This project has received funding from the European's Union Horizon 2020 research innovation programme under Grant Agreement No. 957258

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

Ethics and Privacy manual v1

Deliverable No.	D2.3	**Due Date**	31-01-2021
Type	Report	**Dissemination Level**	Public
Version	1.00	**WP**	WP2
Description	Ethics and Privacy Protection Manual – will formally specify ways in which conformance with ethical and legal guidelines will be ensured, in line with pertinent EU (and local) documents.		

Copyright

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

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

Disclaimer

Authors

This is the list of all contributors; it is recommended to use a neutral sorting, e.g. by partner number or by alphabetical sorting of the names

Name	Partner	e-mail
Georgios Stavropoulos	CERTH	stavrop@iti.gr
Carlos Guardiola	UPV	carguaga@upv.es
Marcin Paprzycki	IBSPAN	paprzyck@ibspan.waw.pl
Ignacio Lacalle	UPV	iglaub@upv.es

History

As mentioned before, in the normal submission process, the version numbers here are in form of 0. and must always end up with 1.0*

Date	Version	Change
12-Jan-2021	0.1	ToC and task assignments
23-Jan-2021	0.4	CERTH & UPV contributions
26-Jan-2021	0.5	IBSPAN contributions
28-Jan-2021	0.8	Consolidated version
01-Feb-2021	1.0	Final version for internal review
05-Feb-2021	1.03	Final version for submission to EC

Key Data

Keywords	IoT, Ethics, privacy, legislation, regulations
Lead Editor	Georgios Stavropoulos (CERTH)
Internal Reviewer(s)	PCC

Executive Summary

The main outcome of ASSIST-IoT is the creation of a reference architecture for the next generation internet of things (NG-IoT), and along the planned technical developments and advances come a series of ethical and privacy issues that need to be tackled. Starting from distributed intelligence (or decentralized AI) and analysing its advantages over the traditional centralized artificial intelligence (AI), where all data and processes are performed on-site, and processing of large datasets (such in the case of IoT networks) requires significant resources and time. Distributed intelligence on the other hand uses multiple points of resources to achieve its goal, while at the same time involves no sensitive data exchange between the involved parties, thus enhancing the level of privacy and security.

Based on the above, the ASSIST-IoT consortium will consider and address the six key ethical issues that the European Commission (EC) has identified for IoT systems deployment, namely: (i) social justice and divide, (ii) Trust, (iii) Blurring of context, in particular the distinction private vs. public, (iv) non-neutrality of IoT metaphors, (v) agency: social contract between people and objects and (vi) autonomy: informed consent vs. obfuscation of functionality.

In order to achieve the above, an ethics framework that will guide all the operations within the project has been defined. The main point of the ethics framework is how the consortium will handle human participants (whether external on internal to the project) ensuring the compliance with ethical and legal guidelines. The framework includes the appointment of a project-wide ethics manager, that will oversee all the project actions, as well as pilot-site ethical managers, who will be responsible for the operations taking place during the pilot demonstrations, including the developments, installations and execution of them.

ASSIST-IoT participants are of two categories: (i) pilot participants, which are the people involved in the pilot demonstrations and (ii) other event participants, that includes the participants in workshops, webinars, conferences etc. (partner employees fall under the same categories, based on their participation in events). For each of these categories, special measures must be taken in order to ensure privacy and confidentiality of information. For the later, as the involved information usually contains name, email and/or photo/video, an informed consent procedure has been devised.

The case of the pilot participants is more complex, as their involvement in the pilot demonstrations may include collection of more personal data, including behavioural or physiological observations. In order to ensure compliance with regulations and guidelines and secure all personal information, a plan on how the participants will be approached and informed has been drafted. This plan will be further elaborated and be customised for the specific needs of each of the three pilot sites that are foreseen in ASSIST-IoT. In short, the plan includes the detailed information of the participant about the tasks their involvement includes, what data will be collected and processed, and of course the signing of an informed consent.

To achieve the above, ASSIST-IoT will need to comply with several legislations and directives, some of which, amongst others, are:

- The General Data Protection Regulation (GDPR)
- The Chapter of Fundamental Rights of the EU
- Directive 2006/24/EC also known as the “data retention directive”
- Regulation 2016/425 that refers to the use of personal protective equipment and more.

Compliance will all these regulations will ensure that the developed ASSIST-IoT architecture will be in accordance with future NG-IoT systems.

Design and development of a reference architecture, such as that of ASSIST-IoT, always has some potential risks which might arise during the project’s lifespan. An initial investigation of these risks from an ethical aspect has been performed and the corresponding mitigation strategies have been identified. Some indicative risks that have been identified include: (i) difficulty in ensuring data security for personal data, (ii) safety of the persons involved in the pilot demonstrations, (iii) accountability for the IoT applications regarding privacy, (iv) digital divide and more. Detailed mitigation strategies have been conceived and the list will be continuously updated as the project progresses.

Finally, ASSIST-IoT's ethical design model has been drafted. In order to ensure security and identity management, the DevSecOps methodology will be used, within the scope of work package 3 and 4, with the former laying the groundwork for the specifications and requirements and the latter providing the core enabler design for the IoT infrastructure.

.

Table of contents

List of tables

List of acronyms

Acronym	Explanation
AB	Advisory Board
AI	Artificial Intelligence
AR	Augmented Reality
CA	Consortium Agreement
CHE	Cargo Handling Equipment
DLT	Distributed Ledger Technology
DOA	Description of Action
DPO	Data Protection Officer
EC	European Commission
EM	Ethics Manager
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
H2H	Human-to-Human
H2M	Human-to-Machine
HMI	Human Machine Interaction
HTTP	Hyper Text Transfer Protocol
IoT	Internet of Things
ISC	In-service Conformity
LED	Light-emitting Diode
M2M	Machine-to-Machine
ML	Machine Learning
MLFT	Malta Freeport Terminal
MQTT	Message Queuing Telemetry Transport
MVP	Minimum Viable Product
NGIoT	Next-Generation Internet of Things
OCR	Optical Character Recognition
OECD	Organisation for Economic Co-operation and Development
OEM	Original Equipment Manufacturer

PC	Project Coordinator
PCC	Project Coordination Committee
PDF	Portable Document Format
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIC	Project Implementation Committee
PII	Personally Identifiable Information
PPE	Personal Protective Equipment
PSEM	Pilot Site Ethical Manager
QR	Quick Response code
SotA	State of the Art

1. Introduction

ASSIST-IoT aims at creating the blueprint architecture for the Next Generation Internet of Things (NGIoT). To do so, a series of technological developments are planned that will be aligned with broad and specific requirements. Both the validation and the use of the platform will entail the intervention of humans. This aspect becomes utterly important considering that one of the main traits of ASSIST-IoT is human-centricity, allowing users to exploit NGIoT capacities with ease and quality.

The fact of involving people from different perspectives (developers, end-users, research subjects, external contributors for fine-tuning the system) puts the privacy and protection in the centre of Consortium's concerns. ASSIST-IoT will continuously respect all current regulations (regional, national and European) and guidelines, ensuring maximum respect to humans' freedom and rights.

However, a detailed analysis of how this privacy protection will be achieved must be done. This deliverable (and the following iterations) aims at conducting this analysis and proposing proper solutions to ensure coverage.

The present deliverable is structured as follows:

- Section 2 provides an overview of ethical aspects in distributed intelligence in general and specifics relating to ASSIST-IoT's scenarios
- In ASSIST-IoT ethics Framework an initial definition of the ethical procedures that will be followed throughout the project's lifespan is presented
- Legal aspects describes the legal aspects of the project, referencing specific legislation that the consortium will make sure to abide by
- Data Privacy Policy in ASSIST-IoT presents the data privacy policy that will be followed, including data protection and anonymization.
- The ethical risks that have been identified so far are presented in Ethical Risk Management and Mitigation Strategy in ASSIST-IoT, along with their respective mitigation strategies.
- ASSIST-IoT Ethical Design Model presents the Ethical Design Model that will be used, including the DevSecOps methodology that will be followed throughout the project.
- Finally, Conclusion / Future Work contains the conclusion and what the next iteration of the Ethics and Privacy Manual deliverable will include.

2. IoT ethics

2.1. Ethics in IoT's Distributed Intelligence

The technical aspects of Distributed Intelligence, as pertinent to the ASSIST-IoT action, have been elaborated in Deliverable D3.1. Therefore, lets summarise only the main points, while reflecting on their status vis-à-vis ethics requirements. The term *distributed intelligence* has at least two meanings: (a) *collective intelligence*, and (b) *distributed artificial intelligence*. In the first meaning, collective intelligence emerges from collaboration and competition of multiple individuals/entities. As the main mechanisms of collective intelligence are believed to be: (a) cognition, (b) cooperation, and (c) coordination. While it can be claimed that collective intelligence can materialize within IoT ecosystems (especially in IoT ecosystems of the future), it is also out of the work's scope that is being undertaken within the ASSIST-IoT action. Nevertheless, in the unlikely case that methods and approaches rooted in collective intelligence are going to be applied, further analysis of pertinent ethical aspects will be undertaken.

Distributed artificial intelligence (sometimes also called Decentralized AI) is a subfield of AI research, dedicated to the development of distributed solutions for problems. First, it is observed that, very often, it is seen as a predecessor to the research devoted to software agents and (multi-)agent systems. However, it should be noted note that the field of software agents has evolved on its own and, nowadays, is heavily loaded with domain-specific concepts, technical terms and results. Therefore, the ASSIST-IoT action may draw inspiration

from agent research. However, to avoid being constrained by its conceptual baggage, it will develop its own, fully independent, methods and approaches. Hence, whatever ethical issues could have been identified as being related to agent systems research (e.g. due to its use of Belief-Desire-Intention grounded thinking, which naturally, brings to the fore area of philosophy known as: theory of action), will not affect work undertaken within the scope of ASSIST-IoT. Nevertheless, a (relatively fresh) comprehensive review of the area suggests the possible value of using software agents in the Internet of Things [1]. Therefore, if methods and approaches rooted in agent systems will be considered, further analysis of ethical aspects that this development will bring, will be undertaken.

This leads us to the area of most interest to the action, which is known as *distributed problem solving*. Here, the main idea is as follows. Let us assume that a computationally intensive task, related to some form of, very broadly understood, machine learning is to be undertaken. For (very) large datasets, completing such task, on a single computer/processor/node, could require a substantial amount of time (hours, days or, even, weeks). Let us now assume that multiple computing nodes are available (in the form of a tightly coupled parallel computer, or a network of workstations, or a cluster computer). In this case, research has been devoted to finding ways how the "work" can be divided (among nodes) to complete the task. While the area is well studied, from the ML/AI perspective, in the context of ethics it should be observed that majority (if not all) of proposed methods and approaches, are designed for a *single stakeholder*. In other words, the main idea is that a single "user" (e.g. a company) is the sole owner of all data and retains full "control" over it. Reflecting on this assumption, form the ethics perspective, it should be immediately clear that research undertaken within the ASSIST-IoT action does not bring about any unique issues. Specifically, in all single stakeholder scenarios, when novel methods/approaches will be developed and implemented (e.g. enablers working within one or more planes of the ASSIST-IoT architecture) they will be deployed in a situation of well-defined control, and responsibility. This, in turn, means that it will be the data owner that will be responsible for assuring that all ethical issues, related to data collection, processing, storage and removal, are handled according to the GDPR and/or other pertinent EU/local regulations.

This brings us to the last aspects of distributed intelligence. Recently, the assumption about single entity having control over all data used in data analytics tasks, has been questioned. For a variety of technical reasons, the vision of a single owner of data that is used to train model(s), starts to be replaced by approaches that are based on coopetition [2]. From the perspective of the ASSIST-IoT action, the most interesting approach is known as *federated learning*, which has been proposed approximately 3 years ago. The main idea of federated learning is as follows. There exists a central (shared) model, training of which is the goal of the federated learning process. While the shared model is available to "all participating entities", individual nodes store private (local) data. During the training, each participating node is using only its data to train its local-sub-version of the model. Next, model parameters (only) are sent to some "central authority" and "combined into the central model". After the update is completed, the next version of the central (shared) model is redistributed (back) to the nodes that participate in the training. Here, the loop closes, and the process repeats, until the shared model is considered to be "good enough quality" (using process specific criteria).

Analysing this process, from the ethics point of view, let us start from the key observation. The idea of federated learning is based on the assumption that no data is exchanged between participating parties. As a matter of fact, one of sub-branches of research in this area is devoted to establishing how to assure that local data is protected from being revealed to the other participants. Hence, let us assume that this is the case (data breaches not related to federated learning, while a problem in its own right, do not belong to this analysis). With this assumption in place, it immediately becomes clear that each owner of local data is fully responsible for assuring that all ethical issues, related to (local) data collection, processing, storage and removal, are handled according to the GDPR and/or other pertinent EU/local regulations.

Next, let us consider the case when there will be a specific entity that will be the holder of the (central) shared model. In this situation it should be obvious that if this entity is external to the stakeholders, who commit their data to federated learning (model training), it is not likely that it will have actual access to the model itself. To illustrate the point, let us repeat the (already existing) scenario where three pharmaceutical companies A, B and C train a shared model, on the basis of their own proprietary data, e.g. to speed the medicine development. If they use, for instance, Microsoft Azure infrastructure, to facilitate federated learning, it is clear that Microsoft will not be allowed to access the model itself (as it is only an infrastructure provider). This also means that

whatever results of using the model will be obtained by either A, B or C, they will have to be "ethically controlled/guided" by their individual procedures (e.g. their DPO will manage this). The situation remains unchanged when the actual (final) model is stored within the infrastructure(s) of A and/or B and/or C. Then the DPO(s) of either, or all, of these companies have to assure that the use of the model complies with the EU/local regulations.

This all being said, we are ready to conclude that there are no special, novel or additional ethical issues generated by the distributed intelligence aspect of the ASSIST-IoT action.

2.2. IoT in ASSIST-IoT scenarios

According to the whitepaper "*Fact sheet- Ethics Subgroup IoT - Version 4.0*" [3] delivered in 2015 by the Experts in the Group of Ethics and IoT established by the European Commission, the use and deployment of IoT systems entail **six key ethical issues** that must be always considered and addressed. Drawing from that axiom, here below there is a reflection upon those, their application in ASSIST-IoT scenarios and how we (the Consortium) will tackle those issues to ensure ethical compliance of the IoT implementations during the project.

Key Issue #1: Social justice and divide
Description of the issue and ethical evaluation: IoT networks, devices, services, and the inner information that is thereof managed may have an impact in the global public day lives. Similarly, to other highly specialized scientific products (e.g. hadron collider), an average citizen does not realise the IoT fundamentals. Although openness and clarity designs are mostly put in place, a deep, conscious awareness of IoT is only reserved to an educated elite. The ethics issues, derived from this fact, may be unwanted data transfers, digital divide increasing (have vs. have-not), geographical and cultural differences (IoT available only for certain people at certain countries), ageing gap, among others. If some of these materialise, the capability of taking advantage of the smart services, and of IoT features, and the ability of protecting oneself against abuse, might be reserved only for a selected sub-set of the population, which would create social injustice and further augment the digital divide.
ASSIST-IoT perspective: Although ASSIST-IoT will be validated in three closed private industry environments, the objective of the action is to generate a blueprint architecture for the NGIoT to come. In this context, foreseeing the likely event of ASSIST-IoT adoption by wider, citizen-close entities, like municipalities, governments, or public-oriented companies of retail, etc., it becomes crucial to tackle aforementioned ethical issues. In particular, ASSIST-IoT must observe the ethics risks associated with accountability, access to the information, usability and traceability of data towards both the user and the data-generator (either a human or a machine).
ASSIST-IoT approach to ensure ethical sustainability: • Authentication and consent need to be put in practice; ASSIST-IoT contemplates and tackles this, see ASSIST-IoT Participants • Usable interfaces will be implemented for making the human machine interaction (HMI) of the developed solution very user friendly and flexible to be adapted for any type of user (advanced, novice etc.) • Easy instructions for any installation and/or user manuals, also translated to local language. • Committed Consortium with wide representation (scientists, construction companies' staff, transport workers, academia) in key phases of the design of all artefacts created within the context of the action.

Key Issue #2: Trust
Description of the issue and ethical evaluation: The essence of this issue is the lack of trust of the user (data-provider) about the use that her/his data will be made of, and by whom. Besides, in the context of IoT, lack of trust is also present in the "confidence" about accuracy of what the data generated by a machine actually means. This is especially the case if this data is going to shape a human-human (H2H) interaction. The lack of trust is, additionally, reinforced by the "omnipresent network presence" feeling (that might lead to an eventual rejection of the technology), the lack of control and the "interaction" with non-human

intelligences that can even act upon a panoply of objects. This issue is intimately related with the potential vulnerability, personal data protection, privacy and security.
ASSIST-IoT perspective: ASSIST-IoT should be designed to be trustworthy. ASSIST-IoT architecture will allow applications H2M, H2H via IoT and M2M, therefore mechanisms must be put in place to ensure traceability of data and interactions, certainty of data origin, and any action occurred upon those data.
ASSIST-IoT approach to ensure ethical sustainability: • ASSIST-IoT will make use (going beyond the SotA) of DLT blockchain. The concept behind the use of this technology in a H2H scenario is: "If you trust the person, you can trust the data he/she is forwarding". • Trust negotiation via Smart contracts and upon SLAs. • Trust based on digital signature and authentication.

Key Issue #3: Blurring of contexts, in particular the distinction *private* vs. *public*
Description of the issue and ethical evaluation: The perimeter of the private context gets blurred, as IoT is increasingly being incorporated to citizen homes' and "mediated environments". The traditional conception of "behind the doors" = private, is now changing as, for instance, the information of smart metering, of water or energy consumption, can be traced to the private life while being owned by the provider and used for improving the distribution network.
ASSIST-IoT approach to ensure ethical sustainability: ASSIST-IoT architecture, since the beginning, is being designed to clearly differentiate computing spots and responsibilities, by incorporating federated learning in the edge of the networks, where the delimitation of public-private fields is clearly easier to deploy. Flexibility on the edge configuration, data inclusion, digestion, etc. will be key for this purpose.

Key Issue #4: Non-neutrality of IoT metaphors
Description of the issue and ethical evaluation: Intimately related with issue #1, the IoT, which is difficult to be grasped by most citizens (and even policy makers), tends to be explained with a series of metaphors and examples that may entail a non-neutral bias. In the IoT, this effect has been hugely noticed due to the attractive possibilities it may offer at different contexts, which makes difficult to distinguish the facts and the expectations. Additional concerns under this classification is the lack of distinction of actors' features, as well as omission of the "tricky parts", when describing a potential IoT product (e.g. smart refrigerator).
ASSIST-IoT perspective: What ASSIST-IoT as a project must ensure, in order to comply with this ethical request, is to clearly an unambiguously announce its findings and solution in the most sincere, accurate, straightforward way. This includes both the "solution" as the architecture, as well as the outcomes of validation and piloting, while making it clear that the data privacy is respected.
ASSIST-IoT approach to ensure ethical sustainability: • Succinct but accurate language on social media expressions, explicitly state, which are plans, which are actual achievements, and the research conducted to arrive there. • Availability of information further than public deliverables. • Available email address on the website for any consultation. • Technologically and operatively, ASSIST-IoT will always state which objects ("things") are just for monitoring purposes. and which ones are devoted to actuation, thus properly informing the user. • The development of semantic interoperability in ASSIST-IoT will help characterise the data managed within the platform. and thus, pinpoint the assets to the common world ontology.

Key Issue #5: Agency: social contract between people and objects?

Description of the issue and ethical evaluation: With many actors, institutions and wide technologies involved, a generic grasping of the implications for citizens is not necessarily existent, resulting in lack of trust and eventual rejection of the technology. This key issue refers to the implicit intervention of various actors, with various intentions that are delegated to intervene upon a complex, interconnected network, upon which the user has seldom control. This fact may end up in unpredictability of behaviours of "things". Therefore, the need of "smart contracting" between humans and machines.
ASSIST-IoT approach to ensure ethical sustainability: ASSIST-IoT must be designed with such a flexibility that it will allow the owners of the system to specify, which actions can be performed over user owned actuators (e.g. LED in glasses, sound, movement in wearables, etc.). Additionally, these possible actions will be clearly informed (and agreed) with the users. This is the strategy that will be followed in all ASSIST-IoT pilots.

Key Issue #6: Autonomy: Informed consent vs. obfuscation of functionality
Description of the issue and ethical evaluation: IoT sensors, devices and even mechanisms, are moving towards miniaturization, which makes them (physically and logically) more difficult to inspect.
ASSIST-IoT approach to ensure ethical sustainability: • Clear documentation (deliverables, manual, page on GitHub, Readthedocs page, and video(s)) will be prepared for all ASSIST-IoT modules, thus ensuring proper communication of functionality. • The "registry service" that will be included in the ASSIST-IoT platform, is aimed at identifying, registering and describing all the devices connected in an ASSIST-IoT deployment. This information will be available for the platform owner, as well as for the data provider (being a company or an individual).

Apart from the previous, other key ethical aspects that are present in IoT, but can be widened to any other ICT technologies are privacy, data protection and security of the data/information processed by IoT systems. As these categories are technically dependent to the implementation of the artefacts that are going to be developed within the scope of the project, it has been decided to elaborate them further later, in Section 5.

3. ASSIST-IoT ethics Framework

3.1. Introduction

In this section, the reader may find the procedures and safeguards that will be followed to include participants in the ASSIST-IoT's activities, focusing on the pilot demonstrations, but also referencing participation and dissemination of other event types, such as webinars, conferences etc. The section is structured as follows: initially, a brief overview of the pilot sites is presented, followed by the ethics strategy that will be implemented. Next, the details for onboarding participants are presented, along with the necessary informed consent form (template provided in this deliverable, final version will be included in D1.1), and the guidelines for obtaining it. In addition, the consortium's policies for incidental findings and delegation of control are presented.

It must be noted here that this information is preliminary, as the present deliverable was submitted on project month 3, where not much information was available on the exact actions and procedures that will take place during the pilot sites (task T3.2 of use-cases definition was on-going), or for the actual data that the ASSIST-IoT system(s) will collect and process. Nevertheless, the present document provides the necessary guidelines that the consortium will follow in planning the pilot demonstrations and other events, while the fine-details will be provided in the next version of the ethics manual.

Thus, the present deliverable will serve as the basis for building a more detailed and tailored ethics strategy over the next months, that will be presented in the next version of the deliverable (D2.4, due on project month 18).

3.2. ASSIST-IoT Pilot Site ethical strategy

3.2.1. Preliminary deployment site description

ASSIST-IoT goal is to design an open and decentralized reference architecture, that will associate all the parts, to help in human-centric applications. The partners are to take actions, like the software applications development and many others, to achieve the project's goal. All these actions are to be demonstrated and evaluated in three different pilot sites. The preliminary sites are the following:

- port automation,
- smart safety of workers, and
- cohesive vehicle monitoring and diagnostics.

The allocation of pilots provides a broader spectrum for the project. In particular, different scenarios will be devised for each pilot. The scenarios range allows the adoption of various technological pillars and enablers based on each scenario's suitability. The pilots' engagement will create a loop, that provides feedback to the project, as the pilots will share their experiences. The feedback opportunity creates a condition to provide results of high quality and broad applicability.

3.2.1.1. Port automation site

The first pilot is on port automation and is lead by Terminal Link Group (TL) . TL is an industrial partner and port terminal operator that offers its premises in Malta Freeport terminal (MFTL) for the deployed of the project solutions. It should be noted that MFTL provides the opportunity to test the project's results in a busy environment. In particular, MFTL has noticed considerable growth since its establishment to the point of exceeding the 2 million containers per year. As a result, MFTL is a critical node in the maritime logistics with its activities covering the container handling and industrial storage.

As an overview of the activities in MFTL, heavy machinery equipment, such as cranes, is tasked to handle the containers. Furthermore, onboard drivers and on-site clerks are employed to handle and deliver freights. The employees are expected to interact with the machinery equipment and communicate with each via a wide range of means. ASSIST-IoT challenge in this environment is to showcase the benefits of technology adaptation in the industrial process transformation and equipment infrastructure in the maritime sector.

The port site, MFTL, has almost peaked to its maximum capacity, which subsequently results in bottlenecks in the operations and congestion in the terminal area. The evident effects of the congestion are the following four:

- Vessels stay is prolonged in time,
- Vessel berthing-wait-time is increased,
- A number of vessels have to be diverted to other terminals,
- Land vehicles record higher wait and turn-around times, which in turn results in environmental footprint concerns, a productivity cost increase, and overall inefficiencies in the supply chain.

To overcome those, ASSIST-IoT is expected to bring the following characteristics to the pilot:

- smart devices and edge nodes handle the generated data by sources in a decentralized fashion,
- efficient data management and interoperability,
- the operations will be enhanced by the deployment of human-centric applications that supports the terminal operators,
- continuous integration of data sources takes place to share knowledge between terminal nodes by means of the ASSIST-IoT architecture.

Four scenarios are considered to assess the results of ASSIST-IoT. The first scenario is on the automated alignment of the cargo handling equipment (CHE). Examples that CHE is referring to are cranes and the transportation vehicles of cranes. In this scenario, complicated tasks are to be automated. The use of Optical Character Reader (OCR) and QR codes offer the opportunity for creating a low-cost Minimum Viable Product

(MVP). The potential development of MVP could increase the throughput volume of containers and diminish human errors.

The second scenario is about the containers traceability and is titles as yard fleet assets location. The current process of the identification is dependent on manual intervention in specified control points. The process is prone to errors as it requires human intervention. An automatic container control could be developed by combining real-time telemetry in the yard, QR codes, and imaged-based positioning.

The third scenario objective is to transform the interaction between the staff and the heavy machinery. The objective will be achieved via the use of Augmented Reality (AR) and Tactile Internet HMIs. In addition to the AR and HMI, analytics techniques and Artificial Intelligence (AI) could be leveraged for automating tasks.

The final scenario focuses on the remote control of the CHE. An operator within a control will control remotely a crane with the extended capabilities from the project. This scenario provides the opportunity to improve the working conditions for the workers and extend the working life of the machinery.

3.2.1.2.Smart Safety of Workers

The industrial partner Mostostal Warszawa S.A. (MOW) will drive this scenario in the construction site of Marshal's Office in Szczecin (Poland). This partner is one of the front runners in the construction sector in Poland and carries out investments in crucial sectors of the construction market. The partner has experience in a wide range of construction facilities such as industrial, environmental and roads.

The workers' safety in construction sites is paramount for the smooth operation and completion of the construction. The safety is not restricted to the heavy machinery and materials in the construction site. The fact, that the construction site is open and vulnerable to the weather and environmental changes, should be considered. Additional to the weather, a construction site is a busy place where materials, machinery equipment and humans are constantly on the move. All the previous facts make it clear that a construction site is a complex environment with various interrelations between the staff and the machinery equipment.

The scenarios for workers smart safety are to be used as the basis for ASSIST-IoT and the solutions that are going to be developed in the project's duration. Initially, there are three scenarios in place to address the needs in a construction site. The first scenario focuses on the safety and health plan optimization with the implementation of Augmented Reality (AR) support. In this scenario, the access in a zone based on relevant permission could lead to increase the safety of workers. Furthermore, AI applications could have a place in this scenario as they could be applied on the walking path prediction and the monitoring of required PPE.

The second scenario is relevant to the smart actuation of smart devices adjustable to individual needs. The main objective is to use the smart devices, that function as objects in the IoT network, in a closed loop for the risk management process in OSH. The actuation will rely on protective measures that will ameliorate or even prevent risks. All in all, a human-centric sensing and actuation in real-time will take place in this scenario.

The third scenario is about the identification of suspicious and undesirable behaviours in the construction site. The risk assessment approaches are traditional static as rules act as the basis. The complex environment in construction sites will benefit from a shift towards a dynamic prediction of hazards. Distributed Ledger Technology (DLT) are to assist in building undesirable behaviours identification systems. DLT will be harnessed in this application, as the technology is implemented to build trust between parties. The data in DLT are immutable and no changes could be performed on the data.

3.2.1.3.Cohesive vehicle monitoring and diagnostics

In this pilot, FORD-WERKE is the selected industrial partner that will act as the driver. FORD-WERKE is a leader in the manufacturers of original equipment whose production exceeds the volume of 5 million vehicles. In the project's context, the partner will supply a hybrid electrical vehicle.

The pilot focuses on establishing a new approach to fleet condition diagnostics at the disposal of manufacturers, fleet managers and repair professionals. All the participants in the fleet condition diagnostics will produce data, which consequently leads to the integration of all the sources to extract knowledge and information out of the produced data. The vehicle condition, the prediction of maintenance tasks, and the evaluation of vehicles for recalls are the knowledge that the data could bring.

The pilot is divided into two scenarios that are relevant to the monitoring and diagnostic of the condition of a vehicle. The first scenario objective is to provide advanced powertrain monitoring. In this scenario, the project should assist the OEMs to abide by the in-service conformity (ISC) verification that instructs the vehicle's emission footprint. ASSIST-IoT will identify units that may not comply with ISC requirements. Furthermore, the combination of units with sensor sets is to be implemented during the project.

The second scenario is conserving the vehicle condition monitoring based on a scanning solution. This type of monitoring for typical maintenance can potentially facilitate swift control with an increase in the audited vehicle. The monitoring will assist in identifying mechanical malfunctions and maintaining the vessels' aesthetics. AI modules are to be harnessed for the deployment of the solutions.

3.2.2. Pilot sites ethics strategy

As it has been identified in the Ethics Requirement No. 4, the most relevant part in the **ASSIST-IoT** project **regarding ethical concerns, are the pilots** (*WP7 – Pilots and validation*). For that reason, the ethic procedures to be put in place for that WP, must be carefully analysed (lead by the project's ethical manager).

In ASSIST-IoT, the place and environment where the pilots will take place has been named as: "Pilot sites".

Apart from the data protection and privacy of the individuals participating in the pilots (which is outlined in ASSIST-IoT Participants), some ethics concerns arise globally in the context of the pilot sites. For tackling those concerns, ASSIST-IoT will conduct a series of activities that are listed hereupon:

Put in place appropriate safety and health procedures, conforming to relevant local/national regulation. This point will be further elaborated during WP1 and D2.4. However, during the work in task T2.3, up to M3, the following activities have been planned to be conducted:

- To carefully analyse the OSH directive [4] and to decide which of its procedures need to be adopted for the ASSIST-IoT.
- Specifically for the pilots, it is crystal clear that ASSIST-IoT must warn, advise and even remove researchers from all dangerous situations, if the case arrives. For doing so, a series of safety checks and procedures will be discussed and decided in WP1.
- To create a risk assessment template, for capturing potential safety and health risks.
- To carefully analyse other laws and guidelines, to ensure proper provisioning of safety and health procedures.

Appoint a Pilot Site Ethical Manager (PSEM), to each of the pilot sites. The PSEM will ensure that all relevant local/national/EU guidelines and legislations will be followed. The ethics manager will be responsible for defining the local data privacy and ethical issues for the pilot, and fill a relevant report (a template for this will be included in the next version of this deliverable (D2.4), that will be tailored to ASSIST-IoT and each pilot site).

Appoint an Ethical Manager of the project. As set out in the Grant Agreement, the Ethical Manager of the Project (EM) will take part in the project as one of the "governance bodies". His main objective is to ensure that EU-funded research is not misused from the ethical perspective. Since the starting stage of the project, the EM will analyse the activities being carried out, and cooperate with pertinent task leaders, to identify potential ethical risks and proposing solutions. The EM will also promote a better alignment of day-to-day tasks with every participant partner country's law and also with EU regulations and recommendations. In this sense, the work of the EM will facilitate, build upon and complement existing oversight regimes by competent ethical and legal authorities, acting as a kind of "proxy" between them and the ASSIST-IoT Consortium. Furthermore, securing the 'best interests' of the general public and civil society will also be one of the main goals for the EM, while supervising the ethical part of the project. Further details will be tackled within WP1, to be closed in M6 and materialised through deliverables D1.1 and D1.2. The ethical manager of the project has been appointed during the project's kick-off meeting and is Dr. Konstantinos Votis from CERTH.

Other activities of the ethical manager address ethical surveillance and participation during the pilots (this point – bullets listed below – will be further detailed in the WP1 deliverables, as well as in the next iteration of this very document (D2.4)):

- To report to the PIC every ethical issue arisen (with the provided template).
- Day-to-day work with Management Committees (PCC and PIC), ensuring alignment of ongoing activities with applicable law(s).
- To keep regular contact with WP7, and task leaders, regarding ethics-related actions.
- To report on any ethical issue arising, either identified by the EM himself, or by any member of the Consortium.
- To propose a solution on ethical issues and, if necessary, escalating the decision to higher levels of project governance.
- To update WP1 deliverables if any condition changes, or under particular request (either by the EC or by a Consortium partner).
- To gather the conducted reports, and elaborate a consolidated document and explanation, before every official review.
- To prepare any requested consent form for associated activities, and to gather the required signatures.

3.3. ASSIST-IoT Participants

In order for ASSIST-IoT to achieve its goals, various participants will be required to be involved. Initial assessment indicates that, in general, participants can be split in to two main categories:

1. **Pilot participants**: people that will be involved in the pilot demonstrations of the project (as described in ASSIST-IoT Pilot Site ethical strategy).
2. **Other event participants**: these can include people participating in webinars, conferences, workshops etc. organized by ASSIST-IoT action.

It should be mentioned here that partners' personnel are categorized as above depending on their involvement in the various activities (i.e. partner employees should not be treated differently than any other participants).

The following sub-sections will describe how the participants will be onboarded, and most importantly, how the informed consent, for their participation, will be obtained.

3.3.1. Communication

The participants in the ASSIST-IoT pilots, before being recruited, will be given a thorough explanation of the project and its aims, including the expected benefits for them, and any possible implications in case they decide to be involved in the project's pilots. Participants will be approached abiding the fundamental human rights principles and special attention will be paid to assure that they do not feel coerced, threatened, or stressed to participate.

The involvement will be on a strictly voluntary base. Moreover, it will be clear from the beginning whether or not monetary, or other type of compensation, or reward, will be provided for their participation. Furthermore, no penalization or punishment will occur if they do not participate.

For the pilot demonstrations, the participation will be strictly restricted to "*healthy adults*"; "*healthy*" in the sense that (i) they are capable of understanding the requirements of their involvement, and (ii) are able to make a decision about their participation on their own, and also (iii) that they have the physical and mental capacity to carry out the required tasks. Moreover, "*adults*" refers to the fact that no minors will be allowed to participate in pilot demonstrations.

Furthermore, specific measures to protect the participants from a breach of privacy/confidentiality and potential discrimination will be applied, as follows:

1. **Confidentiality**: the names of the participants will not be made public in deliverables, reports, etc. All personal data will be kept safely within the pilot organizer's facilities. Any information that needs to be made

public, for reporting or dissemination purposes, will be kept to a minimum and, if only possible, fully anonymized. In an unlikely case, if personal information needs to be released, special permission will be requested, following the EU regulations (the GDPR in particular).

2. **Right to receive more information about the project**: any participant will be able to ask questions about the project, to make sure they do not have any questions, or are unaware of any processes that will take place during their involvement.
3. **Informed consent**: each and every participant will have to sign an informed consent form, that will be carefully evaluated. The consent form will be outlining the scope of the pilot and its purpose along with all the data that will be collected. An initial template of the informed consent is presented in ANNEX I. The consent form will be further elaborated as the project progresses and will be tailor-made for the needs of the individual pilot sites (to be presented in D1.1).

The participants of other type of events will not be involved in the project activities directly, but they will receive information about them. Participation in such events (e.g. workshops or webinars) is already on a volunteer basis and, in many cases, by-invitation only, so there is no need for extra selection criteria. It is important though to mention, that these events will be used primarily for dissemination and exploitation purposes of the project. This means that these events can be recorded (video and audio) and/or covered by press (including photos and/or videos). The participants will be informed of this, and make sure they confirm acceptance (via signing physically or digitally a consent form or by email written consent or by accepting terms at the registration process) that their personal information (including photos or videos) can be used in such a way (e.g. upload of recordings, photos on ASSIST-IoT communication channels such as social media, website etc.). The same applies for regular project communication actions, such as newsletters and social media posts. The process that will be followed to get the consent from all the participants in these cases will be described in 3.3.2.Guidelines for interviews with pilots

3.3.2. Informed Consent

As already mentioned, a signed informed consent will be required for the pilot demonstrations participants. This section will describe the contents of the informed consent form, and a template is provided in ANNEX I. The consent form will be further analysed and developed over the next period and as the project evolves, and different versions will be created if necessary, to cover the specific needs of each pilot site. The final versions of the consent form will be provided in the next version of the "Ethics and Privacy manual" deliverable (D2.4).

It is very important to mention that, if a potential participant is not in place to read, understand and agree/disagree on the informed consent form on her/his own (e.g. due to language barriers or cognitive impairment), they will be immediately rejected from participating in the pilot demonstrations. No proxies will be allowed to sign the consent form on behalf of another. It will be made sure that:

- The participants have enough time to read and understand the project and its aims. A project representative will be available to answer any questions. Contact details for the local representative and/or the coordinator and/or the EM will be available in the consent form and on the project's website.
- The form will be written in a simple language, using short sentences, and making sure that no technical or other expert background is required (unless required by the actions to be performed during the pilot demonstrations). The form will be available in both English and the local pilot site language.
- All the procedures that will take place during participation in the pilot demonstrations will be detailed, including any personal, or otherwise, data that will be collected.
- It will be made clear that no monetary or other type of compensation will be provided (unless decided otherwise by the consortium).
- The participant will be made aware that their participation is strictly volunteer, and they can withdraw at any time without being asked any questions, give a reason, or face any consequences.

In addition, during the pilot preparation phase, the ASSIST-IoT consortium will make sure that:

1. No data can be collected without the explicit consent of the participants.

2. No person unable to express a free and informed consent for any reasons will be included in the pilots (refer to "*healthy adults*" description in Communication).
3. Collected data cannot be used for other purposes that the already defined in ASSIST-IoT and cannot be sold/given/disclosed to 3rd parties.
4. Only data that is strictly necessary to accomplish the project aims and communication will be collected.

The above procedure will be followed for the official pilot demonstrations as well as any other "internal" or "preparatory" pilot tests that will be organized by the consortium for testing purposes or for the preparation of the actual pilot demonstrations.

Moreover, with respect to obtaining a consent from people involved in other type of ASSIST-IoT events, such as webinars, conferences, workshops etc., the procedure agreed between the consortium members is as follows:

Daily communications (e.g. social media) and newsletters: If a person is going to be mentioned, either by name, email, voice, photo, tagging, or otherwise, a confirmation will need to be provided. The content of the post/publication will need to be made available in advance (e.g. by email) and the involved person will need to respond to the email and confirm/reject the mention. The coordinator and/or the project's EM will need to be in copy of the aforementioned email (original and response).

Video recordings: in case of a project meeting, at the beginning of the meeting the participants will be informed of the desire for the meeting to be recorded and disseminated afterwards. If there are no objections, permission is assumed. In case of objections, the objected person will be asked to switch off their camera, and any parts of the recording that the objected person is speaking will be removed from the recording before publication.

In the case of a webinar/conference, or similar event, it will be made explicit that the event will be recorded and used for dissemination purposed in the invitation letter and/or registration form (if there is one), and that the participants' name, email and photo/webcam might be visible. In addition, and similar to the project meeting case, at the beginning of the event a reminder that there will be a recording will be made. Again, if there are any objections, the relevant parts will be removed from the recording before posting it.

In the case of published papers (journal or conference), presentations, interviews etc., no additional consent is required, as this information is already publicly available (e.g. disseminating a link to an already publicly available paper or interview).

Finally, in case of partner specific activities, such as presentations, invited talks, open discussions etc., the participating partner will be responsible for obtaining the necessary consent from the participants, in order for the event to be disseminated through ASSIST-IoT channels. When the partner communicates the activity/event to the consortium with the wish to be disseminated through ASSIST-IoT channels, the partner must make sure they have the consent of all involved persons.

The procedure for obtaining the consent in this case could be an email notification that the activity/event will be publicized, and if any of the participants have any objections they should respond to the aforementioned email. Enough time (e.g. 15 days) should be given to the participants, with a reminder sent at least once during this time. No response is considered as "no objection" and the publication can proceed. This is applicable to all cases where consent is obtained through email notifications.

It should be noted that in the described plan, where an email notification is mentioned, the notification will come from at least one of the following: (i) the project coordinator (ii) the ethical manager (iii) the organizing partner.

The plan described in this section will be constantly monitored and revised as necessary. Any modifications to this plan will be reported in the next version of the deliverable (D2.4) along with a report on any findings on the current plan.

3.3.3. Guidelines for interviews with pilots

In order to ensure compliance with legal and ethical guidelines, a detailed procedure for recruiting volunteers for the pilot will be defined over the next period. The detailed procedure will be documented in the next version of the ethics manual (i.e. Deliverable D2.4, due on M18).

In the present deliverable, the general guidelines for the recruitment of volunteers can be summarized as follows:

- Only volunteer participants will be involved in the pilot demonstrations. No monetary or other compensation will be provided.
- The volunteers will be only healthy adults, meaning only people that can make their own decisions, read and understand the informed consent and decide for their participation.
  - People with special needs, will be allowed to participate in the pilots, provided their condition does not put them in danger during their participation.
- The pilot representatives will make sure to approach the potential volunteers and clearly explain the project, the pilot and what their involvement will require.
- The volunteers will be clearly informed that they can withdraw their participation at any time without any questions asked or any penalization.

As already mentioned, the detailed recruiting guidelines will be presented in the next version of the Ethics Manual deliverable (D2.4, M18).

3.4. Delegation of control

Delegation of control has two different aspects in the Ethics Manual: (a) with respect to the ASSIST-IoT system(s) and (b) with respect to data access rights.

1. All ASSIST-IoT components' operation will be monitored and controlled to ensure their reliability and efficiency. Moreover, all components will be designed with privacy and security in mind, as will be described in ASSIST-IoT Ethical Design Model, and further elaborated within the scope of Task T6.1
2. Data will be collected during the project implementation phase and, especially, during the pilot demonstrations. Access to this data will be granted only on a "need-to-access" basis. Since the collected data might include personal data (from the pilot site participants), this data cannot be made publicly available. Thus, only project partners that require access to the data in the context of the project needs (e.g. deliverables, reports, algorithms adjustments etc.) will be granted access to the data.

The implementation of the ethical design that will be described in ASSIST-IoT Ethical Design Model, will ensure the aforementioned delegation of control.

3.5. Incidental findings

Incidental findings are defined as the findings that maybe by-products or outcomes of the study that were not part of the main research questions and objectives but could be of importance for the wellbeing of the participant.

EC's guidelines for H2020 proposals named "how to complete your ethics self-assessment" [5] addresses the issue of incidental findings, and is included in the ethics issues checklist, under section 2 "Humans". Therefore, any research that involves human participants is obliged to define an incidental findings policy.

As the notion of incidental findings originated from the medical-related research, all existing definitions of it are focused towards health-related observations. Some indicative definitions that can be found in the literature are:

"incidental findings are observations of potential clinical significance unexpectedly discovered in research participants and unrelated to the purpose or variables of the study" [6]

and

"a finding concerning an individual research participant that has potential health or reproductive importance and is discovered in the course of conducting research but is beyond the aims of the study" [7]

In addition to this, incidental findings can be of any kind, ranging from a random behavioural observation to criminal activities.

Although the ASSIST-IoT consortium does not expect any incidental findings, working with volunteers in a pilot demonstration can lead to observations, or findings, that might be considered as such.

ASSIST-IoT's policy in case of incidental findings is described below:

1) Any incidental finding must be immediately reported to:
   a. The consortium's responsible for the pilot site (group of partners realizing given pilot).
   b. The project coordinator.
   c. The project's ethical manager.
2) All participants will be given the informed consent to sign, in which the incidental findings policy will be explicitly described.
3) The persons mentioned in (1), above, will confer to decide:
   a. If the incidental finding data should be deleted.
   b. If the incidental finding includes illegal activity, the consortium will comply with national and EU laws.
   c. If the incidental finding includes information of public interest, the persons in (1) will decide how and when they will communicate the findings to the relevant stakeholders.
4) The incidental finding should be communicated to the involved participant(s), including the decision from specified in (3)

4. Legal aspects

4.1. International and European instruments in the field of data protection

The first international instrument in the protection of data occurred in 1981 with the treaty titled 'Convention for the protection of individuals with regards to automatic processing of personal data'[8]. It should be noted that the treaty is referred, also, as Convention 108. The instrument was signed in Strasbourg, by all the members of the Council of Europe, in order to safeguard rights and fundamental freedoms. Furthermore, the treaty aims to regulate the cross-border flow of personal information. Strengths and limitations of the treaty have been covered in the United Nations work [9]. The comprehensive coverage, the ability for any country to join, and the harmonization, are viewed as the strengths that spring from the treaty. On the other hand, the Eurocentric approach, and the limitations in accommodating various national schemes, are points of consideration.

The European Union has included the protection of personal data in the Chapter of Fundamental Rights of the European Union [10]. The article 8 focuses on the protection of personal data in 3 paragraphs. The article provides the right to the protection to everyone. Moreover, the purpose of processing personal data should be specified, and any process should take place only after the consent. Furthermore, the right of access of information is established. Finally, the responsibility to abide with the rules lies on all the independent authorities.

Another instrument on the data privacy was the implementation of the Recommendation on the Guidelines for the protection of privacy in the information highways in 1999. The Recommendation is in harmonization with the EC Data Protection Directives that set the principles for lawful data processing, the Internet service providers' obligations and the rights that are entitled to data subjects. Users and service providers could advise the Recommendation for information to diminish internet risks. In more details, digital signature and encryption techniques are requirements for users to diminish the risks. On the hand, the service providers are instructed to implement certified privacy enhancing technologies and publish thorough privacy statements. Finally, the consent of collecting data from subjects is incorporated in the Recommendation.

In 1961, an international economic organization was established with the aim of promoting the economic development and world trade. This organization is Organisation for Economic Co-operation and Development, better known by the abbreviation OECD. The organization realized Guidelines on the protection of privacy in 1980 and re-issued in 2013 [9]. The revised guideline [11], sets in total eight principles, which are the collection limitation, the data quality, the purpose specification, the use limitations, the security safeguards, the openness, the individual participation, and the accountability principle.

The European Union currently has four instruments on the data protection [12]. These instruments are the General Data Protection Regulation (GDPR) with the Regulation (EU) 2016/679, the Data Protection Law Enforcement Directive with Directive (EU) 2016/680, the Directive on privacy and electronic communications (Directive 2002/58/EC), and the Regulation on the processing of personal data by the Union institutions and bodies (Regulation (EU) 2018/1725). The GDPR will be examined in a separate Subsection in the current section.

The European Union has issued a directive in 2016 that is relevant to the protection of natural persons' data from processing by competent authorities [13]. It should be noted that the directive is relevant to processes on personal data for the purpose of investigation, prevention, and prosecution of criminal activities.

The Directive 2002/58/EC focuses on the personal data protection in the electronic communications sector [14]. The Directive defines the terms traffic data, location data, communication and value-added service. The location data are the data relevant in pinpointing the geolocation of the users' equipment in a communication network. Additionally, any data that are processed for communication purpose in a network are traffic data. Technical and organizational measures to guarantee the security of the service are necessary. On the occasion of a risk on data breach, the service provider is obligated to inform the subscribers on the risk.

The European Union have regulated the data processing of personal information by its institutions, and bodies with Regulation 2018/1725 [15]. The institutions and bodies that should abide by the regulation are the ones that are set up by the TEU, the TFEU or the Euratom Treaty. The regulation sets standards that the EU bodies should abide by and proves the importance of the matter.

4.2. Relevant legislation, directives, and Guidelines

The European Union's Fundamental Rights [10] expands further than the Article 8 on the personal data protection. The Article 7 is concerning the respect for private and family life, and it is a fundamental right that every citizen possesses. The notions that the article is referring to, are the private life, home and communications.

The Data Protection Directive 95/46/EC [16] is a major work on the privacy and human rights in EU. The subject of the Directive is the protection of individuals in respect to their personal data and the free movement of this kind of data. The Directive in the article 6 lays the principles to data quality such as the lawful processing and the relevancy to the purpose. The article 7 adds criteria to the legitimate process of personal data. The criteria are the clear and unambiguous consent of the data subject and the processing to abide in certain cases. Moreover, Article 8 needs to be considered as the article prohibits the processing of personal data that could potentially reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data relevant to health.

The Directive 2006/24/EC [17], known also as the Data Retention Directive, was about the provision of publicly available electronic communications services. The Directive instructed the retention of data types that were specified in Article 5. These data were data concerning the identification of the communication source and destination, time data on the communication. In 2014, the Court of Justice of the European Union declared the directive as invalid with a press release [18], due to the possibility of the unveiling a person's habits, residence, or movements.

The Commission acknowledging the potential of the Artificial Intelligence (AI) in alleviating contemporary issues have worked to provide a human-centric approach [19]. The AI applications needs to respect seven requirements that are deemed important to guarantee the European human values. These seven key requirements are the human oversight, technical robustness and safety, privacy and data governance, transparency, diversity, societal and environmental well-being, and accountability. It should be noted that the contents are guidelines that are not legal bidding. Nevertheless, the guidelines principles are reflected in the European regulations.

ASSIST-IoT will take place in working environment, such as ports, and other supply chain places. The safety of workers will be taken into account. Legislations that safeguard the safety of workers are in place. The Regulation 2016/425 [20] is referring to the requirements in personal protective equipment (PPE). The regulation provides the definition of PPE in Article 3. Equipment that is worn, or held, for the protection against a person's health and safety, interchangeable components to such equipment that are essential for the protection,

and connexion systems to the equipment could be regarded as PPE. Furthermore, the legislation sets the legal obligations that the PPE on the market should abide by obligations to ensure the safety.

Finally, directive 2002/58/EC (the ePrivacy directive) is also of interest to ASSIST-IoT. A short description of it is provided in the previous section.

4.3. GDPR

The General Data Protection Regulation (GDPR) is a regulation that gathered the interest of public as it was one of the first data regulations in the digital era. In the era of the fourth industrial revolution, the data are proved to be a valuable resource and is compared to oil [16]. The growth in data usage is reflected in the experts' estimation on the internet traffic that the data flow would increase two times in 2021 compared to 2018 [17].

In this environment, the GDPR regulation entered into force in May 2016, and it became applicable in May 2018, after the completion of a two-year span. The regulation is considered to be an essential step in strengthening persons fundamental rights and to provide concrete rules for businesses and public bodies [18]. Furthermore, the regulations could solve the fragmentation in European Union that is caused by the separate national legislations.

The fourth article of the GDPR regulation [19] contains valuable definitions that clarify and set a basic understanding in notions. The main notions that should be taken into account for every participant of the project, are the personal data, and the data processing. The personal data are defined as any information that could identify directly, or indirectly, a natural person. Examples of personal data could be a name, location data or factors specific to physical, mental, economic, cultural, or social identity of a person. Additionally, the processing refers to operations or set of operations, which are performed on personal data, regardless of the automatic level of the operation.

The regulation sets the rights of the data subjects clearly in the third chapter [19]. A division for the different rights springs from the five distinct sections in that chapter. The rights are set in the following sections:

- Transparency and modalities,
- Information and access to personal data,
- Rectification and erasure
- Right to object and automated individual decision-making, and
- Restrictions

Twelve articles are part of the five subsections that cover the rights of the subjects [20]. The rights are set by initially communicating the information that are subjected to processing. The way of communication should be concise, transparent, intelligible and easily accessed by the subject. The second subsection is relevant to information that needs to be conveyed to the data subject in both of the occasions of the collection or absence of collection of personal data. Continually to the third subsection, a data subject has the right to access his personal data that is gathered by the controller. Furthermore, the most noticeable right is the 'right to be forgotten', that allows the data subject to raise the claim to erase the data upheld by the controller. The third subsection provides the right to the processing restriction, an obligation to notify regarding the erasure, rectification of personal data and of data portability. The fourth subsection covers the right to object sharing his personal data and the regulation of the automated individual decision-making. The final subsection sets restrictions on the previous rights based on legislative measures.

5. Data Privacy Policy in ASSIST-IoT

5.1. Introduction

The following section underlines the principles that ASSIST-IoT will follow regarding its data privacy policy. Privacy and ethical risks in the IoT area are constantly increasing and securing personal data against unauthorized, or unjustified, access is becoming more and more critical. The EC, in its "how to complete your

ethics self-assessment" manual, in section 4 "Personal data", states that if a project will process personal data, justification for the processing, as well as the methods to ensure the protection of privacy must be provided. Moreover, it is also stated that in case the collected data is further processed, "*an explicit confirmation that the beneficiary has lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects must be submitted as a deliverable"*. This section will describe the data privacy policy that will be implemented, which will also be explicitly detailed in the project's Data Management Plat (D1.4).

5.2. Confidentiality and Data Protection

Although the details of personal data protection mechanisms to be put in place will be thoroughly discussed in the deliverable D2.4 and in those of WP1, the Consortium has deemed important to set the basis early towards a seamless execution of the first months of the project.

The reference on this point throughout all the action will be to attach to every general provision and article of the General Data Protection Regulation (GDPR).

The most relevant concerns regarding confidentiality and data protection in ASSIST-IoT are: (i) those associated to the processing of data by the ASSIST-IoT platform, (ii) those related to the partners' personnel involved in the execution of the pilots, (iii) the external people who might contribute to the project (e.g. interviewees, participants in events organised by the project, etc.), and (iv) the authorised use of that data.

About the processing of data by the ASSIST-IoT platform, the Consortium has made initial reflections that will be enhanced in the documents that are going to be completed in M6 (Data Management Plan) and M18 (Final version of the Ethics and Privacy protection manual) (D2.2 and D2.4 respectively). One of the goals of ASSIST-IoT is to maximise the exploitation of heterogeneous data, through the logically same space. This circumstance will be repeated in most NGIoT deployments, which the project's architecture aims at covering. Thus, any associated ethical issue must be considered and be made inherent to the ASSIST-IoT product. The following preliminary hypothesis will be followed:

- The data generated within the scope of ASSIST-IoT, and to be used and handled in the same framework, will be managed by applying the highest precautions about protecting personal data. It will be encrypted if it must exit the context of the ASSIST-IoT repository, and the processing will be done according to the mechanisms to be defined later in the project.
- For deployments of ASSIST-IoT technology, the data protection will be ensured via two software-based approaches: encryption and distributed ledger technology (DLT). This is outlined in the next section of the document.
- During the project, in the scope of the applications over potential personal data (e.g. AI models and inferences, discovery services, monitoring, etc.), the technology mechanisms will be supported by a clear specification by the task leaders, of the purpose of the service and the use of that data, always respecting all GDPR articles.
- Data captured and collected in a non-digital way (for example, in the pilot sites, reporting about sensors, about the weather, information in paper provided by a stakeholder) will be digitalised later by the responsible Task Leader. These data will, then, go through the rest of mechanisms stated in this document.

The **data subjects/research participants** in ASSIST-IoT are classified as the following:

- Humans participating in the pilots. Some pilot scenarios (especially in the safety-construction pilot) involve the participation of workers which must inherently be identified, thus generating personal data protection concerns.
- External people participating in operative tasks of the project: participants in surveys, interviews, Q/As sessions, webinars, workshops or meetings organised by ASSIST-IoT.
- ASSIST-IoT partners' personnel.
- Advisory Board members cannot be considered internal members of the project but are also one step closer than general external contributors. As usual in research projects, and drawing from the agreed terms in the CA and GA, a "collaboration agreement" document will be prepared and signed by the PC and each AB

member, detailing the kind of contributions expected, the scope of the collaboration and the personal data protection mechanisms that will be put in place.

About the data protection of Humans participating in the pilots, ASSIST-IoT pledges in appointing one Data Protection Officer for each of the pilot cases in the project. These DPOs will be in charge of ensuring the GDPR compliance in all the actions of associated WP7 tasks, including the provision and gathering of Informed Consents to the participants. The appointment of each DPO is a matter falling under the scope of WP1 and thus there will be further reported. In particular, people who take part in the pilots will be informed formally about the project and its characteristics on the official form called "Information regarding processing of personal data". This document will contain information about purpose of the data processing, treatment modalities, providing data, scope of communication and dissemination of data, the rights of the data subject, the controller and resource person for communications, and requests concerning the privacy or anonymity. After giving this information, the written consent of the data subject is requested.

For external people, just before their participation, a thorough Informed Consent will be forwarded through which: (i) their consent of processing personal data will be gathered, (ii) the use to be done to their data will be detailed, (iii) altogether with the objectives of the processing. Additionally, (iv) withdrawal and (v) restriction options will be made available.

For ASSIST-IoT partners' personnel, the use of their personal data is two-fold: (1) For the management of daily project activities, such as teleconferences, mailing lists, etc. The permission to use this data was granted through the signature of the Grant Agreement, which, in its article 39 depicts: "*The beneficiaries may grant their personnel access only to data that is strictly necessary for implementing, managing and monitoring the Agreement*", therefore, no additional means need to be put. (2) The publication of personal data of those subjects in social media post or any other communication action. More details on the exact procedure to obtain the necessary consent is provided in Informed Consent of the present deliverable.

Apart from all the previous (specific for data protection), the ASSIST-IoT consortium must ensure that the rights and freedoms of all those data subjects/research are safeguarded. To do so, and according to the very definition of those rights by the European Commission, ASSIST-IoT will apply:

Table 1. ASSIST-IoT measures to safeguard data subjects' rights and freedoms

Right	Measure put in place in ASSIST-IoT to safeguard it
Informing the data subject about the use of their personal data	In all cases, the informed consents to be sent to the data subjects must be signed by them, therefore acknowledging the use of the data thereof
Obtaining access to their personal data being held.	The Ethics Mentor contact is always included at the beginning of the Informed Consent. Additionally, the Coordinator contact is available at the public website.
For correcting inaccurate data.	Data collected by the "project" (in repositories) or by "the platform" (used in deployments) will always be located by unique identifiers and will always be accessible by partner to be modified/corrected. A special tag is planned to be attached to any personal data managed.
For erasing their data.	
For being aware of the object of the use of that data.	Within the Informed Consent sheet (at the beginning), there always be included a description of the project, a description of the task and a detail of the objective behind processing that data (e.g. analysing population density)
For allowing the subject to restrict the use of their personal data	Within the Informed Consent, specific check boxes will be included through will the data subject will be able to fine-tune the permissions to use their data, giving the possibility of just allowing a sub-set.
For ensuring "data portability".	The personal data will be provided to the data subjects (if requested) in PDF document. Additionally, the architecture contemplates the development of authorised access to APIs to extract data, which will guarantee interoperable access through usual means (HTTP).
Automated decision making to be made by humans and not only by computers.	ASSIST-IoT will be designed human-centric, which means that the user should have control of the applications and processing that will be performed over their data. This concept is enhanced with the foreseen use of explainable AI. With

	regards to personal data of the external participants of the project, all the data will be controlled by humans.

Regarding "*unauthorised access to personal data or the equipment used for processing it*", this concept could be assimilated as "confidentiality breaches". This aspect will be carefully analysed in further tasks in the project (WP1 and D2.4). For now, the means put are: (i) data stored in the project's repository: the PC handles the access permissions to the folders, which is based on a user-password strategy with usual password restrictions. (ii) usage of the platform's interface, which contemplates authorised access via authentication that will be handled by specific novel technologic modules of the platform.

5.3. Coding Anonymized Data and Storing

The Ethics checklist for H2020 projects, in Point 4.8 states that if personal data will be collected, the description of the anonymization and/or pseudo-anonymization techniques that will be implement must be provided.

In frames of ASSIST-IoT action, data will be collected and processed by several partners, and from different and heterogeneous sources. Partners should make the right decisions as far as the methods they use when collecting and processing data. The methods should abide by the current legislation and be compliant with the data protection approaches adopted by ASSIST-IoT.

Personally Identifiable Information (PII) should be anonymised using appropriate anonymization methods before stored so that identities are concealed and no personal data breaches can occur. PII will be coded in a way that users can use them, but without being able to correlate them with the actual identities of the data owners. Only authorised people shall have access to the data prior to the anonymization. Related methods to anonymise PII are k-anonymity [21], including suppression and generalisation, pseudonymisation, and obfuscation.

More specifically, suppression and generalisation will ensure the minimisation of the risk of re-identifying data through linkage with other datasets. Pseudonymisation will de-identify PII, by replacing identifiers by one or more artificial identifiers, the so-called pseudonyms. Finally, obfuscation will add distracting or misleading data to the PII and will result in frustrating precision analytics [22].

Furthermore, data encryption and homomorphic encryption will be used, to ensure confidentiality of the data, i.e. that data are not accessed by unauthorised entities when stored or processed. Only the owner of the corresponding decryption keys will be able to decrypt, and view, the sensitive part of the data that will be chosen to be encrypted.

Data processing will be done only in the anonymised datasets. Furthermore, it should be stressed that databases used during the project will not be kept after the end of the project. Data owners will be fully informed about data protection policies related with ASSIST-IoT and they will give explicit consent, which data to share, with whom, and for how long given the right to dynamic, fine-grained, and timely consent.

Additional information on the anonymization techniques that will be used within ASSIST-IoT will be provided in the project's Data Management Plan (D1.4)

5.4. Privacy in ASSIST-IoT system

According to some sources, "*Data privacy is about what people who have collected your data lawfully can and should do with it and what control you have over that retention and use of data*".

As specified in Table 4, the data subject will be provided with enough information about the use of their data, the motivation of gathering it, etc. The data retention and destruction strategies have been outlined in the previous section. These will be enhanced later in the project.

With regards to the remaining part of the description, what ASSIST-IoT plans to do with the personal data collected is:

- To digest the data, to obtain a vision of the market status of different technologies and verticals related to the project.
- To generate a baseline for the training of AI models, if needed, and to make assumptions towards technical completions.
- To have a list of potential dissemination recipients.
- To conduct the project pilots, with regards to their safety at work.
- In future versions of this deliverable, more uses could be found and included.

Finally, it is worth to mention that privacy in general in ASSIST-IoT will as well endorsed by the use of distributed ledger technology (any use of the data is registered and the inspection cannot be avoided) and DevSecOps (details on ASSIST-IoT Ethical Design Model).

6. Ethical Risk Management and Mitigation Strategy in ASSIST-IoT

6.1. Risk Assessment Strategy

Acknowledging the existence of risks and trade-offs in the selection, the formulation of a risk management process is essential for the project. Initially, the project ASSIST-IoT will centre the Risk Management around four pillars. These pillars are:

- Effective management.
- Risk tracking.
- Contingency planning.
- Multiple loosely coupled objectives.

The aforementioned pillars are essential in dealing with the risks. The risks are generally composed into two different clusters. The first cluster consists of risks that are related to management. These risks are in a wide range, but they are mainly related to the management and the technical risks. Management risks are related to risks arising from the partners participation, complications in planning, collaboration issues, and risks arising from external sources. Additionally, technical risks that may occur during the project are, among others, the obsolesce occurred from changes in environment, or users preferences, the existence of failures, as a result of limited testing, delays in the software deployment due to integration testing, the interoperability of machine learning models, applicability of self-* mechanisms, the data interoperability, the choice of the most appropriate approach to pilots' requirements, the security to be on par with the market, and the absence of interest from external stakeholders for the solution.

After the establishment of the risks, wellbeing risks of the participants are not anticipated withing ASSIST-IoT's evaluation, but any indirect effect should be taken into account as machinery and workers are to be involved in the pilots. The critical risks are to be documented in detail in a single document that will accommodate the ongoing changes in the project's course. The resulting "living document" will track potential contingencies, and oversee possible mitigation actions, to previously unpredicted and persisting risks. Moreover, a work plan is devised in order to assist in the effective contingency planning. The risks will be tackled by the formulation of strategy to alleviate the probability of risk to arise. The partners' experience on mitigation is to be capitalized as they are in place to deal with in-project contingencies based on previous engagements.

6.2. Ethical Risks in ASSIST-IoT

In this section, an initial list of the ethical risks related to ASSIST-IoT activities is presented. This list will be further elaborated as the project progresses, and the results will be included in the next version of the Ethics

and privacy protection manual (D2.4) as well as in the Risk management deliverables (D2.5, D2.6 & D2.7; 1st, 2nd and final versions respectively)

Table 2. Initial list of ethical risks in ASSIST-IoT

Ethical and social risk	Description	Risk management in ASSIST-IoT
Loss of privacy control	Storage and process of personal and sensitive data confidentiality	All data collected will be anonymized and securely stored as described in Coding Anonymized Data and Storing Raw data will be destroyed according to the project's data management plan (D2.2) Core partners involved in the pilot demonstrations have the experience and capacity to ensure that no loss of privacy will occur.
Data security	Difficulty in ensuring the security of personal data	Special attention will be given to ensure the security of any PII will be collected during the pilot demonstrations of ASSIST-IoT. State-of-Art Privacy Enhancing Technologies will be utilized to ensure protection from data breaches
Accessibility	Third parties' interest in access to electronically recorded and stored personal data. Participant own access to his/her data.	Data protection measures will be taken for each pilot site, respecting both National and European legislation. Limited storage of records coupled with state-of-the-art encryption techniques will reduce risks related to accessibility of data by third parties.
New technologies and IoT-related equipment	Existing infrastructure in the foreseen pilot sites Additional sensor installations needed to validate the new features brought by ASSIST-IoT	The consortium partners have the expertise to make the appropriate installation for the purposes of the pilots, in which only common and certified technologies will be used. Moreover, most of the partners have participated in several National and European projects related to the integration of sensors for demonstration purposes and their use in ethical compliance with National and European legislations
Safety	Pilot testing should not induce any risk for the participants	Guidelines for user involvement have been provided in ASSIST-IoT ethics Framework of the present deliverable and will be further evaluated in its next version (D2.4). Testing of technologies will be always supervised by the relevant ASSIST-IoT team.
Accountability	The accountability of the IoT applications regarding users' privacy	ASSIST-IoT data management plan deliverable (D2.2 will identify the responsible for the accountability of the data throughout the ASSIST-IoT applications.
Digital Divide	Participants have different skill and familiarity with using IoT devices and applications, as well as the privacy risks imposed	ASSIST-IoT by employing a use-centric approach from the beginning as well as having security build-in its systems, minimises as much as possible the digital divide risk.

Conformance to regulatory frameworks	Conformance to regulatory frameworks can be hampered by the speed of the IoT evolution surpassing that of the regulatory processes, so that the regulations can be less effective when they are enforced; and the regulatory framework can be extremely broad due to the participation of many different parties/countries to its definition	All the possible directives, legislations and guidelines will be considered by the ASSIST-IoT consortium. Additionally, the consortium will continuously monitor new regulations that come to force during its implementation period, in order to make sure the developed solutions comply with those as well.

7. ASSIST-IoT Ethical Design Model

In the digital era of the fourth industrial revolution, the digitalisation of material and devices is envisioned to take place. One of the possibilities of the era is the representation of physical objects in the digital world. Moreover, devices are expected to possess capabilities, such possess objects and create value, previously anchored around humans. All these changes would increase the number of smart devices and the communication between them. Despite the changes in the environment, security is a constant requirement in every phase of a solution's development that is tailored for market adoption.

The philosophy around security is adapting to the changes and requirements from the environment. The DevOps paradigm did not include the security department as one of the roles in the chain. The reasoning behind the absence of security and its isolation to the final development stage was documented by RedHat [23]. The development cycles were previously considered in extended time spans, but the case has changed to an accelerated phase that is counted in days. The accelerated pace in development calls to include security in the development cycle, as outdated security protocols could undermine the software.

The characteristics of DevSecOps are described in the literature review by Myrbakken et al. [24]. The characteristics are divided into principles and practices in the analysis. The principles are the set of reasons for adopting DevSecOps. The principles, in detail, are the cultural cooperation between the different teams, the expansion of automation in security to keep up with the fast pace development, the adoption of metrics to track threats and vulnerabilities, the active involvement of the security team in the information sharing and the earlier involvement of the security team in the project.

The practices in the DevSecOps adoption are threat modelling and risk assessments, continuous testing, monitoring and logging, security as code, and security drills. The threat modelling and risk assessments are meant to prepare the organisations prior to the attack occurrences. The risk assessment could be performed in the early development phase and be updated as the project is ongoing. A shortlist [25], with the things to include in the risk assessment, are the possible threats, the types of data and their sensitivity, the system controls, the cloud environment security posture, and the controls in place. The threat modelling investigates the design to find vulnerabilities that an attacker could exploit [26]. The threat modelling could take place in paper and the vulnerabilities are tackled early. Another DevSecOps is the continuous testing for the security exploitations in the code. The code review should be performed by experienced personnel in security issues and is different from the one performed by the developing team. Static analysis tools [24] are suggested to assist in finding changes in the code. Another practice in DevSecOps is monitoring and logging. This practice could save time and enhance efficiency as an auditor could review log resources in demand. Finally, it is advised to run security drills in an attempt to be ahead of attackers [27]. Establishing a Red Team for that purpose could strengthen the security inspection in the organization and permits for inline testing. The actualization of the “Red Team” will be decided as the project developments proceed, if the consortium decides that such a measure is needed.

The DevSecOps methodology is to be incorporated in WP3 and WP4, as foreseeing in ASSIST-IoT's DOA. The WP3 will set the ground in requirements and specifications, along with the architectural blueprint for the software. Additionally, the WP4 will provide the core enabler design for the IoT infrastructure. For the purpose of adopting the DevSecOps methodology, the key security partners (S21SEC, CERTH and UPV) are to be integrated and cooperate with the development and operation activities. The ASSIST-IoT is to develop security aspects in the DevSecOps methodology. The first aspect is the vulnerabilities detection in security analysis of the code. Additionally, the architecture is set to incorporate security tools in the suggested structure. The security compliance to the legislation and standards is to be established with the DevSecOps methodology. Possible risks are to be examined in the software delivery and a descriptive mapping of mitigation actions to these risks is to be included. Moreover, a vulnerability analysis will be devised for the system in place. The final security aspect is to create a team that is mindful towards security and security training is to be provided to achieve this aspect. Finally, a roadmap is to be designed to support the automation of repetitive tasks, component testing and security aspects, and software delivery and packaging.

8. Conclusion / Future Work

ASSIST-IoT aims to deliver a novel set of applications and tools around the IoT ecosystem that, besides their technological advancements, will also benefit the safety, security and productivity of workers in an interdisciplinary area of application scenarios. In order to achieve its scope, it will carry out a series of real-life pilot demonstrations, to assess and validate the performance of the developed solutions, but also to gather valuable information that will help the consortium build those solutions. Since the pilot demonstrations will need to include human participants, an ethics policy needed to be defined, to ensure the safety and privacy of those participants.

The present deliverable is a baseline document, to set the foundations of the ASSIST-IoT's ethical and privacy manual. Within this document, major ethics issues were addressed and listed, while considering and referencing relevant international and EU legislation and guidelines.

Within the project's lifeline, the Ethics Manager, along with the Project Coordinator and the Technical Coordinator, will monitor and scrutinize all project activities to ensure the privacy, confidentiality, anonymity and ethical risk management and mitigation.

The goal of this deliverable was to lay the groundwork for the framework, on top of which all the research actions of ASSIST-IoT will take place. As the flow of information between the various components of ASSIST-IoT is constant and dynamic, it is very important to define as early as possible the ethical principles governing all the activities.

The present "Ethics and privacy protection manual" is the first version of what will be a structured procedure that ASSIST-IoT consortium will follow, to ensure ethical viability throughout and after the project. The final version of this deliverable, D2.4 to be submitted at project month M18, will provide details of all the ethical and privacy preserving aspects of the project, as at that point the developments will be more advanced, and the pilot demonstrations will be under way. In addition, D2.4 will update all the future ethical risks that will be identified over the next period, as well as any new legislations or guidelines that will be published and will need to be taken into account.

ANNEX I – Informed consent template

This project has received funding from the European's Union Horizon 2020 research innovation programme under Grant Agreement No. 957258

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

Informed consent

I, ☐ contractor ☐ ASSIST-IoT partner' member ☐ external participant, the undersigned, volunteer to participate in the test/pilot conducted by the **ASSIST-IoT** consortium, in the project titled "**Architecture for Scalable, Self-human-centric, Intelligent, Secure, and Tactile next generation IoT**". I confirm that (**please tick box as appropriate**):

1.	I have read and understood the information about the ASSIST-IoT project, as provided in the Information Sheet attached with this consent form.	☐
2.	I have been given the opportunity to ask questions about the ASSIST-IoT project to consider the information and have gotten satisfactory answers.	☐
3.	I understand and agree on my eligibility to be a part of this test/pilot (i.e. I am not a minor, nor I fulfil any other exclusion criteria).	☐
4.	I understand that my participation is voluntarily, and I can withdraw at any time without giving reasons and that I will not be penalised for withdrawing nor will I be questioned on why I have withdrawn.	☐
5.	In the case of withdrawing, I understand that I should not disclose and/or share any confidential information about ASSIST-IoT project that I have learned during my participation.	☐
6.	I understand that no payment of incentives and/or rewards will be made to me.	☐
7.	I understand the procedures regarding confidentiality and privacy as they have been explained in the Information Sheet attached with this consent form.	☐
8.	I understand that the data collected in test/pilot can be used for publications and dissemination as explained in the Information Sheet attached with this consent form.	☐
9.	I understand that the data collected in test/pilot will not be re-used for any other purposes than the original purpose of ASSIST-IoT project as explained in the Information Sheet attached with this consent form.	☐
10.	I understand that the confidentiality of data collected about me will be preserved as explained in the Information Sheet attached with this consent form.	☐
11.	I understand that my right to request access to any, and all, personal information that I have voluntarily provided as part of my participation, and that I may ask	☐

	for that information to be rectified and/or amended if it is inaccurate, or request that all personal information that I have provided be deleted.	
12.	I understand that any requests for data access, rectification and/or deletion must be done through representative of the ASSIST-IoT joint Ethics Manager (contact details below).	☐
13.	I was informed by the ASSIST-IoT representative that in case of unexpected findings, the project consortium is obliged to inform: i) The ethical manager (…) ii) The Project Coordinator (…) iii) The European Commission via the ASSIST-IoT Project Officer I understand that the above mentioned bodies, will decide on the need, means and timing of communicating the findings to relevant stakeholders.	☐
14.	I, an external participant (……), along with the ASSIST-IoT team representative, agree to take part in the ASSIST-IoT study, and to sign and date this informed consent form.	☐

I hereby, agree to give personalized permission to ASSIST-IoT to collect, analyse and publish/report my data (when necessary) as provided in the Information Sheet and in compliance with standards and regulations.

Participant:

_____ _____ _____

Name of Participant Signature Date

ASSIST-IoT team representative:

_____ _____ _____

Name of representative Signature Date

Contacts information

Ethics Manager: **Contact person:** **Tel.:** **Email:**	**Local pilot representatives:**

Appendix 1

This project has received funding from the European's Union Horizon 2020 research innovation programme under Grant Agreement No. 957258

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

Data Subject Consent Withdrawal

Full Name	

I confirm that I would like to withdraw my consent to process my personal data from ASSIST-IoT project. ASSIST-IoT project no longer has my consent to process my personal data for the purpose described in the information sheet. I expect processing will be stopped as soon as possible, however, I understand that there maybe a short delay while the withdrawal is processed by all ASSIST-IoT parties.

Signed by data subject: _____ Data _____

Request obtained by: _____ ASSIST-IoT partners name _____

Signature _____

References

[1] Claudio Savaglio, Maria Ganzha, Marcin Paprzycki, Costin Bădică, Mirjana Ivanović, Giancarlo Fortino, Agent-based Internet of Things: State-of-the-art and research challenges, Future Generation Computer Systems, 2020, Volume 102, Pages 1038-1053

[2] Coopetition is the act of cooperation between competing companies; businesses that engage in both competition and cooperation are said to be in coopetition.

[3] https://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1751
[4] https://osha.europa.eu/en/safety-and-health-legislation/european-directives
[5] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf
[6] Incidental findings in research with human participants: Ethical challenges for psychologists (apa.org)
[7] Managing Incidental Findings in Human Subjects Research (nih.gov)
[8] Council of Europe. (2021, January 18). Details of Treaty No. 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[9] United Nations Publication. 2016. Data protection regulations and international data flows: Implications for trade and development. United Nations Conference of Trade and Development. https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf
[10] Chapter of Fundamental Rights of the European Union. (2012/C 326/02). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN
[11] OECD. 2013. The OECD Privacy Framework. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[12] 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. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN
[13] European Parliament. (2021, 18 January). Personal Data Protection. Fact Sheets on the European Union. https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection
[14] 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). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN
[15] Regulation (EU) 2018/1725 of the European Parliament and of the council of on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC 23 October 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN
[16] The Economist. (2017, May 6).The world's most valuable resource is no longer oil, but data.https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
[17] Szczepański, Marcin. January 2020. Is data the new oil?. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf
[18] European Commission. (2021, January 18). The General Data Protection Regulation (GDPR), the Data Protection Law Enforcement Directive and other rules concerning the protection of personal data. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
[19] 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 (OJ L 199, 4.5.2016, p. 1) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN
[20] Wolters, P. T. J. (2018). The control by and rights of the data subject under the GDPR. https://repository.ubn.ru.nl/bitstream/handle/2066/194516/194516pub.pdf
[21] Samarati, P., & Sweeney, L. (1998). Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression.
[22] "What are Privacy-Enhancing Technologies (PETs)?", Medium 2020. [Online]. Available: https://medium.com/golden-data/what-are-privacy-enhancing-technologies-pets-8af6aea9923
[23] RedHat. (2021, 20 January). What is DevSecOps?. https://www.redhat.com/en/topics/devops/what-is-devsecops
[24] Myrbakken, H., & Colomo-Palacios, R. (2017, October). DevSecOps: a multivocal literature review. In International Conference on Software Process Improvement and Capability Determination (pp. 17-29). Springer, Cham.
[25] Dave Shackleford. March 2016. A SANS Whitepaper: DevSecOps Playbook. https://pages.cloudpassage.com/rs/857-FXQ-213/images/sans-a-devsecops-playbook.pdf

[26] Chris Romeo. (2021, 19 January). The 3 most crucial security behaviors in DevSecOps. https://techbeacon.com/devops/3-most-crucial-security-behaviors-devsecops
[27] Shannon Lietz. (2021, 19 January). Principles of DevSecOps. https://www.devsecops.org/blog/2015/2/21/principles-of-devsecops