Ref. Ares(2021)4883306 - 30/07/2021

IoT-NGIN

D4.1
Next Generation IoT PRESS Analysis & Confidentiality Requirements

WORKPACKAGE	WP4	**PROGRAMME IDENTIFIER**	H2020-ICT-2020-1
DOCUMENT	D4.1	**GRANT AGREEMENT ID**	957246
REVISION	V.1	**START DATE OF THE PROJECT**	01/10/2020
DELIVERY DATE	31/07/2021	**DURATION**	3 YEARS

© Copyright by the IoT-NGIN Consortium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 957246

DISCLAIMER

This document does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of its content.

This document may contain material, which is the copyright of certain IoT-NGIN consortium parties, and may not be reproduced or copied without permission. All IoT-NGIN consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the IoT-NGIN consortium as a whole, nor a certain party of the IoT-NGIN consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered using this information.

ACKNOWLEDGEMENT

This document is a deliverable of IoT-NGIN project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957246.

The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

PROJECT ACRONYM	IoT-NGIN
PROJECT TITLE	Next Generation IoT as part of Next Generation Internet
CALL ID	H2020-ICT-2020-1
CALL NAME	Information and Communication Technologies
TOPIC	ICT-56-2020 - Next Generation Internet of Things
TYPE OF ACTION	Research and Innovation Action
COORDINATOR	Capgemini Technology Services (CAP)
PRINCIPAL CONTRACTORS	Atos Spain S.A. (ATOS), ERICSSON GmbH (EDD), ABB Oy (ABB), INTRASOFT International S.A. (INTRA), Engineering-Ingegneria Informatica SPA (ENG), Bosch Sistemas de Frenado S.L.U. (BOSCH), ASM Terni SpA (ASM), Forum Virium Helsinki (FVH), Optimum Technologies Pilroforikis S.A. (OPT), eBOS Technologies Ltd (EBOS), Privanova SAS (PRI), Synelixis Solutions S.A. (SYN), CUMUCORE Oy (CMC), Emotion s.r.l. (EMOT), AALTO-Korkeakoulusaatio (AALTO), i2CAT Foundation (I2CAT), Rheinisch-Westfälische Technische Hochschule Aachen (RWTH), Sorbonne Université (SU)
WORKPACKAGE	WP4
DELIVERABLE TYPE	REPORT
DISSEMINATION LEVEL	PUBLIC
DELIVERABLE STATE	FINAL
CONTRACTUAL DATE OF DELIVERY	31/07/2021
ACTUAL DATE OF DELIVERY	30/07/2021
DOCUMENT TITLE	Next Generation IoT PRESS Analysis & Confidentiality Requirements
AUTHOR(S)	Djordje Djokic (PRI) Farhan Sahito (PRI) Dusan Pavlovic (PRI) Pekka Koponen (FVH) Veli Airikkala (FVH) Maria Anastasi (EBOS) Marios Sophocleous (EBOS) Philippos Philippou (EBOS)
REVIEWER(S)	Terpsi Velivassaki (SYN) Josep Escrig (i2CAT)
ABSTRACT	SEE EXECUTIVE SUMMARY
HISTORY	SEE DOCUMENT HISTORY
KEYWORDS	Privacy, Data Protection, Ethics, Societal Impact, Information Security

Document History

Version	Date	Contributor(s)	Description
V0.1	01/03/2021	PRI	ToC
V0.2	15/03/2021	EBOS	Chapter 4
V0.3	01/04/2021	FVH	Chapter 3
V0.4	15/05/2021	PRI	The first draft
V0.5	01/06/2021	PRI	Updates
V0.6	22/07/2021	i2CAT	Internal review
V0.7	26/07/2021	SYN	Internal review
V1.0	30/07/2021	PRI	The final version

Table of Contents

Document History 4
Table of Contents 5
List of Figures 6
List of Tables 7
List of Acronyms and Abbreviations, ... 8
Executive summary 9
Introduction 10
Relation to the Project Work 10
Structure of the Document 11
1 Privacy and Data Protection 12
1.1 Privacy and Data Protection – the Sources of Regulation 12
1.2 Methodology of Privacy and Data Protection 14
1.3 Privacy and Data Management Plan 14
1.4 The Structure of Data Management Plan 15
1.4.1 Categories of Personal Data and Purpose of Processing 16
1.4.2 Legal Grounds for Lawful Data Processing 17
1.4.3 International Transfers of Data and Data Sharing 18
1.4.4 Technical and Organizational Security Measures 18
1.5 Storage Limitation and Data Erasure 19
2 Ethics Compliance Management 21
2.1 Standards, Principles and Guidelines 21
2.2 IoT-NGIN Ethics Requirements 22
3 Societal Requirements 26
3.1 Concepts of Social Acceptance 27
3.2 Societal Methodology 28
3.2.1 Acceptance journeys 28
3.2.2 Acceptance journeys in detail 30
4 Information Security Requirements 32
4.1 Security legal framework 32
4.1.1 The Directive on Security of Network and Information System 32
4.1.2 EU Cybersecurity Act 33
4.1.3 The EU Cybersecurity Strategy 33
4.2 Security Methodology 34
4.2.1 The Approach 35
5 Conclusions 37
6 References 38
Appendix 1 - Glossary of Terms 39

List of Figures

Figure 1 – Methodology flow of Privacy and Data Protection 14
Figure 2 - The IoT-NGIN Data Management Components 15
Figure 3 - IoT-NGIN DMP: Main Elements 16
Figure 4 - IoT-NGIN within the EU Ethics Appraisal Procedure 22
Figure 5 - IoT-NGIN Social Acceptance Dimensions 27
Figure 6 - Binary acceptance journey's phases 29
Figure 7 - The semi-flexible acceptance journey's phases 29
Figure 8 - The acceptance of an intervention 30

List of Tables

Table 1 - List of Acronyms and Abbreviations 8
Table 2 - Overview of the IoT-NGIN Personal Data Processing Activities 16
Table 3 - List of standards, principles and guidelines applicable to IoT-NGIN 21
Table 4 – Ethics requirements, interpretations and action plans 23
Table 5 - Category areas for security checks 36
Table 6 - List of Terms and their Meanings 39

List of Acronyms and Abbreviations,

Table 1 - List of Acronyms and Abbreviations

Abbreviation	Meaning
CA	Consortium Agreement
CO	Coordinator
DMP	Data management plan
DOI	Digital Object Identifier
FAIR	FAIR Guiding Principles for scientific data management (Findable, Accessible, Interoperable and Re-usable data)
GA	Grant Agreement
GDPR	General Data Protection Regulation
OA	Open Access

Executive summary

This document presents deliverable D4.1 – Next Generation IoT PRESS[1] Analysis & Confidentiality Requirements. It provides a comprehensive regulatory framework to the IoT-NGIN project, and it addresses the privacy and data protection issues, ethics compliance, societal concerns, technology acceptance and information security. Concerning the addressed fields, the objective and structure of this deliverable might be seen as multi-fold.

The section on the protection of personal data gives an overview of relevant privacy and data protection principles and it also covers the data security considerations. In addition, this document outlines the Data Management Plan (DMP) that provides details on the project partners' data management practice. This plan implements the risk-based approach to privacy and data protection. Nevertheless, The DMP should be viewed as a "living" document that will be maintained/updated in future, as the project progresses. Its purpose is to describe the data management lifecycle for the data to be collected, processed and/or generated. The societal aspects address the acceptance of project outcomes. Finally, an approach to information (cyber) security issues is also given.

[1] **P**rivacy, Data P**R**otection, **E**thics, **S**ecurity & **S**ocietal acceptance

Introduction

Protection of personal privacy and personal data protection are crucially important for the success of IoT-NGIN. In addition, transversal issues such as the ethics compliance, societal acceptance and information security are equally important, overlapping issues. In this context, this deliverable details how the IoT-NGIN consortium will manage these various but closely related aspects. However, the particular focus is on the processing and protection of personal data. The document provides an overview of the fulfilment of the ethics requirements within the project. Besides, this document addresses aspects required for ensuring the data security and provides an overview of the data processing activities (Data Management Plan – DMP).

The current document addresses the DMP as an ethics requirement (describing the life cycle of personal data processed within the project). The DMP is the living part of this deliverable and is based on the input provided by all project partners. The DMP provides information on the project data lifecycle, privacy, and the project's policies for data collection, storage, access, sharing, protection, retention, and destruction. Each project partner handling and responsible for data collected, stored or used in IoT-NGIN will ensure compliance with the strategy outlined in this document. All consortium members shall refer to this DMP, if questions about project's data policies and practices arise. Nevertheless, this deliverable does not concern the DMP as part of Open Data Pilot Requirement. This is a mandatory deliverable as the consortium takes part in the Open Data Pilot. The focus in this document is on the management of research information in general, and making it as open as possible and in accordance with the FAIR principles. Open Data Management Plan is part of the Deliverable D7.1, also due M6 (updated version M18). Both documents are considered as living registries and it is up to all project partners to provide timely reporting in case of changes in their data management practices throughout the project. Finally, the activities described here feed into the risk management component of IoT-NGIN.

Relation to the Project Work

This deliverable is deployed as a result of completing the task 4.1 of the project. The task analysed the three 'pillars' concerning application of the technologies in practice - fundamental rights framework, ethical and societal framework and other societal concerns. Therefore, this task cannot be considered as an isolated and separate unity. It is rather to be an analysis that affects other tasks and sets up constrains and instructions concerning development of technological solutions, procedures for its development and project outcomes in general.

This task and the deliverable presented via this document pervade other project tasks and deliverables. It is particularly noticeable by the fact that it outlines Data Management Plan (DMP). As already explained, the DMP encompasses ethical, legal, and managerial aspects of data processing and data protection. The managerial aspects shed light on procedures for processing personal data as well as technical and organizational measures that would be applied to secure data. The legal context is essential for development of appropriate regulation for project procedures and outcomes. Finally, ethics is considered as a benchmark for regulation. Also, ethics plays a fundamental role for social acceptance of innovative technologies at all levels. Therefore, all project activities shall comply with ethical principles and relevant national, the EU and international sources of law.

This deliverable sets up the general principles. For this reason, other tasks and deliverables must comply with promoted principles, and all partners should adhere to the principles. Only in that way, fairness, transparency, and accountability of the data processing will be ensured, the required quality of data will be preserved, and data confidentiality will be granted. Such approach should enable that innovative technologies are deployed as the project outcomes are socially acceptable.

Structure of the Document

As it is explained this deliverable covers four fields. Therefore, the document is composed of four main chapters.

After the introductory section, Chapter 1 is about privacy and data protection requirements. This section contains the Data Management Plan. Chapter 2 is dedicated to the Ethics Compliance Management component of the project. It addresses the position of IoT-NGIN within the EU's Ethics Appraisal Scheme. Chapter 3 sheds light on societal requirements and describes the approach to societal issues including social acceptance of project outcomes. Finally, information security aspects are addressed in Chapter 4.

The overall document is rounded up by conclusion.

1 Privacy and Data Protection

One of the earliest definitions of privacy states that privacy is 'the right to be let alone' (Warren and Brandeis, 1890). Definitions have been shaping the notion of privacy tending to conceptualize it as complete as possible. Nowadays, the concept of privacy is defined in various ways. Therefore, there are many privacy classifications and typologies, but nothing is written in stone, so additional development of privacy classes and subclasses is expectable.

One of many categorizations of privacy proposes four classes as follows:

- Information privacy
- Bodily privacy
- Territorial privacy
- Communication privacy (Densmore, 2019)

Information privacy contains rules that govern the collection and use of personal information. Bodily privacy is composed of rules that protect physical being and any jeopardize thereof. Territorial privacy protects the environment of an individual whereas communication privacy protects the means of correspondence and communication.

There is a common confusion between privacy protection and data protection. Notwithstanding of obvious similarities between these concepts, they are not the same. If we try to substitute data protection under any of the above-presented privacy classes, it might be easily inferred that the protection of personal data belongs to the class of information privacy. Nevertheless, this should be taken with caution. The processing of personal data might relate to all other classes. If we take into account that there is an extension of information classes that might be considered as personal data, it would not be difficult to find examples when processing personal data intrudes bodily, territorial and/or communication privacy. So, does it mean that informational privacy pervades all other classes of privacy? It would not be wrong to come up with such a conclusion, but informational privacy does not coincide with the full scope and meaning of other privacy classes. Privacy is a broader concept than personal data and thus privacy protection encompasses the protection of personal data.

The following chapters present regulatory sources for privacy and data protection as well as operational aspects of protection. These aspects take into account not only general regulatory requirements and elements of privacy management but also the context and needs of this project.

1.1 Privacy and Data Protection – the Sources of Regulation

As the one of the fundamental rights, privacy protection is regulated by the Universal Declaration of Human Rights (hereinafter UDHR). The UDHR enshrines in Article 12 that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." The privacy protection generates protection of related domains as personal data protection. Also, privacy enables the realization of other rights laid down by UDHR - security of person (Article 3), the right to freedom of opinion and expression (Article 19), and right to freedom of peaceful assembly and association (Article 20).

The European Convention of Human Rights (hereinafter ECHR) (ECHR, 1950), was adopted in 1950, and it has been effective since 1953. This convention is an essential instrument for protecting human rights and make them binding for signing states of Council of Europe. The Art 8 of the ECHR enshrines the right to respect for private and family life. This article encompasses a wide range of interests. Apart from private and family life it includes home and correspondence (including communication via mails, emails, phone). In addition, this article protects against arbitrary interferences by public authorities. However, this right is not absolute and hence a fair balance between the competing interests of the individual on one side and of the community on the other should be found. Therefore, contracting parties of the ECHR must develop mechanisms that balance the interests. The mechanism must be 'in accordance with law' and 'necessary in democratic society'.

The ECHR establishes the European Court for Human Rights (hereinafter ECtHR) which is one of the most significant guardians of human rights. This court has delivered more than 16,000 judgments. The ECtHR has developed the case law based on the Art 8 of the ECHR. The case law regulates situations when necessary, measures should be taken to protect each citizen against unjustified restriction of their fundamental rights including privacy. Also, the ECtHR regulated that States should not hinder the exercise of fundamental rights including the right to respect private life.

In the European Union, the Charter of Fundamental Rights of the European Union (hereinafter the Charter) (CFREU, 2000) is one of the most important sources of regulations. The Charter brings together the most important personal freedoms and rights granted by the EU Law into one legally binding document. Also, this source of regulation is superior to the Member States national laws. The Charter contains all rights granted by the ECHR including the right to privacy. The Charter regulates that private and family rights should be respected and enshrines that 'Everyone has the right to respect for his or her private and family life, home and communications.' Moreover, the Charter addresses some additional freedoms and rights in protection of personal data. Article 8 regulates the protection of personal data by granting that 'Everyone has the right to the protection of personal data concerning him or her'.

In addition to the case law of the ECtHR, the Court of Justice of the European Union has formed very comprehensive case law. The Court of Justice of the European Union courts have given rulings on various social issues including protection of personal privacy and personal data. Several dozens of cases decided by the court have provided a vivid perspective to privacy protection.

In 2016 the General Data Protection Regulation (hereinafter GDPR) (GDPR, 2016) entered into force. This regulation became fully effective in May 2018. Nowadays, the GDPR is crucial regulatory source for protecting natural persons with regard to the processing of personal data and on the free movement of such data. The GDPR unifies national systems and presents single law that regulate protection of personal data in the EU Member States. This source of regulation is an essential step to strengthen individuals' fundamental rights in the digital age.

Apart from the GDPR, the EU Data Protection Law contains additional sources such as the ePrivacy Directive (ePrivacy, 2000) and the Data Protection Law Enforcement Directive (DPLE, 2018). Many of currently valid sources are under revision whereas additional regulations are under development.

1.2 Methodology of Privacy and Data Protection

Methodology for privacy and data protection should be well-structured and holistic approach. It generates appropriate privacy management that creates the framework of privacy program. The privacy program framework allows meeting legal compliance requirements and reduces the risk of privacy violation and data breach. Properly structured approach regarding protection of privacy and personal data should prevent sanctions that regulators may impose to entities that violate data protection and privacy regulations. In addition, the development and execution of a proper privacy program increases trust and confidence in this project and its outcomes. Therefore, the program positively affects the exploitability of the results and the social acceptance of the delivered technologies. Also, it should not be underrated that having a privacy program raises awareness about importance of privacy protection and in that way builds the culture of privacy and data protection.

The privacy management combines management principles and privacy regulations. It considers relevant regulation from various jurisdictions tending to implement concepts such as privacy by design end privacy by default. A privacy program can fulfil some or all of the following requirements:

- to identify privacy obligations relevant to certain organization, project or activities
- to identify privacy-related risks
- to identify existing and develop missing policies and procedures
- to create, revise and implement them
- to promote positive practice of privacy and data protection

Figure 1 – Methodology flow of Privacy and Data Protection

In the context of this project, privacy management and privacy program are converged in the Data Management Plan. The structure of the plan is presented in this deliverable by parts that follow.

1.3 Privacy and Data Management Plan

The data management plan is created to ensure that data used for the purpose of project realization is properly and lawfully processed. This plan contributes to the transparency of the data flow as well as addresses data utilization (the use of data during the project realization). The DMP regulates data utilization throughout the whole project lifecycle starting from data creation till reuse of data after the completeness of the project. The plan underpins the development, organization, and improvement of required policies and procedures. Taking into account the data protection risks, the plan includes technical and organizational measures that are supposed to secure data. Therefore, the plan supports data integrity and assurance.

Figure 2 - The IoT-NGIN Data Management Components

Execution of the DMP requires involvement of all consortium partners. This plan is not a static document. It is a living program that must be constantly developing. Therefore, relevant stakeholders should support activities that promote and develop the DMP. In that way privacy-related culture, and relevant project policies and procedures will be developed and/or updated.

The privacy management and data protection in general within an EU Project are not an exclusive job of the project coordinator or the partner(s) leading ethics and privacy issues. It is necessary to engage many individuals whose functions should enable proper execution of the privacy program and the DMP. Also, relevant stakeholders must function as a well-organized team. Therefore, this DMP should not only increase awareness about privacy importance but also involve relevant individuals in the program and align their tasks around the goals of the privacy program.

1.4 The Structure of Data Management Plan

This Data Management plan is composed of the following sections:

- Categories of personal data and purpose of processing
- Legal grounds for lawful data processing
- International transfer of data and data sharing
- Technical and organizational measures
- Storage limitation and data erasure

More about each section of the plan is presented in the following parts.

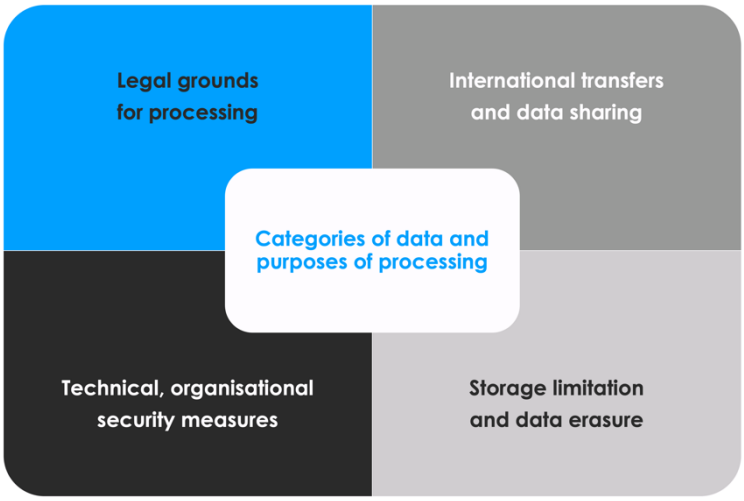

Figure 3 - IoT-NGIN DMP: Main Elements

1.4.1 Categories of Personal Data and Purpose of Processing

The following table contains information about data that is going to be processed within the realization of the project. The overview is composed of indication on categories of personal data, data subjects and purpose of data processing.

Table 2 - Overview of the IoT-NGIN Personal Data Processing Activities

Data subject	Category of personal data	Purpose of processing
Project partners' representatives	Identification Data PII (Name, Surname, email address)	Communication for the purpose of project realization Organization of meetings
	Profession and employment related data Current employment (employer, title, role)	Communication for the purpose of project realization
	Identification Data PII (Name, Surname, email address)	Authentication of a user to project management platform
	Audio-visual Data Photographs, video shots, voice recordings	Communication and dissemination activities Testing and validation of Computer Vision and Speech Recognition algorithms
Advisory Board Members	Identification Data PII (Name, Surname, email address)	Contacting and Interaction with members Organization of meetings
	Profession and employment related data Current employment (employer, title, role description, specialization)	Selection and establishment of the Advisory Board

	Career (prior employment and employers) Review (performance review, possibilities) Education and training Professional qualification (Certificates and professional trainings) Professional experience (Professional interest, research interests, academic interests)	
External people that participate in project trials and research activities	Identification Data PII (Name, Surname, email address)	Gathering opinions via interviews for the purpose of evaluation of project activities
	Audio-visual Data Photographs, video shots, voice recordings	Communication and dissemination activities Testing and validation of Computer Vision and Speech Recognition algorithms
Newsletter subscribers	Identification Data PII (email address)	Commercial communication (Sending newsletter)

1.4.2 Legal Grounds for Lawful Data Processing

One of the most important requirements of data protection legislation is to process personal data lawfully. Lawful data processing refers to data processing that is allowed. In other words, data processing must be carried out within the constraints of the applicable laws. Applicable laws include data protection law as well as laws and regulations form other fields. The GDPR prescribes six legal grounds to ensure lawful processing of personal data:

- consent,
- the performance of a contract,
- legal obligation,
- the vital interest of individuals,
- public interest and
- the legitimate interest.

When personal data processing is consented by data subject the consent must be informed, freely given, specific and unambiguous, given in an affirmative form. When these requirements are met, data processing might be considered as lawful. Prior to data processing, data subject must be properly informed about all relevant aspects of processing data related to him/her. The scope, nature of data, the purpose and consequences of processing should be clearly explained. Relevant information must be given a manner that warrants proper understanding of facts concerning personal data processing. Finally, the evidence about consenting must be collected and recorded.

When other grounds for data processing are used, data controller or processor should ensure that the grounds are appropriate to grant lawful processing. For instance, if a controller uses its

legitimate interests to ground lawfulness of data processing, controller must ensure that its interests do not override interests of data subjects' freedoms and rights.

1.4.3 International Transfers of Data and Data Sharing

The project partners will exchange data for the purpose of the project realization. All project partners are based in the European Union. Therefore, the exchange of data among them should be realized without the necessity to comply with the Chapter V of the GDPR. However, if it would be necessary to share data outside the EU or to transfer data in countries that are not on the adequacy list of countries (decided by the European Commission) then data transferring will be carried out in accordance with appropriate safeguards regulated by the Chapter V of the GDPR. In addition, the relevant Case Law, European Data Protection Board opinions and recommendations, as well as relevant national Data Protection Authorities decisions concerning data transfer to third countries and international organizations must be taken into consideration whenever data is transferred to third countries or international organizations.

Project partners are allowed to transfer personal data to third parties that will process data on their behalf. Whenever they transfer data to third parties that will process data on their behalf, not only requirements imposed by the Chapter V of the GDPR (if a third party is based outside EEA or in a country from 'adequacy list') but also appropriate safeguards, and particularly those regulated by art. 28 of the GDPR must be in place. Third parties must process data only on documented instructions from the project partner as well as in accordance with other requirements imposed by the agreement concluded by the partner and a third party.

1.4.4 Technical and Organizational Security Measures

Each project partner must implement appropriate technical and organizational measures to ensure security of personal data processing, take into account the state of the art, the costs of implementation, the nature, scope, context and purpose of personal data processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each project partner must assess appropriateness of any measure.

To assist the project partners with addressing the ethics requirements and to effectively protect personal data several recommendations in terms of information security are given. Their objectives are:

- Satisfying the security needs,
- Identifying reasonably foreseeable and internal risks to security and unauthorized access to the network,
- Minimizing security risks, including through risk assessment and regular testing.

As a part of the information security efforts a designated staff should coordinate and be accountable for the information security program. The information security efforts are composed of:

- Technical controls,
- Physical controls,
- Administrative controls.

1.4.4.1 Recommendations on Technical Controls

Data access controls – Each project partner should allow access to data on 'need-to-know' bases. Therefore, all reasonable measures should be taken to ensure that personal data is accessible and manageable only by authorized staff. Persons entitled to use a data processing system must have access to the personal data to which they have access privileges. Personal data cannot be read, copied, modified or removed or otherwise processed without appropriate authorization.

Network access controls – Project partners are responsible for securing data while data is being processed on their infrastructure. Therefore, the use of firewalls or functionally equivalent technology as well as authentication controls measures may be required.

1.4.4.2 Recommendations on Physical Security

Physical Access Controls – Each project partner keeps physical components of the network in own facilities. Physical barrier controls must be used in order to prevent unauthorized entrance to the facilities. Passage through the physical barriers at the facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel. Visitors are required to sign-in with designated personnel, must show appropriate identification, and are continually escorted by authorized employees while visiting the facilities.

Limited Access - The access to the facilities should be granted to the staff and contractors who have a legitimate business need. When there is no longer has a reason for the access privileges assigned to staff/contractor, the access privileges should be promptly revoked.

Other Physical Security Controls - All project partners should maintain their access in a secured (locked) state. It is recommended that all access points to the facilities are monitored by video surveillance cameras. The surveillance system should be designed to record all individuals accessing the facilities. Also, electronic intrusion detection systems designed to detect unauthorized access to the facilities, with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the facilities are recommendable to be used. All physical access to the facilities by staff and contractors should logged and routinely audited.

1.4.4.3 Recommendations on Administrative Controls

The security of network and associated services should be periodically audited. It is necessary in order to determine whether additional or different security measures are required to respond to both – existing and new security risks. It is recommendable to review information security program at least once per year.

The incident response plan should be maintained. The plan should be viewed as the cornerstone for responding to potential security threats that my affect personal data. Incident response plan should help to handle potential personal data breach including implementation of corrective action and mitigation of adverse effects on data subjects.

1.5 Storage Limitation and Data Erasure

The principle of storage limitation should ensure that personal data is stored only for a period necessary for the fulfilment of the data processing purpose for which data has been initially

collected. After that period, data will be erased. However, if there are requirements of mandatory law, personal data might be kept for a longer period. Also, data might be kept for a longer period if there are reasons related to the public interests, scientific or historical and statistical purposes.

2 Ethics Compliance Management

This chapter addresses the main lines of the overall ethics compliance management. The ethics has transversal nature and hence it is important for all project aspects. For this reason, this chapter sets out details on how the consortium should manage potential ethical issues according to applicable regulatory frameworks, ethical and data protection standards and other ethics requirements. The IoT-NGIN Consortium understands that the research has ethical implications and confirms its commitment to respect the ethical standards and rules of H2020. We also confirm that the ethics standards and guidelines of Horizon2020 will be rigorously applied, regardless of the country in which the research takes place. All partners will conduct research in accordance with the fundamental principles of research integrity, such as reliability, honesty, respect and accountability. Moreover, adherence to these principles should prevent misconduct, such as plagiarism, fabrication, and falsification.

2.1 Standards, Principles and Guidelines

To ensure the adequate ethics compliance of its research activities, the IoT-NGIN consortium relies on the standards, guidelines and principles provided either as official guidance to project participants by the EC, or the relevant legally binding documents such as the GDPR or the Rules on Participation in Horizon 2020.

Table 3 - List of standards, principles and guidelines applicable to IoT-NGIN

Applicable standards, principles and guidelines
European Commission, The Roles and Functions of Ethics Advisors/Ethics Advisory Boards in EC- funded Projects
European Commission, Guidance Note for Researchers and Evaluators of Social Sciences and Humanities Research
European Commission, Ethics Guidelines for Trustworthy AI
European Commission, A comprehensive strategy on how to minimize research misconduct and the potential misuse of research in EU funded research
European Parliament and the Council, Regulation (EU) 2016/679 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR)
European Commission Directorate-General for Research & Innovation, H2020 Programme Guidelines on FAIR Data Management in Horizon 2020, Version 3.0, 26 July 2016
European Commission, H2020 Programme Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020, Version 3.2 21 March 201711
Research integrity standards, for instance, in the ALLEA European Code of Conduct for Research Integrity
H2020 regulation: Article 19 "Ethical principles"
Rules for Participation: Article 12 "Proposals" and Article 13 "Ethics Review"
Grant Agreement (GA): Article 34 "Ethics"
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)

2.2 IoT-NGIN Ethics Requirements

After the successful scientific evaluation of the proposal, IoT-NGIN was evaluated by a panel of ethics experts. This is part of the EC's Ethics Appraisal Scheme (check Figure 4). The ethics panel conditionally cleared the project. The conditional ethics clearance the IoT-NGIN received includes:

- Ethics requirements,
- Submission of further information/documents beyond what was included during the proposal submission

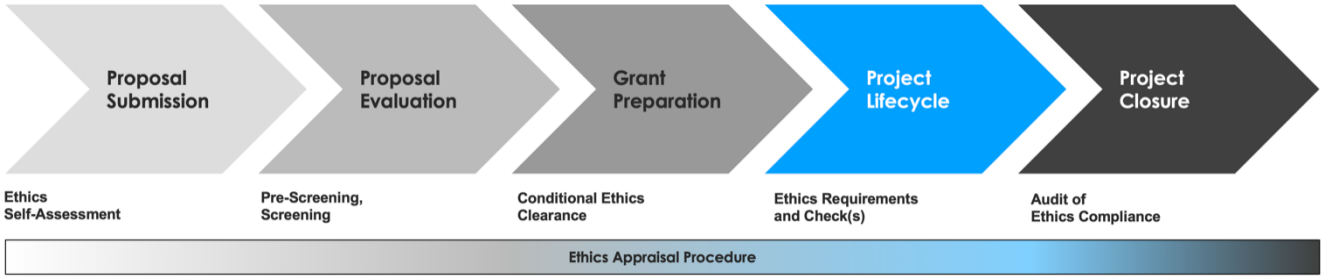

Figure 4 - IoT-NGIN within the EU Ethics Appraisal Procedure

It must be stressed that each coordinator and beneficiary is responsible for identifying any potential ethical issues. Also, ethical aspects of the project/research must be handled properly. Finally, each coordinator and beneficiary should specify plan to address ethics issues in sufficient details. This is also complementary with the article 34 of the Grant Agreement on "Ethics".

When complying with the ethics requirements the overall goal is to provide the Ethics Panel with details and information exactly what they are looking for. In some cases, it explains what the Ethics Panel expects to receive from the consortium (e.g. what kind of information or documentation should be submitted in fulfilment of a particular requirement).

The conditional ethics clearance means that the project can run but the clearance is subject to conditions that must be included as "ethics requirements". These ethics requirements concern the following categories:

- Human beings,
- Protection of Personal Data,
- Potential Misuse of Data,
- Environment, health & safety.

The interpretation of the Ethics Requirements the project received is given in this document as follows in the sections/tables below.

Table 4 – Ethics requirements, interpretations and action plans

Deliverable	Requirement	Interpretation / Action Plan
D10.1 H – Req. No.1 Lead: CAP	**2.1**. The procedures and criteria that will be used to identify/recruit research participants must be submitted as a deliverable. **2.2**. The informed consent procedures that will be implemented for the participation of humans must be submitted as a deliverable. **2.3**. Templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants) must be submitted as a deliverable.	**2.1** - The Ethics Summary Report (EthSR), references the pages in the submitted proposal and indicates: • *collection of documentation of end-users needs and opinions; such activities include surveys and feasibility studies, courses and workshops as well as field trial demonstrations (p48)* • *preliminary details concerning informed consent procedures and documents used to obtain their consent have been provided in Part B2 Ethics* • *Over 30 types of IoT devices will be tested in several environments and scenarios where human's involvement is required via wearable devices, smart phones and other systems or devices that may impact on or monitor human behaviour.* • *Additional details are needed to describe the human participants involved in project activities (i.e. trials and other activities indicated in Part B p. 85)* To address this requirement, the coordinator have requested from all partners organising activities with human participants to provide their feedback and describe in sufficient detail the inclusion/exclusion criteria. **2.2** - To address this requirement the coordinator should check back with partners responsible for project activities involving individuals external to the project (i.e. students, experts in workshops, survey participants) and get feedback on how the partners intent to recruit research participants and manage the consent. The feedback required from partners concerns who the participants are, what they are required to do, how they will be informed, how their informed consent will be given/saved/withdrawn etc. **2.3** - The partners responsible for organising research activities with individuals external and internal to the project should provide templates of the informed consent forms + information sheets they intent to use in order to inform participants about the project and manage their consent. These templates must be GDPR-compliant (i.e. include all the information about who does the research, DPO contact info, what to do to withdraw, how to withdraw etc).

D10.2 POPD – Req. No.2 Lead: CAP	**4.2** The host institution must confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR a detailed data protection policy for the project must be submitted as a deliverable. **4.4** The beneficiary must explain how all of the data they intend to process is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation 'principle). This must be submitted as a deliverable. **4.5** The beneficiary must explain whether and why the research data will not be anonymised/ pseudonymised. This must be submitted as a deliverable. **4.6** A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants must be submitted as a deliverable. **4.8** Description of the anonymysation/pseudonymisation techniques that will be implemented must be submitted as a deliverable. **4.13** In case the research involves profiling, the beneficiary must provide explanation how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded. This must be submitted as a deliverable.	**4.2** – For all requirements in this section, the EthSR indicates: • *Project will utilise open data sets and citizen volunteered data for designing accessible on-demand cocommuting solutions on social networks (p13)* • *Personal data may be collected as part of Living Labs in Helsinki/Tallinn, Helsinki/Pitäjänmäki, Barcelona and Terni (p22)* To address this particular requirement, the coordinator should make a list of all partners, and ask them to either 1) provide the contact information of their DPO or 2) provide a short project-specific privacy policy in case they are not legally bound to have a DPO. In addition, all partners who are organising activities involving humans (D10.1) must include the information of the DPO in their consent/assent forms and information sheets. **4.4** – The consortium partners responsible for technology development and the ones who collect the personal data must explain how the personal data is they process relevant for what they do. The categories of personal data processed must be trimmed down to the necessary minimum. In short - the partners must demonstrate that the personal data they collect is in proportion with what they process it for. The consortium partners must collect only what they really need, and not keep this data longer than needed. **4.5** – In accordance with the EthSR: *It is not entirely clear when and why personal data will not be anonymized in compliance to GDPR and other national, EU or H2020 data protection regulations.* Consortium partners (beneficiaries), processing personal data to develop the project outcomes must justify why they need "raw" personal data instead of using only pseudonymised or even anonymised data. Please note that pseudonymisation is reversible (replacing identifiers with numbers e.g. 239sIKs9 instead of John). Pseudonymous personal data remains under the scope of GDPR. Anonymisation is irreversible (removal of all identifiers without possibility of re-identification of data subjects). **4.6** – The ethics requirements 4.6 and 4.8 are closely related. To address this particular one, the coordinator should get feedback from all partners involved in data processing activities on the relevant privacy safeguards which will implement within the project. These may include encryption, access controls such as passwords, description of physical security where the files are kept etc. **4.8** – Following the logic of the requirement 4.6, the project partners should describe if they plan to use anonymisation techniques during the research (i.e. for the pilots if we process personal data). This information should be presented under one chapter, per partner. **4.13** – The EthSR states: *The proposal does sufficiently not clarify weather wearable technologies and other devices will be used to track behaviour or collect other personal data from human subjects involved in use cases or other activities.* To reduce the scope of this requirement and focus only on the relevant partners, it would be prudent to seek the technical coordinator's advice on which partner may engage in tracking of individuals during the project. These partners should provide their feedback

	4.15 In case of further processing of previously collected personal data (e.g. data from social media T7.2), 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.	on these particular activities. Once collected, the information should be presented in one document. **4.15** – The Ethics Summary Report specifically mentionnes "*user volunteered data on social networks (p14 of the submitted proposal)*". "Previously collected personal data" means personal data which was collected for a different purpose. In the case of IoT-NGIN, the data from social media will be used. The EC Ethics Team wants to see that the partners collecting the data from social media have a valid legal basis for this (for example contract, legitimate interest, etc). In some cases, social media platforms may have specific Terms of Use and closed APIs which means that the use of the personal data within the IoT-NGIN must be in respect to those Terms and APIs as well (and not infringing on them).
D10.3 M – Req. No.3 Lead: CAP	**10.1**. Risk assessment and details on measures to prevent misuse of research findings must be submitted as a deliverable.	**10.1** - The EthSR states the following: *The project includes research and testing activities designed to protect IoT systems at risk of cyber- attacks. Also, a secure by design approach will be implemented to both protect confidentiality, integrity and cybersecurity and prevent malicious tasks.* It would be good idea to reduce the scope of this requirement (not to contact all the partners, but to work only with selected ones i.e. technical coordinator). Also, in terms of subject matter, we focus only on the research activities concerning the risk of cyberattacks and also mass surveillance.
D10.4 EPQ – Req. No.4 Lead: CAP	**7.1**. Further information about the possible harm to the environments tested in the different trials caused by the research and the measures that will be taken to mitigate the risks must be submitted as a deliverable. **7.3**. The applicant must demonstrate that appropriate health and safety procedures conforming to relevant local/national guidelines/legislation are followed for staff involved in this project. This must be submitted as a deliverable.	**7.1** – With regard to project activities where the Ethics Panel perceives potential harm to the environment - it is required that the consortium describes (in particular for the project trials) - what kind of safeguards are in place to reduce or completely avoid the risks these activities may cause to the environment. **7.3** - "The applicant" in this case refers to project partners engaging in research activities that may expose to health/ safety risk its own staff (researchers). The Ethics Panel focuses on the trials/pilots. To clearly assign the responsibility for such activities to a specific project partners, the Ethics Panel requires confirmation that 1) health and safety procedures exist and are in place and 2) confirmation that these procedures correspond to local legal requirements applicable in the country where these research activities take place. The EthSR states: *Additional details are needed to assess the risks and potential impact of the proposed technologies on human life, industrial, city settings, infrastructures, agricultural practices and work conditions*. The two ethics requirements included within D10.4 are closely related. The best way forward is to address both of them at the same time.

3 Societal Requirements

The following review of academic literature gives an overview of the current state of research on social acceptance of innovative technologies deployed in smart cities and communities, helps to understand the different concepts, and approaches to the subject.

The research on social acceptance of technological innovations has been a popular research field since the 1980s and gained great scientific importance in the last decades, especially the research on acceptance of renewable energy technologies (GAEDE & ROWLANDS, 2018)[2]. Social opposition and resistance against the expansion of technological innovations, especially of renewable energy technologies and corresponding infrastructure and the question how a greater level of public acceptance can be achieved, generally induce studies on social acceptance. (EKINS, 2004)[3]. A widespread social acceptance is crucial for the successful implementation and operation of modern technologies in the public sphere.

Some of the planned test domains of IoT-NGIN ('Smart Cities' & 'Smart Grid') have direct contact with the public presuming, therefore a great deal of attention to the possible concerns and conceptions of the general public should be noticed. While not so visible or obvious to the citizen, 'Smart Agriculture' and 'Smart Industry 4.0' domains also have effects and indirect consequences to the lives of the population. New technologies, even when deployed and operated under private ownership are known and operated by private citizens. Transparency of information is crucial when dealing with street cameras, car charging and agricultural or industrial automation alike. The digital sphere, especially with increasingly accurate simulative models is touching on important aspects such as privacy concerns. The digital twin concept, of crucial importance to the IoT-NGIN project, too, can be an efficient and informative tool that need to be nevertheless examined with lawful scrutiny and full transparency and adaptability to concerns and objections coming from any stakeholder involved.

Renewable technologies and their ascent into everyday life have been a used subject for scientific examination and have, indeed, provided a literal framework for understanding key factors in social acceptability in emerging technologies.

In the renewable energy sector various technologies capture different natural resources in different ways causing the consequences on environment, economy and society to deviate from one another (DEVINE-WRIGHT, 2008)[4]. This idea could be extended to concern different technologies in general validating the assumption that consequences on the environment, economy and society vary and have to be carefully examined on an individual level.

The academic research referenced in this chapter will emphasize studies focusing on renewable energies because of its predominance in the field of social acceptance studies. There exists an extremely wide range of studies focusing on social acceptance of renewable energy technologies, but only a limited number of studies considering the acceptance of smart city solutions. While the research on renewable energy technologies often focuses on siting decisions and respective social acceptance, studies on smart city and its technologies rather

[2] Gaede, J.; Rowlands, H. (2018): Visualizing social acceptance research. A bibliometric review of the social acceptance literature for energy technology and fuels. In: Energy Research & Social Science, vol. 40, pp. 142-158.

[3] Ekins, P. (2004): Step changes for decarbonizing the energy system: research needs for renewables, energy efficiency and nuclear power. In: Energy Policy, vol. 32, pp. 1891-1904.

[4] Devine-Wright, P. (2008): Reconsidering public acceptance of renewable energy technologies: A critical review. In: Jamasb T., Grubb, M., Pollitt, M. (Eds): Delivering a Low Carbon Electricity System: Technologies, Economics and Policy. Cambridge University Press

investigate the social acceptance in terms of using specific technologies or pursue the question whether the provided technologies cause a change of behaviour. Social acceptance of smart city development and smart city solutions in general is a large field as it contains a wide range of different technologies and thematic areas as well as having rather fuzzy limits to distinct it from other fields of research.

3.1 Concepts of Social Acceptance

So far, there are different popular approaches, concepts and definitions in the field of social acceptance theory. Firstly, DEVINE- WRIGHT (2008)[5] distinguishes three different scales of implementation of renewable energy technologies considering different impacts on the local economy, community and public attitudes:

- micro (at single building or household level)
- meso (at the local, community or town level)
- macro (at the large scale 'power station' (level)

In a different approach, WUESTENHAGEN proposes a concept breaking social acceptance into the following dimensions: socio-political acceptance, community acceptance, and market acceptance. By considering three dimensions as well as respective sub-dimensions, the proposed model is differentiated and might cover the complexity of social acceptance. [6]

Figure 5 - IoT-NGIN Social Acceptance Dimensions

In their bibliometric review on social acceptance research for energy technologies, GAEDE & ROWLANDS (2018) conclude that the schema of social acceptance with the dimensions of community, market and socio- political acceptance remains one of the most popular approaches on this topic.

[5] Devine-Wright, P. (2008): Reconsidering public acceptance of renewable energy technologies: A critical review. In: Jamasb T., Grubb, M., Pollitt, M. (Eds): Delivering a Low Carbon Electricity System: Technologies, Economics and Policy. Cambridge University Press

[6] Wuestenhagen, R.; Wolsing, M.; Bürer, M.J. (2007): Social acceptance of renewable energy innovation: An introduction to the concept. In: Energy Policy, vol. 35, pp. 2683-2691

While most of the literature studies energy solutions, other fields are represented. BARETTA (2018), for instance, conducted an analysis on social impacts of smart environmental projects implemented in Italian cities. The study, which referred especially to social inclusiveness and eco-gentrification, reveals that smart environmental projects focusing on mobility and energy have significant risks for causing eco-gentrification and not including all societal groups due to the use of advanced technical tools (BARETTA 2018: 119f.)[7] This is not an isolate finding and reflects the overall tendency for resources (financial or otherwise) to accumulate disproportionately. To ensure inclusiveness and preserve a vibrant and efficient community, capacity building efforts should be properly planned and resourced. Especially in areas that have otherwise been neglected in terms of technological development efforts in this regard produce cumulative results.

3.2 Societal Methodology

During previously conducted multi-case analysis, findings have suggested that all case studies can be analyzed according to two criteria: three different phases of their journey over time (design, delivery and use) and three different levels of actors (micro, meso and macro) which have an influence during these phases. Based on these criteria we can distinguish three different patterns, which we present below. The different patterns help to see which tools for social acceptance need to be employed for whom and at what time in this journey.

The definition of the three different levels of actors is based on the previous chapter where the distinction is made according to Devine-Wright into three different levels of interventions and their impacts on the local economy, community and public attitudes is introduced: these are characterized as micro (at single building or household level), meso (at the local, community and town level) and macro (at the large-scale level).

For the following, the Devine-Wright's categorization has been adapted as follows:

- Micro level –individuals & households influence the intervention
- Meso level – the local community & town actors influence the intervention
- Macro level – the regional & national actors / policies influence the intervention

These constitute the levels of actors which have an influence on the acceptance journey at different times. In addition to these different levels, the journeys consist of the following three phases:

- Design – where the details of the interventions are decided
- Delivery – where the intervention is put into place
- Use – where the intervention is used

3.2.1 Acceptance journeys

Based on an analysis of these two categories of levels and phases of acceptance journeys, we can find differences in the levels of actors, which have an influence on relation to the stages of the journey. According to these phases, we have identified three different types of acceptance journeys. For the visual representation, we have displayed the different phases at an equal length. This is to offer an easy visual comparison on the differences in the levels of

[7] Baretta, I. (2018): The social effects of eco-innovations in Italian Smart cities. In: Cities, vol. 72, pp. 115-121.

actors involved. In practice, the length of the different phases may of course not be equal. The respective levels of actors that influence the different phases strongly influence the scope and the point of time during the acceptance journey when different measures to increase social acceptance for an intervention are to be implemented. The three different acceptance journeys are described as follows.

Binary Acceptance Journey

The binary acceptance journey (delivery is final without influence of micro level) is characterized by the fact that the macro (regional & national) and meso (local community & town) levels of actors of this journey influence both the design and delivery of the intervention. The micro level (individual & household), and hence the user, only influences the use of the intervention. The journey is considered "binary" in the sense that once the intervention is delivered, the infrastructural decision being made beforehand cannot be reversed. Therefore, it is crucial to include important points for user acceptance into these infrastructural decisions. The divide between the macro/meso and micro level characterizes the binary acceptance journey as an acceptance journey that consists of two parts. Regional / national level such as policies as well as local, community stakeholders, influence the binary acceptance journey in the design and the delivery of the intervention. The decisions made in the design phase are influenced by national policies / financial investment decisions. In the binary acceptance journey's, the micro level influence is limited to the user phase. The binary acceptance journey's phases are illustrated below:

Figure 6 - Binary acceptance journey's phases

Semi-Flexible Acceptance Journey

Compared to the binary acceptance journey (delivery is final without influence of micro level) in the semiflexible acceptance journey the macro (national & regional) as well as the meso phases (local community & town actors) cover the design of the intervention and the micro level (individual & household) is covering the delivery and the user phase. This implies that changes to the intervention can still be made during the delivery phase depending on users' feedback for example what part of a retrofitting package to use. During the design and the delivery phase of the intervention, regional and national factors play a role; however, the micro level (individual & household) plays also a part (user orientation). This means that there is room to adapt the delivery of the intervention according to users' feedback, which can be used to increase the intervention's acceptance. The semi-flexible acceptance journey's phases are visualised below:

Figure 7 - The semi-flexible acceptance journey's phases

Flexible Acceptance Journey

The flexible acceptance journey is characterised by the macro (national & regional) and meso (local community & town actors) level only covering part of the design phase and the micro level (user level, individual & household) influence during the design (to a limited extent) and delivery of the intervention as well as the use. Therefore, the user can have an influence already earlier in an intervention's journey. This means that feedback loops can be implemented with the users, where even the design of the intervention can be adapted. This is a very important opportunity to increase the acceptance of an intervention. This journey is outlined in the visual below:

Figure 8 - The acceptance of an intervention

3.2.2 Acceptance journeys in detail

Binary Acceptance Journey

Upon review of the described interventions, the use cases planned in these cases represent a binary acceptance journey. Both deployments will be executed in privately owned enterprises (Bosch, ABB & Cooperative Winery of Nemea) leaving little to no influence to the user regarding the design and delivery.

Smart Agriculture

The use case is expected to combine various types of sensors gathering data and drones to assess the evolution of the crops, detect diseases and optimize irrigation and fertilization as well as mobile robots to support manual harvesting.

Much of the impact will be on the meso level, developments affecting local communities and employees. Good understanding of this level is important for the acceptance journey.

Smart Industry 4.0

In both use cases of this domain, an extra information layer will be developed to aid the usage of and track assets important to the manufacturing process. Much like in the agriculture counterpart, the impact will be on the meso level.

Semi-Flexible Acceptance Journey

Smart City

With 3 different use cases the Smart City domain offers a heterogenic pallet of applications. The emphasis of this domain in the IoT-NGIN project is to adopt cross-border-by-default twin city capabilities between Helsinki and Tallinn. The use cases vary from traffic (motorized and pedestrian) monitoring to crowd management and seeking co-commuting solutions. Some of these applications will rely heavily on micro level engagement to assure social acceptance and might therefore fall under the flexible journey category. Sensor installations in the urban landscape are processes that are very meso and micro level heavy in terms of influence. Most of the sensors that collect data have been installed already though and this work can be seen

as an ongoing process. Monitoring devices in public spaces is a very sensitive subject and requires careful consideration. While all Devine-Wright's categories are involved in these scenarios, extra attention has to be given to micro level influence. Information acquired from this process needs to be incorporated in deployment actions to ensure optimal acceptance.

Flexible Acceptance Journey

Smart Grid

This domain contains two use case scenarios. One aims to develop features like voltage quality analysis functions and Micro Synchro Phasor Measurement for advanced grid monitoring. The second one involves users outside the domain in form of Electric Vehicles' (EV) drivers. While the first mentioned use case follows the patter of binary acceptance journey, the second strongly involves micro-level users. For a successful roll-out the micro level users are part of the design and delivery phases of the pilot.

4 Information Security Requirements

Most organisations often acknowledge that security should be an important consideration when developing systems however, business performance and cost often precede security. It is satisfying to see that awareness is raised on security issues but instead of security considerations throughout the lifecycle, companies focus on applying security practices only at the initiation of the development or in the final design, which often affects the efficient application of security on the final product. Evidently, what is required is integrating security at every step a from initiation to design and development and then to deployment to maintenance, as an effective way to protect against cyber threats. This sequential approach is what is called the Security-by-Design (SBD) and it is the suggested approach to capture risks and vulnerabilities deriving from the different technologies proposed within the IoT-NGIN.

The scope of this Chapter is to consider and present common risks and vulnerabilities in the proposed IoT-NGIN technologies, that can tamper with security, compromising the functionality, safety, and privacy of the IoT-NGIN. Additionally, the legal framework forming the current legal framework for security is also presented.

4.1 Security legal framework

4.1.1 The Directive on Security of Network and Information System

The Directive on Security of Network and Information Systems (NIS Directive, 2016) is applied horizontally in the EU aiming to increase the Union's cybersecurity. The NIS Directive into force in August 2016 and Members States transposed it into national laws by 9 May 2018. In 2020, the NIS Directive was reviewed and in December of the same year, a revised legislative proposal was submitted.

The NIS Directive was designed to improve Member States' cybersecurity capabilities; the cooperation between Member States; and Member States' supervision of critical sectors. The Directive established a culture of risk management and incident reporting among key economic actors - operators providing essential services (OES) and Digital Service Providers (DSPs). The Directive also set out cooperation mechanisms, such as the NIS Cooperation Group and the network of national computer security incident response teams (CSIRTs).

The NIS directive aims to provide legal measures that can boost the overall level of cybersecurity in the EU by ensuring:

- Member States' are equipped appropriately to face cyberthreats preparedness. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,
- Collaboration between Member States, with the formation of a Cooperation Group that will ensure support between the States by facilitating strategic collaboration and transparency in the exchange of information
- Creation of security culture across sectors that are vital for economical and societal progress

Businesses identified by the Member States as operators of essential services in the above sectors will have to take appropriate security measures and to notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the new Directive.

In the new Directive, the scope of application was extended and includes these additional sectors: water & waste management, public administration, and space sectors. It also considerably expands cooperation between the authorities of the Member States throughout the Union. It provides for an obligation of the competent authorities to exchange cybersecurity information (Art. 1 II lit. c draft NIS2 Directive), expanded tasks of the cooperation group (Art. 12 draft NIS2 Directive) and the CSIRT network (e.g. Art. 13 III lit. b draft NIS2 Directive) as well as the establishment of a European network for massive cybersecurity incidents made up of the competent national authorities (Art. 14 draft NIS2 Directive). Therefore, it goes significantly further than the previous regulation showing that the implementation of the NIS Directive to date has not been sufficiently consistent and that the aim is to tighten the legal obligations and achieve greater EU-wide harmonisation.

4.1.2 EU Cybersecurity Act

ENISA is the European Agency for Cybersecurity tasked to set up and maintain a pan-European cybersecurity framework, mandated by the EU Cybersecurity Act to prepare the technical specifications that would grant certification of cybersecurity under specific certification schemes.

Article 1 of the EU Cybersecurity Act provides the scope of the document as that of high level of cybersecurity, cyber resilience, and trust by ensuring the proper functioning of the European market. Specifically, the scope is presented in the two points below directly from the Act:

(a) objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and
(b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

Within the IoT-NGIN project, the EU Cybersecurity Act and the NIS Directive will be consulted upon in parallel to ensure that a high level of cybersecurity is achieved within the project.

4.1.3 The EU Cybersecurity Strategy

The EU Cybersecurity Strategy was also presented in December 2020 and its focus is to ensure trust and security within the new digital era. The strategy will build on three actions that would work in harmony to achieve high levels of cybersecurity. The Strategy will be implemented via procedures that establish resilience, technological sovereignty, leadership, ones that enhance proactivity and collaboration by building operational capacity to prevent, deter and respond, and last by promoting collaboration with international partners ensuring global cybersecurity protection of human rights and fundamental freedoms (New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient, 2021) .

4.2 Security Methodology

According to Mayer, "security requirements describe a solution domain by defining a condition we wish to make true by installing the system to mitigate risks" (Mayer, 2009). For the purposes of this deliverable, we refer to a generalised approach regarding security requirements as specific sets will be decided upon during further developments of the project. The specific requirements of the project with regards to security will be defined through the work conducted under WP5 – Enhancing IoT Cybersecurity & Data Privacy and its respective deliverables, which report on the enhancement of IoT Cybersecurity (D5.1 - D.5.2) and the enhancement of IoT Data Privacy and Trusts (D5.3 – D5.5). To reach a set of security requirements prior to beginning the software development lifecycle, it is advisable that one considers elements from several disciplines from information security and requirements engineering to software application engineering and even organizational behaviour (Crook, Ince, Luncheng Lin and Nuseibeh, 2002). As mentioned previously, omitting security considerations in from the start and throughout the development cycle can result in exhaustion of resources and unnecessary additional cost. Security requirements can be captured and later assessed with the use of questionnaire roadmaps directed towards both the stakeholders and the software developers. The questionnaire can be designed against an initial set of simplified questions that map the usefulness of the questionnaire as they are presented below.

- What are you trying to secure against?
- Who are you trying to secure against?
- How do you understand security?
- Who or what should provide security?
- What ways do you believe should be used to provide security?

The basis and the overall approach of the security methodology relies heavily on three factors:

- What the project objectives are and the scope of work
- What kind of data will be collected or produced during the lifetime of the project and the Data Management Plan (DMP)
- What the risk assessment has shown and of course the analysis of concerns in the whole PRESS domain outlined in previous sections of this document.

Earlier sections of this report identify the project objectives, whilst the risk assessment is performed through Task 9.3. Finally, the DMP of the project is documented in D7.1: Data Management Plan. The outcome and findings of these reports will give the necessary focus to the Information Security domain aiming towards a relevant and coherent approach to address security aspects. Risks and nature of data to be processed will guide the preventive actions to be taken for immediate and effective results.

The IoT-NGIN GA has recognized the importance of the Ethics and Data management aspects and as such it has addressed in detail the overall approach. This is laid out in section 5 page 138 of the GA and in summary the discussion relates to:

- The recognition for full compliance and adherence to current EU legislation and practises/ recommendations and the current document is a proof of this commitment
- The fact that throughout its activities (example research participation and surveys) the project will fully respect the well-being, rights and interests of the human participants involved.
- All technical and organizational measures needed to ensure above will be designed and implemented.

4.2.1 The Approach

The Security Methodology consists of several steps, numbered below:

- A continuous and dynamic **assessment of the risks** prevailing, and the data collected/ produced by the project. The risk registry and data inventory need to be assigned to specific work parts and project work packages for easier and more targeted actions
- A continuous evaluation of the **impact of these risks** within the framework of the PRESS context and in liaison with the risk assessment function.
- A continuous **scan of the external (to the project) environment** for new requirements, regulations, or any other development that the project must attend to should the need arise.
- The design of necessary and **relevant technical and organizational measures** to minimize or eliminate specific risks especially the high-impact ones. These measures should be incorporated at the design phases of the architectural building blocks (protection-by-design) for a more effective design of a robust and secure infrastructural environment.
- The **identification and maintenance** of the sources of data, the storage locations of data, of any data transfers executed because of project needs, the parties with access to data and their compliance to data protection and whether the users accessing the data are authorised to do so always within the project scope, data policies and framework.
- A clear and simple **communication path** to all consortium members to emphasize the need for proper data management and precautionary actions as well as easy avenue of monitoring until the end of the project. The methodology and processes must be clearly understood and communicated in writing to avoid any misunderstandings or confusion as to what needs to be done and by who.
- A continuous **monitoring activity** by the relevant project partner to ensure compliance to the security policies. On a similar note, **the recording of actions** and results is always a must to guarantee auditability of the system to any auditing authority. Proof must be provided of actions taken and results.

4.2.2 Security Requirements for IoT

Large numbers of security requirements can be found in existing literature and need to be met by any system for it to be secure. Standard security requirements as described in (Pal, Hitchens, Rabehaja, & Mukhopadhyay, 2020) should be met for IoT devices to be secure and specifically for IoT-NGIN, to be granted security clearance and show that consideration over risks and threats was performed. Task 4.3: Pervasive Security and Ambient Intelligence based Control deals with access control, along with security, privacy and trust management of IoT devices in IoT-NGIN. In general, key security requirements applicable for all systems are listed below:

- Confidentiality
- Access Control
- Authentication
- Authorization
- Availability
- Key Management
- Integrity
- Trust
- Non-repudiation
- Accountability

- Usability

Deciding on the security requirements one must consider a variety of areas to capture as many security aspects as early as possible, before starting to develop a system (Silva, 2015), (Reznik et al 2017). An indicative list of actions that can be implemented to meet security requirements for four of the requirement categories can be seen in

Table 5 below.

Table 5 - Category areas for security checks

Categories	Actions/Measures
Integrity	Access control, Non-repudiation, Physical protection, Attack detection
Confidentiality	Access control, Physical Protection, Security Policy
Accountability	Non-repudiation, Attack detection
Availability	System recovery, Physical protection, Security policy

IoT systems carry certain concerns that should be considered and mitigated to meet security requirements and comply with the relevant legal frameworks. Such concerns include but are not limited to: the resource-constrained nature of things, end-to-end security, privacy of the users and data, scalability-being able to support large volumes of data, interoperability, real-time data and federation ensuring that security policies of all domains involved are enforced.

5 Conclusions

Focusing on privacy and data protection, ethics, security & societal aspects this deliverable identifies and analyses concerns associated with each field in the context of the realization of Iot-NGIN project. Nevertheless, this document does not only focus on potential threats but also provide solutions to overcome obstacles that may hinder the realization of the project and/or use of the project outcomes.

The chapter on privacy and protection of personal data creates the legal framework applicable to the context of the project realization. Moreover, the Data Management Plan outlined in this chapter should be perceived as self-regulation that all project partners should adhere to. The DMP provides a practical and usable dimension of general (or even abstract) provisions of data protection legislation.

The DMP's foundation could be found in ethical requirements. Ethics is a transversal issue and ethics compliance substantially affect societal acceptance. This is pointed out in the second chapter that provides instructions on how to comply with concrete requirements in this field. Equally important and to a certain extend overlapping issue (with all other fields) is information security. Even though that there is a separate chapter on information security, there are also instructions on how to secure data in the DMP.

Finally, proper protection and securing of data as well as being compliant with all ethical requirements contribute to trustworthiness. Prevention of both discrimination and stigmatization as well as acting in favour of European citizens living/wellbeing might be seen as social requirements. Taking into account that there are social requirements and concerns related to social acceptance of the project and its outcomes the separate chapter is dedicated to this issue. The chapter explains the notions of societal requirements and social acceptance. Also, different forms of social acceptance are elaborated.

6 References

Densmore, R. (Ed.). (2019): Privacy Program Management; Tools for Managing Privacy Within Organization (Second ed.). IAPP Publication.

Devine-Wright, P. (2008): Reconsidering public acceptance of renewable energy technologies: A critical review. In: Jamasb T., Grubb, M., Pollitt, M. (Eds): Delivering a Low Carbon Electricity System: Technologies, Economics and Policy. Cambridge University Press.

Devine-Wright, P. (2008): Reconsidering public acceptance of renewable energy technologies: A critical review. In: Jamasb T., Grubb, M., Pollitt, M. (Eds): Delivering a Low Carbon Electricity System: Technologies, Economics and Policy. Cambridge University Press.

Ekins, P. (2004): Step changes for decarbonizing the energy system: research needs for renewables, energy efficiency and nuclear power. In: Energy Policy, vol. 32.

European Commission. (n.d.). *Adequacy decisions; How the EU determines if a non-EU country has an adequate level of data protection.* An official website of the European Union. Retrieved July 26, 2021, from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Gaede, J.; Rowlands, H. (2018): Visualizing social acceptance research. A bibliometric review of the social acceptance literature for energy technology and fuels. In: Energy Research & Social Science, vol. 40.

The Council of Europe. (1950). Convention for the Protection of Human Rights and Fundamental Freedoms. Rome.

The European Parliament and The Council of The European Union. (2016). 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. Luxembourg: Office for Official Publications of the European Communities.

The European Parliament and The Council of The European Union. (2002) 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). Luxembourg: Office for Official Publications of the European Communities.

The European Parliament and The Council of The European Union. (2018). Directive (EU) 2016/680 — protecting individuals with regard to the processing of their personal data by police and criminal justice authorities, and on the free movement of such data. Luxembourg: Office for Official Publications of the European Communities.

The European Parliament., & Office for Official Publications of the European Communities. (2000). Charter of fundamental rights of the European Union. Luxembourg: Office for Official Publications of the European Communities.

Warren, S. D., & Brandeis, L. D. (1890): The Right to Privacy. Harvard Law Review, vol. 4(5).

Wuestenhagen, R.; Wolsing, M.; Bűrer, M.J. (2007): Social acceptance of renewable energy innovation: An introduction to the concept. In: Energy Policy, vol. 35.

Appendix 1 - Glossary of Terms

Table 6 - List of Terms and their Meanings

Term	Explanation
Data management plan	A plan that includes information on the handling of research data during and after the end of the project, what data will be collected, processed and/or generated, which methodology and standards will be applied, whether data will be shared or made open access and how data will be curated and preserved (including after the end of the project). (H2020 Guidelines on FAIR Data Management, 2016)
Open access	Open access (OA) refers to the practice of providing online access to scientific information that is free of charge to the end-user and reusable. 'Scientific' refers to all academic disciplines. In the context of research and innovation, 'scientific information' can mean peer reviewed scientific research articles (published in scholarly journals) or research data (data underlying publications, curated data and/or raw data). (H2020 Guidelines to the rules on open access to Scientific Publications and Open Access to Research Data in Horizon 2020, 2017)
Personal data	Any data relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Research data	Information, in particular, facts or numbers, collected to be examined and considered as a basis for reasoning, discussion, or calculation. (H2020 Guidelines to the rules on open access to Scientific Publications and Open Access to Research Data in Horizon 2020, 2017)
Scientific information	Can mean peer-reviewed scientific research articles (published in scholarly journals) or research data (data underlying publications, curated data and/or raw data). (H2020 Guidelines to the rules on open access to Scientific Publications and Open Access to Research Data in Horizon 2020, 2017)