5.5 IoT European Platform Initiative (IoT-EPI)

IoT-EPI¹⁸⁷ is a European Initiative addressing the new EU-funded H2020 programs about IoT platform development.

Its main objective is to build a vibrant and sustainable IoT ecosystem in Europe.

At the core of IoT-EPI are the seven research and innovation projects: Inter-IoT, BIG IoT, AGILE, symbloTe, TagItSmart!, VICINITY and bloTope.



Figure 6: Innovation IoT projects H2020

With a total funding of 50 M€ and a partner network of 120 established companies and organisations these projects develop innovative platform technologies and foster technology adoption through community and business building.

¹⁸⁷ <http://iot-epi.eu>

5.6 ENISA

The European Union Agency for Network and Information Security (ENISA)¹⁸⁸ is an agency dedicated to preventing and addressing network security and information security problems and a centre of expertise for cyber security in Europe.

Since 2004, ENISA assists the Commission, the Member States and private sector in meeting the requirements of network and information security (NIS). It's as a centre of expertise for both Member States and EU Institutions to seek advice on matters related to NIS. ENISA also contribute in updating and developing European policy and law on matters relating to NIS. This cooperation includes, the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies, CSIRTs cooperation and capacity building, but also studies on secure Cloud adoption, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, and identifying the cyber threat landscape, and others.

The activities of ENISA are focused mainly in three areas: recommendations in the field of NIS, activities that support policy making and implementation, and direct collaboration with operational teams throughout the EU.

The ENISA strategic objectives arise from the NIS needs faced by member states, relevant communities and private companies. These objectives can be grouped into 5 categories:

- **Expertise:** Study the digital environment to anticipate and detect new NIS challenges that can be dangerous for the EU.
- **Policy:** Assist the European Commission and member states in promoting a NIS policy, and help to develop new legislation related to NIS.
- **Capacity:** Assist the European Union and member states in maintaining and enhancing their NIS capacities.
- **Community:** Promote the cooperation of the NIS community at EU level among European Union bodies, Member States and relevant NIS stakeholders, including the private sector.
- **Enabling:** Strengthen the ENISA's impact at international level by expanding their relationships with NIS community and with relevant publications on the subject.

About IoT and Smart Infrastructures, ENISA develops guidance to secure from cyber threats, by highlighting good security practices and proposing recommendations to operators, manufacturers and decision makers. The term Smart Infrastructures includes several domains of activity, such as energy, public transport, and public safety. All of them have equipment that controls critical systems, and therefore must be protected from cyber-attacks. The usage of software-controlled devices that interact with the physical world, bring new risks on the economy and on the safety of citizens.

ENISA is focused in three domains where systems migrates to Smart environments by deploying IoT, remote management, and big data to improve the quality of service.

The first one is Smart Cities, whose main objective is interconnect different operators and service in order to improve functionalities and the quality of life of citizens. In this case, the cyber security is very relevant as all kind of systems (energy, public transport, public safety,

¹⁸⁸ <https://www.enisa.europa.eu>

etc.) rely on Information and Communication Technology (ICT) architecture to retrieve, process and exchange data.

Another booming sector is Smart Homes, which is a clear case of IoT application, since the goal is to connect all the devices and systems of a home to enhance the functionalities (e.g. reduced energy consumption, dynamic heating, etc.). This involves rely on third-party technologies and components, so ENISA aims at increasing their resilience against cyber threats by promoting security by design, i.e. the integration of security at every stage of the lifecycle of IoT products and services.

Finally, ENISA it's working on Smart Cars and Intelligent Road Systems. These two domains rely on the Internet of Things, and cyber threats have real consequences on the safety of citizens.

In Table 8 there are last publications related to security issues in Internet of Things.

Table 8. ENISA last publications

Architecture model of the transport sector in Smart Cities	Published on January 12, 2016
The main objective of this study is to model the architecture of the transport sector in SCs and to describe good cyber security practices of IPT operators. The good practices are put into a relationship with different city maturity levels. This...	
Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations	Published on January 12, 2016
This study proposes a pragmatic approach that will highlight the critical assets of Intelligent Public Transport systems. It gives an overview of the existing security measures (good practices) that could be deployed to protect these critical assets...	
Cyber security and resilience for Smart Hospitals	Published on November 24, 2016
This study proposes key recommendations for hospital information security executives and industry to enhance the level of information security in Smart Hospitals. Through the identification of assets and the related threats when IoT components are...	

5.7 The European GNSS Agency

The European GNSS Agency (GSA; formerly European GNSS Supervisory Authority)¹⁸⁹ was initially established as a Community Agency on 12 July 2004, by Council Regulation (EC) 1321/2004, status amended in 2006 by Council Regulation (EC) No 1942/2006.

¹⁸⁹ <http://www.gsa.europa.eu/>

Its objective is to ensure that essential public interests are properly defended and represented in connection with European Union's satellite navigation programmes (GALILEO and EGNOS). In addition, the agency is responsible for managing and monitoring the use of the program funds, and helps the European Commission deal with any matters relating to satellite radio-navigation.

By developing a new generation of Global Navigation Satellite Systems (GNSS), Europe is opening new doors for industry development, job creation & economic growth. Galileo has the potential to become a cornerstone of the global radio navigation positioning system of the future.

GSA is currently responsible for a range of activities:

- Preparing for the successful commercialisation & exploitation of the systems, with a view to smooth functioning, seamless service provision & high market penetration;
- Ensuring the security accreditation of the system & the establishment and operation of the Galileo Security Monitoring Centres;
- Accomplishing other tasks entrusted to it by the Commission, such as managing GNSS Framework Programme Research; promotion of satellite navigation applications & services; and ensuring the certification of system components.

GNSS has a notable role as an element within smart applications and as integral to the Internet of Things. Inasmuch as the European GNSS provides a level of reliability, precision and robustness that can help expand the Internet of Things and its benefits throughout the EU and beyond. By allowing for the development of new applications, in addition to the improvement of existing applications, European GNSS will provide new avenues of economic opportunity to EU countries, businesses and citizens via IoT.

European GNSS are considering transport safety and liability solutions defined as those solutions that possess the potential to directly or indirectly cause harm to humans, destruction of the carrier vehicle, damage to external properties or environment or significant legal or economic consequences. Within this segment, all applications require a high level of confidence and resilience, which translates in five key performance parameters which are integrity, continuity, robustness, availability and accuracy. The signal authentication capability of Galileo is one of the features which can bring robustness to the applications based on geo-location. However, mature safety and liability critical applications require not only a mature GNSS industry but also an ad-hoc legal framework in place.

Table 9. GSA last publications

GSA last publications	
GNSS User Technology Report	Published on 2016
<p>This report provides an in-depth analysis of GNSS user technology as it pertains to three key macrosegments: mass market solutions; transport safety and liability-critical solutions and high precision, timing and asset management solutions. In addition, it also provides a general overview of the latest GNSS receiver technology, common to all application areas, along with a supplement on location technologies that looks beyond GNSS in the positioning landscape.</p>	

5.8 The European Telecommunications Standards Institute (ETSI)

The European Telecommunications Standards Institute (ETSI)¹⁹⁰ is the European Standards Organization (ESO) dealing with Information and Communication Technology (ICT) standards. Founded (1988), ETSI produces technical standards for both European (regulatory) and global use.

ETSI has over 800 member companies, of various sizes, from 64 countries covering 5 continents

The ETSI's member companies are a mixture of manufacturers, network operators, service and content providers, national administrations, ministries, universities, research bodies, consultancies, user organizations.

Founder of several major international initiatives including

- 3GPP (evolving 3G/4G/ and soon 5G mobile system standards)
- oneM2M (creating service-layer standards for M2M). The work of oneM2M builds on the activities of ETSI committee, TC SmartM2M.
- and NFV

ETSI is involved in standardizing many of technologies associated of to connect things in the Internet of Things (IoT).

Within ETSI there are addressing various applications of M2M technology concerning to IoT: Smart appliances, Smart metering, Smart cities, Smart grids, eHealth, Intelligent Transport Systems and Wireless Industrial Automation.

Additionally ETSI provides support to aspects such as:

- Security for the IoT.
- Low power supplies in the IoT.
- Radio spectrum requirements – helping to find the necessary radio spectrum for connecting things wirelessly in the IoT.
- Embedded communications modules.

Table 10. Latest published ETSI standards on internet of things

Standard No.	Standard title.
TR 103 376	SmartM2M; IoT LSP use cases and standards gaps
TR 103 375	SmartM2M; IoT Standards landscape and future evolutions
TS 118 104	oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004 version 2.7.1 Release 2)
TS 118 101	oneM2M; Functional Architecture (oneM2M TS-0001 version 2.10.0 Release 2)
GS NGP 001	Next Generation Protocol (NGP); Scenario Definitions

¹⁹⁰ www.etsi.org

TR 118 522	oneM2M; Continuation & integration of HGI Smart Home activities (oneM2M TR-0022 version 2.0.0)
TR 118 524	oneM2M; 3GPP Release 13 Interworking (oneM2M TR-0024 version 2.0.0)
TS 118 114	oneM2M; LWM2M Interworking (oneM2M TS-0014 version 2.0.0 Release 2)
TR 118 512	oneM2M; End-to-End Security and Group Authentication (oneM2M TR-0012 version 2.0.0)
TR 118 516	oneM2M; Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies (oneM2M TR-0016 version 2.0.0)

5.9 OneM2M

oneM2M¹⁹¹ was launched in 2012 as a global initiative to ensure the most efficient deployment of Machine-to-Machine (M2M) communications systems and the Internet of Things (IoT).

oneM2M partner standards development organizations are: ARIB (Japan), ATIS (U.S.), CCSA (China), ETSI (Europe), TTA (U.S.), TTA (Korea), and TTC (Japan). Additional partners contributing to the oneM2M work include: the BBF (Broadband Forum), Continua, HGI (Home Gateway Initiative), the New Generation M2M Consortium – Japan, and OMA (Open Mobile Alliance).

Its aim is to develop technical specifications for a common M2M Service Layer that can be embedded within various hardware and software to connect the wide range of devices worldwide with M2M application servers.

oneM2M specifications provide a framework to support a wide range of applications and services such as smart cities, smart grid, connected car, home automation, public safety, and health.

Initially, oneM2M shall prepare, approve and maintain the necessary set of Technical Specifications and Technical Reports for:

- Use cases and requirements for a common set of Service Layer capabilities;
- Service Layer aspects with high level and detailed service architecture, in light of an access independent view of end-to-end services;
- Protocols/APIs/standard objects based on this architecture (open interfaces & protocols);
- Security and privacy aspects (authentication, encryption, integrity verification);
- Reachability and discovery of applications;
- Interoperability, including test and conformance specifications;
- Collection of data for charging records (to be used for billing and statistical purposes);
- Identification and naming of devices and applications;
- Information models and data management (including store and subscribe/notify functionality);
- Management aspects (including remote management of entities); and

¹⁹¹ <http://www.onem2m.org>

- Common use cases, terminal/module aspects, including Service Layer interfaces/APIs between:
 - Application and Service Layers;
 - Service Layer and communication functions.

5.10 ISO - International Organization for Standardization

ISO¹⁹² is an independent, non-governmental international organization with a membership of 163 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.

In the field of information technologies and information security management systems, we have identified the following international standards:

ISO 27001 Information technology - Security techniques - Information security management systems -- Requirements

ISO 27002 Information technology - Security techniques - Code of practice for information security controls

ISO 27009 Information technology -- Security techniques -- Sector-specific application of ISO/IEC

ISO 27011 Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO 27017 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

TR 27019 Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

ISO 29100 Information technology -- Security techniques -- Privacy framework.

ISO 29134 Information technology -- Security techniques -- Privacy impact assessment -- Guidelines

ISO 29151 Information technology -- Security techniques -- Code of practice for personally identifiable information protection

ISO 27018 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

¹⁹² <http://www.iso.org/iso/home.html>

6 Conclusions

This document contains an analysis of the European legislation related to the scope of the project. All this information will be considered during all project development phases to ensure that all products conform to legislation and recommendations.

As stated above, data security is a key concern with the Internet of Things, taking into account just how much data can be collected and how sensitive it could be (i.e. personal data, accountable data, etc.). The potential scope for damage is high. As an example, in hospitals, IoT devices can be used to track the vital information of patients, which medical practitioners can use to determine required medication. If these systems were hacked the result could potentially be life threatening. Therefore, it is very important to ensure user security, confidence and trust.

Real progress and the vast implementation of the INTER-IoT solutions can be achieved only by ensuring confidence of all parties. Therefore, convincing consumers that the use of IoT devices is safe and secure is a key activity. In order to achieve user confidence, the above legal requirements will be carefully considered when developing INTER-IoT solutions.

Firstly, the European legislation related to interoperability, security, privacy, anonymization, goods or people positioning, etc. has been analysed. All this legislation may affect the development of the project in some way, and therefore a national search of these laws has been carried out. For each of the countries that is part of the project (Spain, Italy, France, Slovenia, UK, Poland and Netherland), the law corresponding to European legislation has been sought.

However, the most important legislation needed is that related to the pilots. Therefore, specific legislation has been analysed regarding port logistics and e-health in the two countries where pilots will be implemented, Spain and Italy.

Although there is hardly any legislation at the international level, there are some recommendations and good practices established by international organizations. These recommendations have to be taken into account, since the market is usually oriented in the same direction and new standards may appear.

It is important to mention that the countries involved in the consortium have very specific laws regarding the issues of the project. This thorough analysis will be very helpful with the legislation that will come in the future. The INTER-IoT consortium will review the work done in this deliverable to ensure that the new regulations that appear in the coming years are included in the design process.