Legal & Ethical Compliance Guide

D12.1

July 2021

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Deliverable

PROJECT ACRONYM	GRANT AGREEMENT #	PROJECT TITLE
TWINERGY	**957736**	**Intelligent interconnection of prosumers in positive energy communities with twins of things for digital energy markets**

DELIVERABLE REFERENCE NUMBER AND TITLE

D12.1

Legal & Ethical Compliance Guide

Revision: v1.0

AUTHORS

Arthur van der Wees	Anna Ida Hudig	Dimitra Stefanatou	Prakriti Pathania	Valeria Righi
Arthur's Legal B.V.	Arthur's Legal B.V.	Arthur's Legal B.V.	Arthur's Legal B.V.	IDEAS FOR CHANGE

Funded by the Horizon 2020 programme of the European Union
Grant Agreement No 957736

DISSEMINATION LEVEL

✔ P Public

C Confidential, only for members of the consortium and the Commission Services

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Version History

REVISION	DATE	AUTHOR	ORG…	DESCRIPTION
v0.1	15.06.2021	Dimitra Stefanatou	Arthur' Legal	Creation of initial Table of Contents
v0.2	30. 06. 2021	Anna Ida Hudig	Arthur' Legal	Initial input under chapters 1, 2 and 3
v0.3	07.07 2021	Prakriti Pathania	Arthur's legal	Additional input under chapter 2
v0.4	19.07.2021	Valeria Righi	IDEAS FOR CHANGE	Input under chapter 3
v0.5	21.07.2021	Arthur van der Wees	Arthur's Legal	Input across the entire document
v0.6	22.07.2021	Prakriti Pathania	Arthur's legal	Consolidation of input and editing across the entire document
v0.7	23.07.2021	Dimitra Stefanatou	Arthur's legal	Refinements across all chapters
V0.8	30.07. 2021	Prakriti Pathania, Anna Ida Hudig, Dimitra Stefanatou	Arthur's Legal	Integration of reviewers' comments and submission of the final version to the coordinator
v1.0	31.07. 2021	Prakriti Pathania, Anna Ida Hudig, Dimitra Stefanatou	Arthur's Legal	Draft submitted to EC by the PC

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Statement of Originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Executive Summary

Work Package 12 of TwinERGY provides for ethics, legislation and standardisation related aspects pertinent to the project's scope. This document falls under Task T12.1 on identification of legal and ethics requirements and aims to provide guidance to technical partners at the early project stage. To this end, the document puts forward a Pilots' Guide a set of suggested questions based on the analysis of various applicable regulations and related perspectives from a European Union perspective, this, in order to enable and facilitate the partners contributing to the pilots' activities.

Based on their nature, perspective and scope, the identified regulatory frameworks that are either already applicable or currently proposed can be sorted into different categories. This report introduces two variables that help classifying the frameworks: the direction and the perspective. The direction could be horizonal, vertical, or a converged ecosystem. Horizontals focus on 'non-functionals' or attributes such as safety, security and privacy, that reoccur as an essential dimension across different verticals. Verticals, however, are market or sector-specific. Driven by the increased complexity and our increased dependability of digital products, systems and services, the converged ecosystems, as a third category, is taken increasingly often as the most efficient approach to start with. Applied to the TwinERGY pilots, this would mean that the 'owner' can be a producer and/or a consumer and/or a storage provider and/or an exchange manager.

These directions will be mentioned and discussed across the clusters of regulations in each of the four perspectives: (1) market-centric, (2) human-centric, (3) system-centric and (4) data-centric. Regulations are not necessarily bound to one or two perspectives. Rather, the perspectives resemble a spectrum or lens through which light can be shined on the specific subject matter, in this case the TwinERGY project. The subject matter can then be regarded on the basis of three separate scales: small scale (e.g., individuals or households), medium scale (e.g. neighbourhoods) or large scales (e.g. communities or towns). This, as the applicability of regulatory frameworks can depend on the scale on which a project is performed.

(1) The market-centric perspective is the most generic perspective, as it represents the views and interests of the whole range of different market actors. This can be local, regional, national, European or Universal (e.g., the United Nations). The relevance of the market-centric frameworks discussed in this report will, naturally, increase as the project scale increases.

(2) Human-centric regulations focus on the different persona of stakeholders involved in this projects, such as users, owners, consumers, producers and investors. A range of regulatory frameworks is discussed in this section. Some focused on protecting the rights of individuals, such as the right to privacy and data protection, as well as on consumer protection. These regulations are of relevance for TwinERGY, mostly by

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

making provisions for the processing of personal data. Others are more geared towards digital identity and payment services.

(3) Furthermore, rather than positioning the individual at the core of the related provisions, the Cybersecurity Act and the Artificial Intelligence Act are relevant for TwinERGY, as they provide for the technological, or cyber-physical systemic, aspects aspect, entailing obligations for those who provide or develop certain systems. Yet also product liability and product safety provisions are important.

(4) For the data-centric regulations provisions with regards to the free flow of non-personal data cross EU borders will be most relevant, given the transnational nature of TwinERGY.

The subsequent deliverables D12.2 -1st Year Legal and Ethical Compliance Report and D12.3 - 2nd Year Legal and Ethical Compliance Report will produce an interim and final assessment respectively on the extent to which the aspects covered by the present report are taken into account, especially by the TwinERGY pilots. It will further elaborate also on the applicability of the regulatory framework to the TwinERGY Project.

In addition, this deliverable provides a short questionnaire for ethical review, corresponding to a following summary of general principles of ethics. These ethical principles are primarily centred around a participatory and empowering approach we aim to use, taking into account the ambitions of the TwinERGY project as a whole. In this respect, the present report put forward five sets of ethical principles.

1. More specifically, the first set of principles is that of equity, diversity and inclusion (EDI), which points at encouraging and enabling participation of everyone, including vulnerable or marginalised communities.

2. The second principle relates to a recruitment process built upon empathic, honest, and trustworthy relationships with participants, for example by being transparent and realistic about the impact as well as the required efforts.

3. Thirdly, TwinERGY encourages democratic and empowering participation, by aiming to move away from the relationship ‘expert vs. research/data subject’, and instead strive for more equal relations between those involved.

4. Furthermore, TwinERGY aims to approach the use cases in such a way that they actually respond to societal needs, taking into account the local context and the realities of the participant.

5. The final set of principles focuses more specifically on data, striving for a citizen- or human-oriented approach to data collection and governance; not only the data collection processes should be made transparent to participants, but they should also be granted authority over their own data and have the opportunity to engage in data collection processes themselves.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Although the above list of ethical principles may not exhaustive, it is intended to act as a useful tool in the context of the piloting activities.

Overall, the work captured in the present document relates to the work conducted under Work Package 13 on Ethics Requirements, in particular under D13.1 'H- Requirement No. 1' and D13.2 'POPD Requirement No.2' reports, submitted in January 2021. In particular, the aforementioned deliverables focused mostly on the specific legal and ethics requirements pertinent to the involvement of research participants in the piloting activities of TwinERGY, as these requirements are defined under the General Data Protection Regulation (GDPDR). To this end, the earlier stated WP13 deliverables provided, for instance, for the consent forms to be used by each pilots and described the related recruitment process. The present deliverable although it does take into account processing of personal by TwinERGY pilots, it goes beyond the area of personal data protection by discussing a series of other currently applicable (proposed) regulations in key areas for TwinERGY, such as the area of consumer protection and cybersecurity. Furthermore, this deliverable takes into account the work conducted under Work Package 2 on Stakeholder Requirements, Obstacles to innovation and Business Models and, more specifically, of D2.1 Best practice guidelines for engaging citizens in the pilots and metrics for diversity and inclusion, submitted in June 2021.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Index

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

List of Figures

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

1. Introduction

The energy utility grid has to characteristic properties: it is highly regulated, and highly critical for businesses, citizens and governments. This emphasises the need for a thorough analysis of regulatory frameworks, whilst taking into account the perspectives of different stakeholder groups.

This Chapter produces an overview of TwinERGY project, focusing on the purpose and scope of the present deliverable, on the stakeholder analysis, as well as on the related methodology pursued.

1.1 Purpose and Scope

TwinERGY will introduce a first-of-a-kind Digital Twin framework that will incorporate the required intelligence for optimising demand response (DR) at the local level without compromising the well-being of consumers and their daily schedules and operations. The main idea behind the conception of the TwinERGY project lies on the interest of the project partners to exploit the new business opportunities that project implementation delivers and increase the relevance of the DR optimisation tools and strategies in the new generation of energy management systems. By coupling mature practice for citizen engagement with service innovation through the lens of public value, TwinERGY will ensure that a wide range of interests – especially those of consumers/prosumers – will be represented and supported in the energy marketplace.

In this context, TwinERGY will develop, configure and integrate an innovative suite of tools, services and applications for consumers, enabling increased awareness and knowledge about consumption patterns, energy behaviours, generation or demand forecasts and an increase in local intelligence via properly established Digital Twin-based Consumer-Centric Energy Management and Control Decision Support mechanisms that locally optimise demand response.

Key use cases will be trialled across 4 pilot regions making use of cutting-edge methods and tools. Special focus is provided on standardization and policy & market reform as key enablers for the successful commercialisation of the TwinERGY results. Additional attention is given to establishing knowledge transfer and exchanging synergies with similar projects listed under the BRIDGE Initiative, while explicit focus will be given on the establishment of close collaboration with the projects funded under the LC-SC3-ES-5-2018 topic, to further reinforce and catalyse collaborative advancements in research, innovation, regulatory and market issues around Demand Response, RES Integration and Consumer Engagement.[1]

[1] TwinERGY Consortium. Grant Agreement – 957736 – TwinERGY, August 2020.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

In light of the scope and aims of TwinERGY project as a whole, Work Package 12, in particular, provides for the Ethics, Legislation and Standardisation related aspects. To this end, the present document falling under the scope of Task 12.1 on the Identification of Legal and Ethics Requirements produces an inventory of the main applicable high level regulatory and ethical requirements of horizontal relevance across all pilots. To this end, the deliverable builds on the work conducted under Work Package 13 on Ethics Requirements, as captured under D13.1 'H- Requirement No. 1' and D13.2 'POPD Requirement No.2', submitted in January 2021; it, also, takes into account the work conducted under Work Package 2 on Stakeholder Requirements, Obstacles to innovation and Business Models and, more specifically, of D2.1 Best practice guidelines for engaging citizens in the pilots and metrics for diversity and inclusion, submitted in June 2021.

Overall, considering that TwinERGY evolves around data sharing, citizen engagements and energy generation, usage and exchange, it is of critical importance to pave the way for the adequate protection of the interests of consumers, communities and organizations possibly exposed to certain risks by the implementation of TwinERGY solution throughout the project duration and beyond. In this context, this document aims to serve as a guide -primarily-addressed to pilot partners, in order to navigate them through the most relevant legal requirements and ethical considerations at an early phase of the process. This document is, thus, not intended to provide a complete and comprehensive overview of the related aspects nor of the full theoretical framework covering data ethics. Updates of the present document will be provided under D12.3 1st Year Legal &Ethical Compliance report due in month 24, as well as under D12.4 2nd Year Legal &Ethical Compliance report, due in month 36 of the project.

1.2 Stakeholder Landscape

Producing a stakeholder landscape falls under an Ecosystem Analysis Phase, in the context of which the individual stakeholders in the ecosystem are identified, information flows between stakeholders are mapped, and appropriate standards are outlined. Examples of these stakeholders can be identified under the Grant Agreement, including in a wider context, consumers, governments, energy aggregators, distribution system operators, service providers, community organizations and other non-government actors[2] (Figure 1)

Stakeholder mapping is an important tool to identify all persons acting in multiple capacities, as well as organisations that can influence or are affected by the activities of the project, and how they are connected. Stakeholder mapping is reflected, in essence, under the TwinERGY tasks and deliverables. Work Package 2, for instance, covers stakeholder requirements, obstacles to innovation and business models. More specifically, D2.2 provides for a stakeholder analysis, including KPI's, Scenarios and Use Case Identification (D2.2). Similarly, D2.1 expands on the best practice guidelines for engaging citizens in the pilots and metrics for diversity and inclusion.

[2] TwinERGY Consortium. Grant Agreement – 957736 – TwinERGY, August 2020, page 161

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

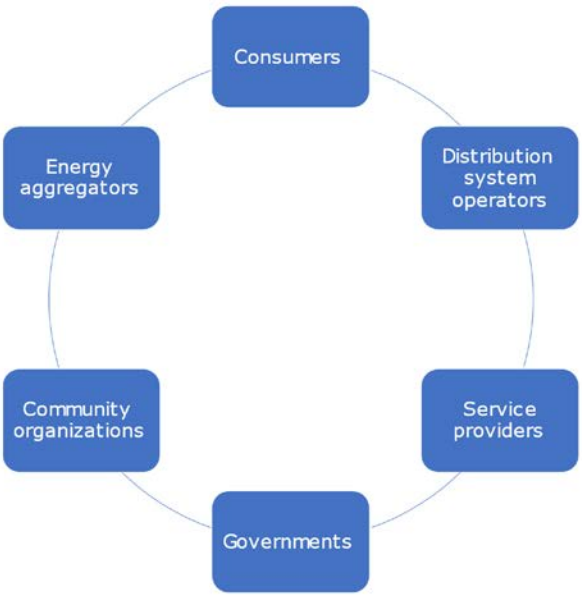

Figure 1: Stakeholders identified in TwinERGY Grant Agreement.

Furthermore, in view of identifying effectively the applicable legal requirements and relevant ethical considerations, it is of key significance to identify beforehand the interactions between stakeholders, as well as the links between the stakeholders, the stakeholder qualifications and the related interests. Apart from those depicted in Figure 1, there are, however, more stakeholders who play a role in the project, even though they may not be obviously identified at first sight. In this respect, a framework for outlining the multi-angled stakeholders and influencers in a human-centric technology ecosystem is captured in Figure 2 below.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Figure 2: Multi-angled stakeholders & influencers.

When applied to the information available on the TwinERGY use-cases at this early stage, this holistic framework allows for the identification of the following stakeholders or stakeholder groups:

1. The user: prosumers, that is, the households that generate and consume electricity in the TwinERGY pilots. Others to be identified in the context of the TwinERGY use cases,
2. Customers: to be identified in this context
3. Suppliers & value ecosystems: service providers, including software developers, information system providers, grid operators, smart meter vendors, energy generation and consumption technology vendors, data controllers and processors, and others to be identified.
4. Ecosystem and society: the environment, including the impact of material mining, transport & end-of-life of TwinERGY infrastructure, as well as the local emissions and GHG emissions of the electricity generated. Furthermore, the people indirectly involved with the pilots are stakeholders, such as members of the community that do or do not profit from the TwinERGY project although not directly involved. Others to be identified
5. Malicious actors: hackers, frauds.
6. Data absorbers and data brokers: to be identified in this context.
7. Policy makers, standardisation organisations & markets: EU, national governments, standardisation in cybersecurity, data market and energy market. Further to be identified in the pilot use cases.
8. Authorities: local, national and European, and universal.
9. Data access: law enforcement, intelligence services & others

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Note that the regulations to be discussed in the subsequent chapter -among others- provide, also, for the role of most of the above-mentioned stakeholders.

1.3 Methodology

The work captured in the present document forms the outcome of desk research, as well as with interactions with WP2 on Stakeholder Requirements, Obstacles to innovation and Business Models, as well as with WP13 on Ethics Requirements.

Based on their nature, perspective and scope, the identified regulatory frameworks that are either already applicable or currently proposed can be sorted into different categories. This report introduces two variables that help classifying the frameworks: the direction and the perspective. The direction could be horizonal, vertical, or a converged ecosystem. Horizontals focus on 'non-functionals' or attributes such as safety, security and privacy, that reoccur as an essential dimension across different verticals. Verticals, however, are market or sector-specific. Driven by the increased complexity and our increased dependability of digital products, systems and services, the converged ecosystems, as a third category, is taken increasingly often as the most efficient approach to start with. Applied to the TwinERGY pilots, this would mean that the 'owner' can be a producer and/or a consumer and/or a storage provider and/or an exchange manager.

These directions will be mentioned and discussed across the clusters of regulations to be discussed below under each of the four perspectives: (1) market-centric, (2) human-centric, (3) system-centric and (4) data-centric.

Furthermore, given that the present deliverable is based on input delivered by an interdisciplinary team of experts (e.g., legal experts, social scientists) the terms used, especially, in relation to the individuals acting in multiple capacities, for example, as consumers, data subjects, user are interchanged, as deemed appropriate for the scope of each chapter and section. This is particularly relevant for Chapter 2 and Chapter 3 focusing on the legal and ethical aspects respectively.

1.4 Target Audience

The present document is primarily addressed to TwinERGY pilot partners. Nevertheless, this document being a public deliverable it is not only addressed to the TwinERGY consortium and the European Commission services, but it will be -also- made available to the wider public through the project's website.

1.5 Structure

Following the present Chapter introducing the discussion captured in this deliverable, Chapter 2 produces a guide that aims to navigate primarily the pilot leaders through the most relevant currently applicable and proposed regulations at EU level; similarly, Chapter 3

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

produces a guide for the ethical principles applicable in the context of TwinERGY. Finally, Chapter 4 provides for the concluding remarks, while the consent form drafted for the purpose of the interviews carried out in Spring 2020 by the University of Lisbon by TwinERGY's legal partner (Arthur's Legal) are integrated under the Appendices.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

2. Regulatory Frameworks in the TwinERGY Era

With regards to the need to preserve and improve the environment, The Treaty of Lisbon requires EU policy on energy to, besides other aspects, promote energy efficiency and energy saving and the development of new and renewable forms of energy. The EU Green Deal further acknowledges the need to prioritise energy efficiency and to create a framework that fosters the deployment of innovative technologies and infrastructure, such as smart grids, hydrogen networks, energy storage and the like.

This Chapter dives into the regulatory landscape that is of relevance for TwinERGY and touches upon not only existing legislation but also legislations that may be implemented in the near future. While there are several other legislations such as the Open Data Directive, the Digital Services Act and the Digital Markets Act, however, given the initial stages that the said legislations were at the time of drafting the deliverable, the said legislation may be further elaborated upon in the subsequent deliverable i.e. D12.2 which is the 1st Legal and Ethical Compliance Report due in October 2023. For the scope of this TwinERGY, contract law remains relevant for the TwinERGY output. Any contractual arrangements in place should be in accordance with the relevant provisions dictated under the respective regulations.

For the sake of convenience and to provide a more structured overview, the chapter takes a lifecycle approach by categorising the relevant legislations into four overarching themes namely human-centric perspective, system-centric perspective, data-centric perspective and market-centric perspective. This chapter below discusses legislations which are of direct relevance for TwinERGY but does not provide an exhaustive list of all legislations applicable to the project. In addition, it is pertinent to note that this Chapter elaborates on legislations applicable at an EU level and that national laws pertaining to the pilots remain applicable. The regulations discussed below are primarily relevant for the three TwinERGY pilots i.e. the pilots taking place in Germany, Italy and Greece. The extent to which the regulations are relevant for the UK pilot, it is briefly touched upon in each section.

2.1 Pilots' Guide

The questions below are formulated to be addressed by technical partners in the TwinERGY consortium. For the purpose of a user-friendly questionnaire, the following questions do not make references to the regulations specifically discussed under the subsequent sections of chapter 2.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

The questions are in line with the discussions that follow in the upcoming sections on the applicable regulatory frameworks. The distinction of perspectives is not absolute, therefore certain regulations and questions can fall under several categories. The key aspects of these regulators to be further discussed are captured in the figure below.

Figure 3: Key aspects of regulations in the TwinERGY era.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Human-Centric Perspective

Questions below are based on the General Data Protection Regulation, the ePrivacy Directive and forthcoming Regulation, and Consumer Protection regulations

- Do the piloting activities include the processing of any **personal data**? Personal data could be, for example, a name, location, identification number, or physical, psychological, or social attributes of a person. Formally, personal data are any information associated with an identified or identifiable natural person.
- How will the data intended to process be relevant for the purposes of the research project (**data minimisation principle**)?
- What do the **data flows** between machines look like?
- What is the **lawful basis** for processing the personal data?
- Who **decides upon** personal data?
- Who **process** personal data (e.g., collection, storage, transmission)?
- **Where** does the processing of personal data take place, such as storage (e.g., within EU or outside of EU)?
- For **how long** is the data stored?
- **Who** can access the data, and do individuals have access to their own data?
- Is it technically possible for a user to execute its rights under the GDPR? For example, if a user wants to **stop sharing (part of) their personal data**, for privacy protection or other reasons, without stopping the infrastructure or devices from functioning.
- What **pseudonymization/anonymisation** techniques will be implemented?
- Did those whose personal data are collected provide **informed consented** for the processing of their data?
- Is there any kind of **profiling of individuals and groups** performed in the piloting activities by means of data processing, and if so, what are the consequences and how will the participants be informed about this?
- What **security measures** will be implemented to safeguard the (privacy) **rights and freedoms** of those whose data are collected?
- How will the end-point users in the project ecosystem be **authenticated** and **authorised**?
- Is there any non-personal data that, when analytics are applied to it, such as a pattern recognition algorithm, could **reveal information that can be related to an identified or identifiable person** or household, and could hence be qualified as personal data?
- How will the data be **securely stored**?

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

System-Centric Perspective

Questions below are based on the Cybersecurity Act andtThe Artificial Intelligence Act

- Which **intelligent systems** that are being used qualify as 'artificial intelligence systems' (e.g., demand-response systems, digital twins)?
- Who is **the provider or developer** of each of these intelligent systems?
- Who is **the user** of each of these intelligent systems?
- Are there any components of TwinERGY that could be certified on the short term, in the light of the provisions of the Cybersecurity Act as being discussed in Section 2.3.1?

Data-Centric Perspective

Questions below are based on the Free Flow of Non-Personal Data Regulation.

- What types of **non-personal data, if any,** are processed by the piloting activities?
- Who or what **sends** the information (e.g. a user, application, service provider or device)?
- Who or what **receives** the information? e.g. a user, application, service provider or device?
- Who is responsible for the **processing** (e.g. collection, storage or exchange) **of non-personal data**?
- Are the sender and the receiver of the information **authenticated** and **authorised**?
- What **security measures** will be implemented to secure the confidentiality, integrity and availability of the non-personal data?

Market-Centric Perspective

The NIS-Directive

- Given that the TwinERGY platform is currently unlikely to be identified as an operator of essential services, the market-centric regulations are unlikely to apply as being discussed in Section 2.4.

The figure below attempts to map the currently applicable regulations at EU level with the focus areas identified, namely networks, systems, data, applications and people. To this end, the mapping was based on the articles providing for the subject matter and scope under the respective regulations discussed. It should be made explicit that the focus area 'people' identified does not only cover end-users, but also people, in general, acting in their other capacities.

REGULATORY FRAMEWORKS IN THE TWINERGY ERA	PEOPLE	SYSTEMS	DATA	APPLICATION	NETWORK
General Data Protection Regulation	✓	✓	✓	✓	✓
Free Flow of Non-Personal Data Regulation	✓	✓	✓	✓	
Open (& Re-Use of) Data Directive, Data Governance Act* & Data Act*			✓	✓	
PSD2 & Regulatory Technical Standard	✓	✓	✓	✓	
ePrivacy Regulation *	✓	✓	✓	✓	✓
eIDAS Regulation *	✓	✓	✓	✓	✓
Cybersecurity Act	?	✓	✓	✓	✓
Digital Services Act *	?	✓	✓	✓	✓
Product Liability Directive *	✓	?	?	?	?
Contract Law, IPR Law & Tort Law	✓	✓	✓	✓	✓
NIS Directive 2.0 *		✓		Impact-Based?	✓

Figure 4: Applicable EU regulations and technology domain of interest[3]

[3] The (*) is added next to the title of regulations which are either under development or under update reviews, but either expected this year or in a few years from now.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

2.2 Market-Centric Perspective

When it comes to rules and regulations related to energy, there are five layers that need to be taken into consideration: local, regional, national, European, universal. For the purpose of this deliverable, this section along with subsequent sections focus on laws applicable on an EU level. In the context of the energy sector, the figure below shows that there are multi-persona in any prosumer ecosystems (either small, medium or large) and it will not only be about demand and supply of energy, but also demand and supply many other essentials, such as systems, data, applications and networks.

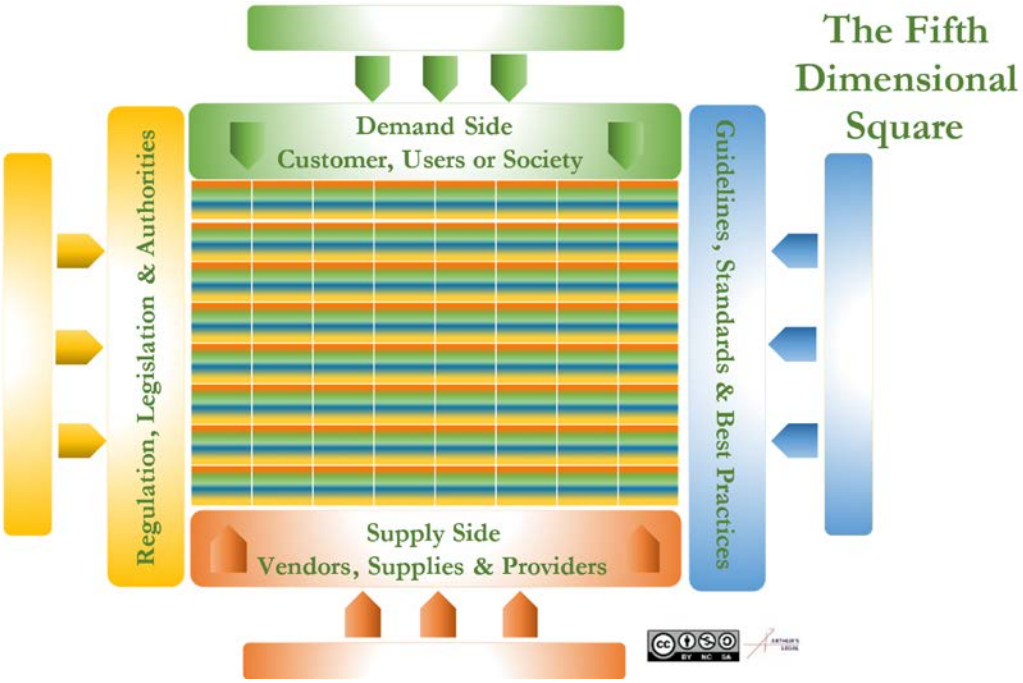

Figure 5: The Fifth Dimensional square

2.2.1 Directive on security of network and information systems (NIS Directive)

2.2.1.1 Scope, objectives, and key definitions

The Directive concerning measures for high common level of security of network and information systems across the Union ('NIS Directive')[4], applicable since May 2018, was the first piece of EU wide legislation that aimed at providing legal measures to increase the overall level of cybersecurity in the EU. The NIS Directive applies to operators of essential

[4] 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 OJ L 194, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

services, including electricity supply, energy, healthcare, transport as well as digital service providers. Overall, the NIS Directive lays down measures aimed at achieving a high level of security of network and information systems in the EU.

Despite the intention with which the NIS Directive was proposed, the implementation of the Directive as well as the national transposition by the EU member states was met with several obstacles. The Inception Impact Assessment published by the European Commission in June 2020 highlighted that due to the minimum level of harmonisation and the identification process applicable to operators of essential services, Member States opted for diverging approaches when implementing the NIS Directive.[5] This ultimately resulted in major inconsistencies and fragmentation in the regulatory landscape which could undermine the level playing field for certain operators.[6] Additionally, the fragmentation also resulted in certain sectors and actors that provide critical and economic activities, which are vulnerable to cyber incidents, from being excluded from the scope of the Directive.

In order to address the challenges faced during the implementation of the NIS Directive, the European Commission adopted a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive).[7] The European Commission also cited its priorities to make Europe fit for the digital age and to be build a future ready economy that works for people as an additional contributor for the proposal for the NIS 2 Directive.[8] With the NIS 2 Directive, the European Commission aims to align the previous NIS Directive with the dynamic technical and threat landscape and to make it more future proof. For this purpose, the scope of the NIS 2 Directive has extended to include more sectors and services that are either essential or important entities namely space, wastewater and waste management, public administration, providers of public electronic communications networks or services, digital services such as social media platforms. The distinction between operators of essential services and digital service providers which was made in the NIS Directive has also been removed under the proposal for the NIS 2 Directive.

2.2.1.2 Legal requirements under the NIS Directive

The NIS Directive was implemented with the intention of providing a risk framework based on operational aspects and losses, essentially economic in its nature. Under the Directive, Member States were required to ensure that operators of essential services and digital service providers take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they

[5] Combined Evaluation Roadmap/ Inception Impact Assessment, Revision of the NIS Directive, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:Ares(2020)3320999&from=EN

[6] Combined Evaluation Roadmap/ Inception Impact Assessment, Revision of the NIS Directive, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:Ares(2020)3320999&from=EN

[7] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

[8] Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72176

use in their operations.[9] Subsequently, in the event of incident, the said organisations were required to notify the relevant competent authorities without undue delay. An 'incident' under the NIS Directive is any event having an actual adverse effect on the security of network and information systems[10]. Hence, not all security incidents fall under the radar of the NIS Directive but mostly incidents that affect the availability, integrity, authenticity or confidentiality of networks and information systems used for the provision of essential services fall under the scope of the Directive.

As mentioned previously, the proposal for the NIS 2 Directive aims at expanding the scope of the NIS Directive and to make it more future proof to keep up with the unprecedented digitalisation that has taken place in the last few years. Moreover, additional security requirements have added under the new Directive with a list of focused measures such as incident response and crisis management, cybersecurity testing, use of encryption and vulnerability handling and disclosure. As per the proposal for the NIS 2 Directive, enhancing the overall level of cybersecurity could also result in prevention of environmental risks/damage in case of an attack on an essential service especially for the energy, water supply and distribution or transport sectors. [11]

The proposal for the NIS 2 Directive will now be subject to negotiations between the Council of the EU and the European Parliament. Once agreed upon and subsequently adopted, Member States will be given 18 months to transpose the Directive into their national laws.

2.2.1.3 Relevance of the NIS Directive for TwinERGY

Given that TwinERGY covers activities with regards to electricity supply, which are considered 'essential services' under the existing NIS Directive, it may be relevant to take cognizance of this Directive and its provisions. However, at the present stage where the project is working with the different pilots, it can be argued that it is unlikely to identified as an operator of essential services since it does not 'provides a service which is essential for the maintenance of critical societal and/or economic activities' If the proposed solution of TwinERGY enters into the market, then the NIS Directive might be applicable.

The UK has already implemented measures under the NIS-directive, which apply to operators of essential services, including DSRs, and Relevant Digital Service Providers (RDSPs). A RDSP has 50 or more staff, or a turnover of minimum 100 million Euro per year, has its main establishment or a representative in the UK and offers services in the EU. It is worth analysing whether the TwinERGY consortium and/or participating organisations that also operate in the EU as part of the TwinERGY activities can be qualified as RDSP. If this is the case, they must register with the Information Commissioner's Office (ICO) and ensure the appropriate and proportionality security measures to manage the risks in this sector, as

[9] 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) OJ L 194, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
[10] NIS Directive, art 4(7)
[11] Proposal for NIS 2 Directive.

well as notifying the ICO in the occurrence of incidents that have substantial impact on their service delivery.[12]

2.3 Human-Centric Perspective

2.3.1 Personal data protection

2.3.1.1 Scope, objectives and key definitions

The General Data Protection Regulation (GDPR) governs processing of personal data at EU level and is horizontally applicable across all EU Member States.[13] The GDPR, which came into force in May 2018, applies to processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[14]

The concept of 'personal data' is defined under Article 4(1) of the GDPR as *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.* Given that the definition includes 'any information', one can assume that the term 'personal data' should be interpreted in a rather broad manner.

The GDPR identifies several roles which imply a certain level of legal responsibilities for each role. A 'controller' means *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*.[15] There can also be instances two or more controllers that jointly determine the purposes and means of processing in which case they will be joint controllers.[16] On the other hand, a 'processor' is *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*.[17]

[12] UK Government (31 December 2020). NIS Regulations: UK digital service providers operating in the EU [Guidance]. Retrieved from: https://www.gov.uk/guidance/nis-regulations-uk-digital-service-providers-operating-in-the-eu.
[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(General Data Protection Regulation) OJ L 119, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[14] General Data Protection Regulation, art 2.
[15] General Data Protection Regulation, art 4(7).
[16] General Data Protection Regulation, art 26.
[17] General Data Protection Regulation, art 4(8).

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

2.3.1.2 Legal requirements under the GDPR

The GDPR stipulates that for processing to be lawful, there needs to be a lawful basis, i.e. processing can be done based on consent of data subject, for performance of a contract, legitimate interest, to protect vital interest of data subject or another person or in public interest. Article 5 of the GDPR also lay down six key principles that form a critical part of the data protection regime, namely:

a) Lawfulness, fairness and transparency;
b) Purpose limitation;
c) Data minimisation;
d) Accuracy;
e) Storage limitation; and
f) Integrity & Confidentiality.

The GDPR also provides certain rights to individuals whose personal data is being processed by organisations including the right of access to their personal data, the right to be forgotten, right to rectification and the right to object to processing of personal data for certain purposes. To ensure that processing personal data is done in a secure manner, organisations are required to implement appropriate technical and organisational measures. While no specific measures are mandated for organisations to implement, the GDPR provides organisations the flexibility to implement safeguards keeping in mind the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.[18] Pseudonymisation and encryption of personal data are provided as suggestions of ensuring security of processing under the GDPR.

The GDPR also introduces the principle of data protection by design and by default wherein organisations are required to ensure that privacy protections are to be embedded in the design of business operations, processes and services. Another measure worth mentioning is the need, in certain circumstances, of data protection impact assessments which need to be conducted in the event the processing is likely to result in a high risk to an individual's rights.[19] It may also require pre-consultation with the relevant supervisory authority.

2.3.1.3 Relevance of the GDPR for TwinERGY

The GDPR forms the currently applicable regulation that is governing processing of personal data at EU level, that is horizontally applicable across all EU Member States and hence relevant for TwinERGY. Given that data on energy generation, usage and consumption of households will be collected, exchanged, stored, or analysed pursuant to TwinERGY project, the GDPR will be of considerable importance within this project since that data can be traced back to specific individuals.

[18] General Data Protection Regulation, art 32.
[19] General Data Protection Regulation, art 35.

The lawful basis at present for the four TwinERGY pilots is based on consent wherein each pilot will be considered to be a controller for the processing done under their respective pilot. In the event the TwinERGY solution is placed in the market at a later stage, legal ground for processing data most likely will be based on performance of contract. It is also relevant to mention that each pilot has designated a Data Protection Officer (DPO) for their respective pilots. In terms of data transfers, at present all data under TwinERGY is being processed within the EU apart from the processing that will be undertaken pursuant in the context of piloting activities to be conducted in the UK. However, since the EU has adopted an adequacy decision on 28 June 2021, no additional steps are required to undertaken at a project level to enable seamless processing. [20]

The Data Protection Act (2018) has implemented the requirements under the GDPR in national law, which became applicable 1 January 2021. The Data Protection, Privacy and Electronic Communications (DPPEC) has amended this Data Protection Act, into the so-called 'UK GDPR'. Post-Brexit, organisations in the UK are obliged to comply with the specific scope and wording of this UK GDPR. However, UK organisations that process data of EU residents, must comply with the EU GDPR as well. [21]

2.3.2 ePrivacy Directive and forthcoming Regulation

2.3.2.1 Scope, objectives and key definitions

The ePrivacy Directive has been applicable since 2002 with the primary purpose to protect privacy of EU citizens as well as the confidentiality of tracking and monitoring practices. The Directive applies to the processing of personal data in the electronic communications sector, such as the internet or mobile phone networks, and is thus sector-specific.[22] Given that it is a Directive, the requirements for privacy protection have been implemented into national laws or regulations.

To ensure alignment of the ePrivacy Directive with the GDPR, the ePrivacy Directive is currently being updated into the ePrivacy Regulation. The draft version of the ePrivacy Regulation was finalised on 10 February 2021 by the EU Council.[23] The ePrivacy Regulation specifies how the rules of the GDPR will be applied to personal data processed through electronic communication services. [24] The Regulation widens the scope of the Directive: it

[20] Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, available at: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf

[21] Information and Communications Office (ICO) (10 July 2020). Information rights at the end of the transition period Frequently Asked Questions. Retrieved from: https://ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexit-faqs-v2_3.pdf.

[22] 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 (ePrivacy Directive), OJ L 201, art 1, available at: https://eur-lex.europa.eu/eli/dir/2002/58/oj.

[23] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (ePrivacy Regulation), COM/2017/010 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

[24] ePrivacy Regulation, Section 1.

covers both content and metadata, including cookies, search engines and direct marketing.[25] As a consequence of the Directive becoming the ePrivacy Regulation, it will not only become self-executing and legally binding in EU countries, but the rules will also be tightened. Most importantly, with the introduction of the ePrivacy Regulation, privacy rules will become automatically applicable to modern communication services[26], including WhatsApp, Facebook and Skype, as well as to new forms of electronic communications such as Internet-of-Things.[27]

2.3.2.2 Legal requirements under the ePrivacy Regulation

The primary implications of the ePrivacy Regulation are the introduction of rules for management of metadata and stricter rules for cookies provision and marketing calls. [28] Fines will be up to 2% of the company that breaches the Regulation.[29] Yet not only will the Regulation cause restrictions, it will also streamline processes such as cookie provision and the collection of meta-data. After implementation, no consent is needed for non-privacy intrusive cookies. Another consequence of the ePrivacy Regulation is that the principle of confidentiality will also apply to machine-to-machine communication.[30] The next section discusses what this could imply for the TwinERGY project.

2.3.2.3 Relevance of the ePrivacy Regulation for TwinERGY

The ePrivacy Directive will have no direct impact on the TwinERGY project, as it will not introduce any new obligations. However, given that the proposed ePrivacy Regulation will apply to machine-to-machine communication, and its applicability is not limited to personal data, it is likely become relevant for the communication between smart meters, energy generation, peer-to-peer sharing or storage infrastructure and electronic home devices. The Regulation may introduce obligations to adopt specific safeguards with regards to the processing of data generated by smart energy grids, specifically driven by smart metering devices. More research is required to specify the implications for data exchange in the TwinERGY project of the forthcoming ePrivacy Directive.

The UK has already implemented the provisions under the ePrivacy Directive, into the Privacy and Electronic Communications Regulations (PECR). This national regulatory framework provides rules on marketing communication, cookies, security of communications services, and customer privacy. The scope is somewhat broader than that of the ePrivacy Directive, as it includes cookies and online marketing, issues that were only discussed under the proposed ePrivacy Regulation on an EU level.[31] Given that the proposed ePrivacy regulation has not yet been agreed on, hence is not applicable, its provisions have as of now no impact on the UK.

[25] ePrivacy Regulation, Art. 1,2 & 4.
[26] ePrivacy Regulation, Articles 1,2 & 4.
[27] ePrivacy Regulation, preface under (12).
[28] ePrivacy Regulation, Articles 4, 6, 7 & 11.
[29] ePrivacy Regulation, Article 23.
[30] ePrivacy Regulation, preface under (12).
[31] The Privacy and Electronic Communications (EC Directive) Regulations 2003. Retrieved from: https://www.legislation.gov.uk/uksi/2003/2426/contents/made.

2.3.3 Consumer protection

While there are various legislations that safeguard the interest of consumers such as the Consumer Rights Directive[32], Directive on Unfair Terms in Consumer Contracts[33] and the Product Liability Directive[34], this section focuses on the sector specific legislation pertinent to the energy sector i.e., the Directive on common rules for the internal market for electricity[35].

2.3.3.1 Scope, objectives and key definitions

In its Communication titled 'A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy' in February 2015, the European Commission set out its vision for an Energy Union with citizens as an integral part in terms of taking ownership of the energy transition while at the same time benefiting from new technologies to reduce their bills and participating actively in the market. Subsequently, another Communication by the European Commission entitled 'Delivering a New Deal for Energy Consumers' that put forth the vision for a retail market that better serves energy consumers.

That said, the Directive on common rules for the internal market for electricity sets out common rules for the generation, transmission, distribution, energy storage and supply of electricity, together with consumer protection provisions, with a view to creating truly integrated competitive, consumer-centred, flexible, fair and transparent electricity markets in the Union.[36] With the objective of providing affordable, transparent energy prices and costs for consumer, the Directive sets out key rules in relation to the organisation and functioning of the Union electricity sector with a specific focus on consumer empowerment and protection.

Under the Directive, the term consumer deals with 'wholesale consumer' which is *a natural or legal person who purchases electricity for the purpose of resale inside or outside the system where that person is established* and a 'final customer' which is defined as *a customer who purchases electricity for own use.*

2.3.3.2 Legal requirements under the Directive on common rules for the internal market for electricity

Under the Directive, Member States shall ensure that all customers are free to purchase electricity from the supplier of their choice and that all customers have the option to have

[32] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council OJ L 326, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0083.
[33] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts OJ L 95/29, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31993L0013.
[34] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products OJ L 141, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A31985L0374.
[35] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU OJ L 158/125, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0944
[36] Directive on common rules for the internal market for electricity, art 1.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

more than one electricity supply contract at the same time as long as the required connection and metering points are established.[37] The Directive requires Member States to ensure that final customers have the right to a contract with a supplier of their regardless of the Member State in which the supplier is registered. Moreover, the contract should clearly specify besides certain other details, the identity and address of the supplier, the services provided, the service quality levels offered, the types of maintenance service offered and the means by which up-to-date information on all applicable tariffs, maintenance charges may be obtained. Overall, Suppliers are required to ensure that they provide final customers with fair and transparent general terms and conditions in plain and unambiguous language and suppliers must include non-contractual barriers to the exercise of customers' rights, such as excessive contractual documentation.[38]

Interestingly, the Directive also introduces a provision for an 'active customer' who is defined as a *final customer, or a group of jointly acting final customers, who consumes or stores electricity generated within its premises located within confined boundaries or, where permitted by a Member State, within other premises, or who sells self-generated electricity or participates in flexibility or energy efficiency schemes, provided that those activities do not constitute its primary commercial or professional activity.* For this purpose, Member States are required to ensure that active members are entitled undertake certain activities such as to operate either directly or through aggregation, to sell self-generated electricity, including through power purchase agreements, to participate in flexibility schemes and energy efficiency schemes and under certain circumstances be financially responsible for the imbalances they cause in the electricity system.[39]

2.3.3.3 Relevance of the Directive on common rules for the internal market for electricity for TwinERGY

Given that the Directive was amended rather recently in 2019, it acknowledges the benefits of new technologies such as smart meters in empowering citizens as it allows customers to receive accurate and near real-time feedback on their energy consumption or generation, and to manage their consumption better, to participate in and reap benefits from demand response programmes and other services, and to lower their electricity bills.[40]

The Directive contains provision regarding smart metering systems that may be of relevance for TwinERGY. To promote energy efficiency, the Directive requires Member States and where relevant the regulatory authority to strongly urge electricity undertakings and other participants to optimise the use of electricity by providing energy management services, developing innovative pricing formulas, and introducing smart metering systems that are interoperable, in particular with consumer energy management systems and with smart grids. [41] Moreover, Member States that do deploy smart metering systems are required to ensure that final customers also contribute to the related costs of deployment in a

[37] Directive on common rules for the internal market for electricity, art 4.
[38] Directive on common rules for the internal market for electricity, art 10(8).
[39] Directive on common rules for the internal market for electricity, art 15(2).
[40] Directive on common rules for the internal market for electricity, recital 52.
[41] Directive on common rules for the internal market for electricity, art 19.

transparent and non-discriminatory manner, while accounting for the long-term benefits to the whole value chain.[42]

The relations between the UK and the EU on energy are currently governed by the EU-UK Trade Cooperation Agreement and the Euratom-UK Agreement. The EU-UK cooperation on energy will continue to exist.[43] This means that the UK leaving the EU will not hinder the provision of gas and electricity from and to the UK. However, other than this, and given the local nature of the TwinERGY activities, provisions regarding the integration of the UK grid with the European grid will not be highly relevant on the short term.

2.3.4 Other relevant legislations

In addition to the legislations mentioned above, there are certain other regulations that need be taken into account for the purpose of TwinERGY.

2.3.4.1. Regulation on electronic identification and trust services for electronic transactions

The implementation of the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) was a significant milestone towards building trust in the online environment. The Regulation provides for a harmonized framework that allows people and businesses of a Member State to use their national electronic identification schemes (eIDs) in order to gain access to public services of other Member States where eIDs is available. Moreover, the Regulation provided for an internal market for electronic Trust Services (eTS) namely electronic signatures, website authentication, electronic seals, time stamps etc., thereby giving them the same legal status to processes that may be paper-based. The relevance of the eIDAS was further underscored during the COVID-19 pandemic which witnessed more and more governments and organisations move their services and operations online.

Electronic identification offers several benefits to organisations by allowing them to authenticate the identity of customers and other businesses so as to establish contractual relationships in an agile yet secure and seamless manner. By providing secure authentication methods in different EU member states, the eIDAS enables organisations to expand their clientele. Moreover, a qualified electronic signature has the same legal effect as a handwritten signature pursuant to the eIDAS Regulation. In July 2020, the European Commission launched a public consultation to determine the drivers and barriers to the adoption of electronic identification and trust services for electronic transactions in the EU. The Inception Impact Assessment (IIA) report of eIDAS highlighted various problem areas that needed to be tackled including the fact that when the IIA report was published only 15 of 27 Member States offer cross-border electronic ID under eIDAS to their citizens.

[42] Directive on common rules for the internal market for electricity, art 19.
[43] European Commission (no date) Electricity Market Design. Retrieved from: https://ec.europa.eu/energy/topics/markets-and-consumers/market-legislation/electricity-market-design_en.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

In addition to the eIDAS Regulation, the recent proposal of the European Commission regarding a framework for a European Digital Identity is of relevance to TwinERGY given its focus on digital twins. If adopted, the new proposal will enable any EU citizen to easily access services using their European Digital Identity without having to use private identification methods or unnecessarily sharing personal data. By making it easier for businesses to verify the identity of citizens, the proposal for the European Digital Identity is expected to boost competitiveness in the EU and to allow organisations to benefit from a harmonised European approach to trust, security and interoperability.

The eIDAS Regulation is a EU Regulation and will not apply in Post-Brexit UK. However, the eIDAS has been adopted into the UK law[44][45]. Nevertheless, the UK Information Commissioner's Office (ICO) advises UK trust service providers to assume they have to comply with the eIDAS.[46]

2.3.4.2 Revised Payment Services Directive

Prior to the enactment of the Revised Payment Services Directive (PSD II)[47], EU lawmakers acknowledged that solutions developed by third party organisations fell outside the scope of applicable regulatory framework for the payments market which resulted in the environment of card payments and new means of payments (such as internet and mobile payments) becoming fragmented, inconsistent and under-regulated[48] The enactment of the revised Payment Services Directive helped address these challenges and to also transform traditional methods of banking to more innovative ones.

The PSD II opened up the EU payments market to organisations that were providing payment services by allowing them to gain access to information about payment accounts provided that the organisation has been granted authorisation as a payment institution under the Directive. The PSD II imposed measures to manage operation and security risks. Payment service providers were also required to establish and maintain effective incident management procedures such as detection and classification of major operational and security incidents.[49] In September 2019, Strong Customer Authentication (SCA) was introduced in EU as a part of the PSD2 to reduce instances relating to fraud and to make online payments more secure. SCA ensured that proper identification or authentication was

[44] The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019). Retrieved from: https://www.legislation.gov.uk/uksi/2019/89/contents/made.
[45] The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 (2016 No.696)). Retrieved from: https://www.legislation.gov.uk/uksi/2016/696/pdfs/uksi_20160696_en.pdf.
[46] Information and Communications Office (ICO) (10 July 2020). Information rights at the end of the transition period Frequently Asked Questions. Retrieved from: https://ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexit-faqs-v2_3.pdf.
[47] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366.
[48] Commission Staff Working Document, Impact Assessment accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market and amending Directive 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions",
[49] Revised Payment Services Directive, art 95.

undertaken for all payments exceeding €30 and is to take place via an authentication process based on two specific factors supplied by the user, e.g. a password, PIN code, a mobile phone or a fingerprint.

At present the eIDAS is not of direct relevance for the TwinERGY output, however, depending on future uptake of the solution in the long run, the eIDAS might become applicable at a later stage. On a separate note, with the UK leaving the EU, the UK will also leave the single payments market and will therefore not be subject to the provisions under the PSD II. This means that payments across the European Economic Area, and across the UK, are no longer treated as domestic payments.

2.4 System-Centric Perspective

2.4.1 The Cybersecurity Act

2.4.1.1 Scope, objectives, and key definitions

Given the pervasive use of network and information systems by citizens, organisations and businesses across the EU and the increasing cybersecurity risks, a growing need was felt for a regulation that would bolster cybersecurity at an EU and Member State level. With that objective, the Cybersecurity Act (CSA) was implemented in order to establish a cybersecurity certification framework for products, services and processes across the EU in a holistic manner.[50]

The CSA also strengthens the mandate of the European Union Agency for Cybersecurity (ENISA) and is responsible for carrying out all tasks assigned to it pursuant to the CSA in order to achieve a high common level of cybersecurity across the EU. Under the CSA, the ENISA is the centre of expertise on cybersecurity and is required to assist Union institutions, bodies, agencies as well as Member States in creating and implementing Union policies relating to cybersecurity. In the context of capacity building, ENISA is required to assist Member States in their efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents by providing them with knowledge and expertise.[51]

2.4.1.2 Legal requirements under the Cybersecurity Act

Besides giving the ENISA more teeth, the Cybersecurity Act deals with the establishment of a European cybersecurity certification framework to enhance the conditions for the functioning of the internal market by bolstering the level of cybersecurity within the EU. In addition, the European cybersecurity certification framework shall provide for a mechanism to create European cybersecurity certification schemes and to also attest that the ICT products, services and processes that have been assessed in line with such schemes

[50] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151, available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[51] Cybersecurity Act, art 6.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

maintain the security requirements to protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by those products, services and processes throughout their life cycle.[52]

Pursuant to the CSA, the European Commission is required to publish a Union-wide rolling work programme that will include a list of ICT products, services and processes or categories thereof that could potentially benefit from being included within the scope of a European cybersecurity certification scheme. Article 51 of the CSA requires European cybersecurity certification scheme to be designed to achieve certain objectives including: (a) to safeguard stored or otherwise processed (e.g. collected, analysed, exchanged) data against accidental or unauthorised storage, processing, access or disclosure during the life cycle of the ICT product, service or process (b) to ensure that authorised persons and machines can only access information to which their access rights refer, (c) to identify and document any vulnerabilities (d) to ensure that the ICT products, services and processes are secure by design and by default.

Interestingly, the CSA also introduces assurance levels wherein European cybersecurity certification scheme may specify one or more assurance levels for ICT products, services and processes - basic, substantial or high. These levels are to be commensurate with the level of the risk associated with the intended use of the said for ICT products, services or processes. A European cybersecurity certificate or EU statement of conformity for the assurance level 'basic' that is given for ICT products, services or processes would mean that the said products, services or processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks.[53] Similarly, A European cybersecurity certificate that refers to assurance level 'substantial' would mean that the ICT products, services or processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources.[54] Lastly, a European cybersecurity certificate that refers to assurance level 'high' would translate to the ICT products, services or processes meeting the corresponding security requirements, including security functionalities, and having been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources.[55]

2.4.1.3 Relevance of the Cybersecurity Act for TwinERGY

At present, the CSA states that the certification under the Regulation is voluntary unless European or national law provides otherwise.[56] Moreover, the CSA enables manufacturers of ICT products, services or processes to an EU statement of conformity wherein the fulfilment of the requirements set out under the scheme has been demonstrated. By doing so, the manufacturer of the said products, services or processes assumes responsibility for

[52] Cybersecurity Act, art 46.
[53] Cybersecurity Act, art 52(5).
[54] Cybersecurity Act, art 52(6).
[55] Cybersecurity Act, art 52(7).
[56] Cybersecurity Act, art 56(2).

compliance with the requirements set out int the scheme. The European Commission will also be conducting an assessment by 31 December 2023 to determine the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level of cybersecurity.[57]

That said, while certification under the CSA is voluntary at the time of drafting this deliverable, it might be beneficial to obtain certification under the CSA in the event that the TwinERGY solution enters the market. This is also because the certification will be recognized by all EU Member States and may also give consumers the assurance that the solution meets certain security standards. It is pertinent to note that voluntary nature of certification under the CSA will need to be rechecked in the event the TwinERGY solution enters the market since the Commission might at a later stage assess and identify products, services and processes covered under an existing certification scheme which should be covered by a mandatory scheme.

Taking into account that the Cybersecurity Act mainly focuses on the functioning of the EU Single Market aiming to achieve a high level of cybersecurity within the Union and that it became applicable across all EU Member States on the 28th of June 2021, meaning, after the withdrawal agreement of UK from the EU came into force on 31 January 2020, the discussion below is not of direct relevance for the UK pilot, at first glance. However, Article 42 of the Cybersecurity Act does provide for the cooperation with third countries and international organizations, provided that certain requirements are met. Bearing that in mind, as well as the nature and the intrinsic dependencies within the domain of cybersecurity domain itself, the discussion below may become directly relevant for the UK pilot as well, for instance, in the context of the earlier stated cooperation mechanism.

2.4.2 Artificial Intelligence Act

2.4.2.1 Scope, objectives, and key definitions

On April 21st, 2021, the European Commission published the proposal for a Regulation laying down harmonised rules on artificial intelligence ('Artificial Intelligence Act').[58] It is intended that the proposed Regulation forms the first legal framework in the EU regulating the use of AI following a proportionate, risk-based approach.[59] Overall, the Artificial Intelligence Act aims at strengthening the uptake of AI in Europe, by building trust in AI systems addressing 'human and societal risks associated with specific uses of AI'.[60]

Under the Regulation, Artificial Intelligence is defined as:

[57] Cybersecurity Act, art 56(3).
[58] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
[59] Proposal for the Artificial Intelligence Act, Explanatory Memorandum, under 1.1.
[60] Speech by Executive Vice-President Vestager at the press conference on fostering a European approach to Artificial Intelligence, Brussels, 21 April 2021 [transcript], available at: https://ec.europa.eu/commission/presscorner/detail/en/speech_21_1866.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
(c) Statistical approaches, Bayesian estimation, search and optimization methods.[61]

The Artificial Intelligence Act does not regulate AI technology per se, but, instead, it provides for what AI is used for and how it is used. As mentioned earlier, the Artificial Intelligence Act is a risk-based regulation; the higher the risk that the use of AI may involve, the stricter it is regulated. To this end, the uses of AI systems are classified in four categories: low or minimal risk, limited risk, high risk, and unacceptable risk uses (Figure 3).[62] The qualifications of each risk level as well as the obligations that follow from this classification will be discussed in the next section.

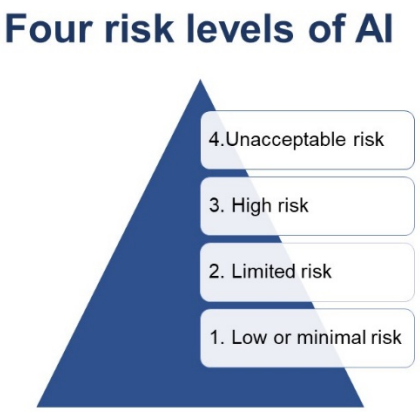

Figure 6: The four risk levels of AI as indicated by the proposed Artificial Intelligence Act.

2.4.2.2. Legal requirements under the Artificial Intelligence Act

Low or minimal risk uses

It is expected that the majority of AI systems such as, for instance, email spam filters or AI in video games, entails minimal to no risk.[63] According to Article 1 of the proposed Artificial Intelligence Act, low or minimal risk uses are outside of its scope.[64] The Regulation therefore allows the use of such applications, without any restrictions. Nevertheless, the use of such applications will, certainly, remain to be regulated on the basis of other already applicable regulations.

[61] Proposal for the Artificial Intelligence Act, Annex I.
[62] Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, Brussels, 21 April 2021 [press release], available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.
[63] Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, Brussels, 21 April 2021 [press release], available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.
[64] Proposal for the Artificial Intelligence Act, art. 1.

Limited risk uses

The second category consists of AI uses that are intended to interact with people, such as chatbots or self-checkout services in shops.[65] Furthermore, other applications that are considered 'limited risk' include emotion recognition systems, biometric categorisation systems and AI used for media content manipulation, such as image, audio or video.[66] Based on the rationale that users should be aware that they are interacting with a machine, these limited risk uses are subject to transparency obligations.[67]

High-risk uses

As Vestager points out, high-risk uses, that is, uses that 'interfere with important aspects of our lives', are the main focus of the Artificial Intelligence Act.[68] The European Commission has drafted a list of such uses in Annex III of the proposal, which serves as a reference for indicating high-risk. Prioritisation in access to jobs, education or eligibility for public assistance benefits and services form examples of such high-risk AI systems. Other examples include systems deciding on the creditworthiness of individuals, emotion detection or assistance of judges in court.[69] There are two necessary conditions for classifying other AI systems as high-risk. Firstly, it the system should be used in any of the areas listed in Annex III. Secondly, the system constitutes 'a risk of harm the health or safety' of humans, or 'a risk of adverse impact on fundamental rights'. The 'severity and probability of occurrence' of the risk should be equal to or higher than that of the systems already listed in Annex III.[70]

According to the proposed Regulation, providers of certain high-risk AI systems are obliged to:

1. provide their system with *high-quality data*, that does not contain biases and inaccuracies, and are adapted to the setting where the system is intended to be used, so that the system will not be biased or discriminating.[71]
2. *maintain detailed technical documentation* to demonstrate and assess compliance with applicable requirements set under the Artificial Intelligence Act.[72]
3. ensure that the functioning of the AI system remains traceable throughout its lifecycle (*record-keeping*), so that it can be explained.[73]
4. share substantial information with users to help them understand the output and how to properly use AI systems (*transparency*).[74]

[65] Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, Brussels, 21 April 2021 [press release], available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.
[66] Proposal for the Artificial Intelligence Act, art. 1.
[67] Proposal for the Artificial Intelligence Act, art. 52.
[68] Speech by Executive Vice-President Vestager at the press conference on fostering a European approach to Artificial Intelligence, Brussels, 21 April 2021 [transcript], available at: https://ec.europa.eu/commission/presscorner/detail/en/speech_21_1866.
[69] Proposal for the Artificial Intelligence Act, Annex III.
[70] Proposal for the Artificial Intelligence Act, art. 7.
[71] Proposal for the Artificial Intelligence Act, art. 10.
[72] Proposal for the Artificial Intelligence Act, art. 11.
[73] Proposal for the Artificial Intelligence Act, art. 12.
[74] Proposal for the Artificial Intelligence Act, art. 13.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

5. ensure a proper level of *human oversight*, both in the design as well as in the implementation stage of AI. [75]
6. respect the highest standards of *accuracy, robustness, and cybersecurity*.[76]

Unacceptable risk

The last category covers the uses of AI systems that are strictly prohibited, based on the type of AI technology and the intended use. There are four sub-categories of such uses (Figure 4). Firstly, the prohibition applies to AI systems that use subliminal techniques that can cause physical or psychological harm to someone. Secondly, AI systems that manipulate behaviour of vulnerable people on the basis of age or physical or mental disability, to make them cause harm, are strictly prohibited; for example, the use of AI in a toy that involves voice assistance to manipulate a child into doing something dangerous is prohibited. Thirdly, the proposed Regulation provides for a ban on AI systems that are used by public authorities to examine the trustworthiness of people for the benefit of a social scoring system. Finally, according to the proposal, the use of biometric identification systems in publicly accessible spaces for law enforcement purposes will be, in principle, prohibited. There are certain exceptions provided in this respect, such as a search of a missing child or threat of terrorist attacks.[77]

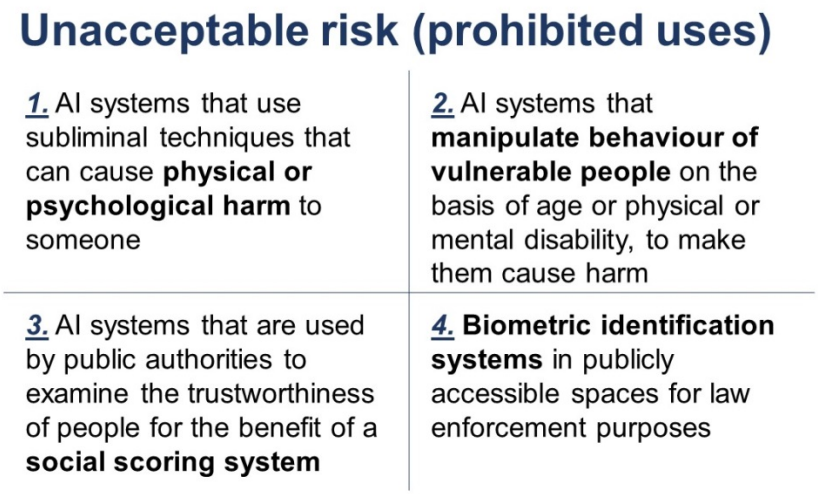

Figure 7: Prohibited uses of AI, according to Article 5 of the proposed Artificial Intelligence Act.

2.4.2.3 Relevance of the Artificial Intelligence Act for TwinERGY

The Artificial Intelligence Act is relevant for TwinERGY if any or more of the technologies used in TwinERGY can be defined as Artificial Intelligence Systems, given the definition given before, and can be classified in the limited risk, high-risk or unacceptable risk categories. Two technologies that potentially qualify for Artificial Intelligence Systems are digital twins and demand-response systems.

[75] Proposal for the Artificial Intelligence Act, art. 14.
[76] Proposal for the Artificial Intelligence Act, art. 15.
[77] Proposal for the Artificial Intelligence Act, art. 5.

Digital twins may fall under (b) of the definition, as they are knowledge-based approaches, such as knowledge representation or knowledge bases. The next question is whether the risk level exceeds the low-risk classification. Following from the regulation, digital twins are unlikely to be assigned to the unacceptable risk category nor the high-risk category. However, depending on the context and the interaction of humans with digital twins, they may qualify as limited risk. Therefore, the transparency obligations following from the regulation may apply.

With regards to demand-response systems, depending on the type of systems, they may include (a) machine learning approaches, (b) logic- and knowledge-based approaches or (c) – most likely – statistical approaches, including optimisation techniques. Although these systems are not likely to be strictly prohibited, they may under specific circumstances be qualified as high-risk AI systems, given that they are intended to be used for the management and operation of critical infrastructure. Therefore, it is useful to take into account the obligations for demand-response infrastructure under the AI Act to ensure future alignment.

This is an early analysis, and it should be taken into account that the AI Act is still evolving and its definition of Artificial Intelligence had been criticised for its ambiguity. Therefore, this analysis on the classification of the technologies is not set in stone. It is recommended to assess the risk level of any advanced technologies, other than digital twins or demand-response systems, used in the TwinERGY project in the light of the Artificial Intelligence Act, as it continues to develop over time, to ensure alignment and compliance with the Regulation before it enters into force.

Should it be adopted, the proposed AI Act will be of relevance for organization located outside the EU (in a third country) and, therefore, for organizations involved in the UK piloting activities and/or in its potential future uptake, due to the extraterritorial effect of the proposed Act. In this respect, Article 2 explicitly dictates that the Regulation shall -among other- *apply to providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country, as well as to providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union.*

2.4.3 Other relevant legislations

2.4.3.1 Product Liability Directive

Keeping in mind that defective products can result in physical damage to consumers and their property, the Product Liability Directive was introduced in way back in 1985 to provide a high and equal level of consumer safety and protection.[78] The Directive holds producers liable for any damage that results from the use of their defective products. The Directive defines 'product' as *all movables, with the exception of primary agricultural products and*

[78] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products OJ L 210, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31985L0374.

game, even though incorporated into another movable or into an immovable. Moreover, the PLD requires the person injured by the use of the defective product to prove the damage, the defect and the causal relationship between defect and damage.

Given the fact that the Directive was implemented more than 35 years earlier, a need was felt to assess and address existing gaps in the PLD also keeping in mind the technological developments. For this purpose, the European Commission had launched a public consultation in January 2017 to get feedback from stakeholders on the application and relevance of the PLD. In the subsequent report that was published, the European Commission acknowledged that while the PLD had been able to cover a broad range of products for a considerable period of time, it did not mean the Directive was perfect. Moreover, the report stated that the effectiveness of the PLD was hampered by concepts (such as 'product', 'producer', 'defect', 'damage', or the burden of proof) that could be more effective in practice.[79] That said, the report stated that the Commission would reassess and update certain aspects of the PLD including existing definitions.

Since the applicability of the PLD is dependent on the use of a defective product as defined within the Directive, it is unclear whether the tools or applications developed pursuant to TwinERGY will qualify as a product. However, since the European Commission is in the process of amending the PLD wherein it might broaden the definition of the term product to include software and certain other applications, it is possible that the PLD might become applicable to TwinERGY at a later stage.

2.4.3.2 General Product Safety Directive

Similar to the objectives of the Product Liability Directive discussed above, the General Product Safety Directive (GPSD) aims at ensuring that only products that meet certain safety requirements are placed on the market. [80]The GPSD defines a 'safe product' as any product which, under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account the following points in particular: (i) the characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance;(ii) the effect on other products, where it is reasonably foreseeable that it will be used with other products; (iii) the presentation of the product, the labelling, any warnings and instructions for its use and disposal and any other indication or information regarding the product; (iv) the categories of consumers at risk when using the product, in particular children and the elderly.[81]

[79] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:246:FIN

[80] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety OJ L 11/4, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32001L0095

[81] General Product Safety Directive, art 2(b).

To ensure consumer awareness, the GPSD requires producers to provide consumers with the necessary information to help them be aware of the inherent risks of the products throughout the normal period of use in cases where such risks are not apparent and to also enable consumers to take precautions against the risks. [82] Similarly, distributors are required to act with due care to ensure with the applicable safety requirements, in particular by not supplying products which they know or should have presumed do not comply with those requirements.[83]

Unlike the definition of product under the PLD, the GPSD takes a rather broader approach and is applicable to products as well as services that are intended for consumers or are likely to be used by consumers and which are supplied or made available, whether for consideration or not, in the course of a commercial activity. Keeping that in mind, in the event the TwinERGY solution enters the market, the provisions of the GPSD will need to be taken into consideration.

Note that the discussion below is of direct relevance for the UK pilot as well, given that the General Product Safety Regulations of 2005 implemented the earlier stated general product safety in the national law of UK[84].

2.4.3.3 Radio Equipment Directive

The Directive on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment (RED) provides a framework for placing radio equipment in the EU market.[85] The RED applies to electrical or electronic products, which intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination, or electrical or electronic products which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination.[86] The RED provides a framework to ensure that such products meet certain standards when it comes to certain aspects such as safety, health and electromagnetic compatibility.

Obligations of manufacturers of radio equipment are laid down in the Directive to ensure that the radio equipment is designed to meet certain essential requirements including protection personal data and privacy, facilitating access to emergency services, enabling use by users with disabilities and the like.[87] Similarly, distributors and importers of radio equipment are required to refrain from making radio equipment available on the market which they believe do not conform to the prescribed essential requirements till the time such products are

[82] General Product Safety Directive, art 5(1).
[83] General Product Safety Directive, art 5(2).
[84] See, also, https://www.legislation.gov.uk/uksi/2005/1803/made

[85] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC OJ L 153, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053
[86] Radio Equipment Directive, art 2(1).
[87] Radio Equipment Directive, art 10.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

brought into conformity. [88] To ensure that the radio equipment meets all requirements laid down in the directive before it is placed on the market, manufacturers are required to perform conformity assessment of the radio equipment.[89]

Article 3(3)(e) and (f) of the RED require certain categories of radio equipment to be constructed ensuring that the said equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber and that it supports certain features ensuring protection from fraud respectively. Between 2019 – 2020, an impact assessment study was conducted on behalf of the Commission to analyse the different policy options to strengthen safeguards for internet-connected radio equipment (RE) and wearable RE as regards data protection and privacy and protection from fraud and to verify whether a minimum level of 'baseline' security requirements measures should be integrated into the RED. The study involved assessment of relevant EU legislation, more than 70 interviews with relevant stakeholders and two online surveys and subsequently provided recommendations which might be useful for TwinERGY to consider at a later stage in the event the TwinERGY tool is place on the market.

Same as it was the case for other regulations discussed in the present document, the Radio Equipment Directive is relevant for the UK pilot as well. More specifically, the Radio Equipment Regulations of 2017 transposed in the UK legal order the Radio Equipment Directive, which, thus, constitutes currently integral part of the UK law[90].

2.5 Data-Centric Perspective

2.5.1 The Free Flow of Non-Personal Data Regulation

2.5.1.1 Scope, objectives and key definitions

One of the risks of data protection frameworks is that of 'vendor lock-in': the situation where a user is stuck with a digital service provider because it is unable to avoid moving its data from one provider to another. Where in 2018, the GDPR has provided for measures to avoid this from happening with regards to personal data, the Regulation on the Free Flow of Non-Personal Data promotes portability of data.[91]

The framework for the Free Flow of Non-Personal Data in the EU is applicable since 28 May 2019 and aims at fostering the data economy by facilitating the exchange and storage of electronic, non-personal data across EU borders by removing certain obstacles to the free

[88] Radio Equipment Directive, art 12 & 13.
[89] Radio Equipment Directive, art 17.
[90] See, also, https://www.legislation.gov.uk/uksi/2017/1206/note/made

[91] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

movement. The overarching purpose it to facilitate businesses to share data and thereby potentially improve and extent their business services.[92]

The Regulation applies to processing of electronic data, other than personal data, within the EU zone, thereby complementing the GDPR. In addition to data being in the EU, the Regulation is also applicable when the users of the service are located in the EU, or when the services are carried out by an entity in the EU. [93]

2.5.1.2 Legal requirements under the Free Flow of Non-Personal Data Regulation

With the introduction of this Regulation, data localisation requirements are prohibited, provided that they serve public security objectives.[94] Another key implication of the Regulation is that competent public authorities will be able to retain access to the data in the case when it is stored and processed in another Member State or in the cloud. [95] Furthermore, the Regulation facilitates businesses to switch of cloud service providers without losing their data. Under the framework, the Commission stimulates providers to write codes of conducts that allow users to transfer data between cloud providers or local IT environments.[96] Finally, the Regulation ensures that security requirements following from the cybersecurity package that apply to processing of data by businesses within the EU, will apply likewise to processing data across EU borders or in the cloud. [97]

2.5.1.3 Relevance of the Free Flow of Non-Personal Data Regulation for TwinERGY

The Regulation on the Free Flow of Non-Personal Data applies – as the name reveals – to non-personal data, that is, any data not relating to an identified or identifiable person. Firstly, given the transnational nature of the TwinERGY project, the free flow of non-personal data across EU borders will be relevant, hence will be beneficial for TwinERGY. Furthermore, by means of smart meters, plenty of non-personal data will be processed, including energy usage, energy generation, time, anonymised user data and possibly other raw data shared by machines. In this respect, the Regulation will be relevant for the TwinERGY project. Finally, the substance on data portability and the opportunity to switch cloud service providers without losing the data, which also applies to the use of a device[98], can be relevant in the context of TwinERGY, and in particular to the 'raw' data generated by a smart meter. It is recommended to take this Regulation at hand whilst designing and deploying the piloting activities. In a later project stage, when the data flows are more clearly mapped, an analysis for the specific application of this Framework will be provided.

[92] European Commission (8 July 2019). Regulation on the free flow of non-personal data [publication]. Retrieved from: https://knowledge4policy.ec.europa.eu/publication/regulation-free-flow-non-personal-data_en.
[93] Framework for the free flow of non-personal data in the European Union, art. 2.
[94] Framework for the free flow of non-personal data in the European Union, art. 4.
[95] Framework for the free flow of non-personal data in the European Union, art. 2.
[96] Framework for the free flow of non-personal data in the European Union, art. 6(2).
[97] European Commission (8 July 2019). Regulation on the free flow of non-personal data [publication]. Retrieved from: https://knowledge4policy.ec.europa.eu/publication/regulation-free-flow-non-personal-data_en.
[98] Guidelines on the right to data portability of 13 December 2016, available at: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

The discussion below could be relevant for the UK pilot as well; in particular, according to Article 2, Free Flow of Non-Personal Data regulation *applies to the processing of electronic data other than personal data in the Union*, which -among other- *is provided as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established or not in the Union.* So, in the future, depending on the exact form of the uptake of the TwinERGY output in the future, an organization established in a third country such as UK, offering services to users in EU would be bound by the obligations set under this specific legislative act.

2.5.2 The Data Governance Act

2.5.2.1 Scope, Objectives and Key Definitions

For 2019 – 2024, one of the main priorities for the European Commission is to make Europe fit for the digital age given the unprecedented rate at which digital technology is shaping people's lives. In this context, the European Commission also set out its vision and avenues to facilitate Europe's digital transformation by 2030 which focuses on four main themes namely skills, secure and sustainable digital infrastructures, digital transformation of business and digitalisation of public services. Moreover, in order to reduce dependencies on other countries for goods, products and services, the European Commission has already prioritised the need to accelerate digital and data sovereignty.

The European Commission published a Communication on 'A European Strategy for Data' in the beginning of 2020 wherein it highlighted the significance of data for economic growth, competitiveness, job creation, innovation and the like. The objective of the Strategy is to create a single market for data to ensure Europe's competitiveness and digital sovereignty globally. The first deliverable under this Strategy for Data, which was published in November 2020, was the proposal for new rules on data governance (DGA).[99]

The DGA aims at enabling data sharing between organisations to address the issue of low availability of data for research and innovative uses resulting from transaction costs that hinder data exchanges.[100] It also intends to look into the issue of insufficient resourcing in public sector organisations in relation to ascertaining requests for use of data that is in principle not accessible and the use of which is subject to the respect of rights of others.[101] Taking into account the fact that large amounts of data is being generated by public bodies, businesses, organisations and citizens on an everyday basis, the DGA aims at harnessing this data in an effective and structured manner. The Regulation aims at facilitating seamless data sharing across the EU and between sectors to generate wealth for society and to make public sector data available for re-use in certain circumstances. Given the lack of trust between stakeholders, the DGA also proposes measures to increase trust in data sharing.

[99] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767
[100] Inception Impact Assessment, Legislative framework for the governance of common European data spaces, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=PI_COM:Ares(2020)3480073&from=EN.
[101] Inception Impact Assessment, Legislative framework for the governance of common European data spaces, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=PI_COM:Ares(2020)3480073&from=EN.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

2.5.2.2 Legal requirements under the Data Governance Act

Chapter II of the DGA clarifies that it does not create any obligation on public sector bodies to facilitate the re-use of data nor do they release them from their confidentiality obligations.[102] Moreover, agreements and other practices that grant exclusive rights to certain categories of data held by public sector bodies or which restrict the availability of data re-use by other organisations are expressly prohibited. Public sectors bodies that are competent under national law to allow or refuse access for the re-use of one or more of the categories of their data are required to publicly make available the conditions for allowing such re-use.[103] The DGA clarifies that such conditions must be non-discriminatory, proportionate and objectively justified with regard to categories of data and purposes of re-use and the nature of the data for which re-use is allowed. These conditions shall not be used to restrict competition.[104] In the same context, public sector bodies that allow for such re-use may also charge a fee for allowing the re-use of such data provided that such fee shall not be non-discriminatory, proportionate and objectively justified and shall not restrict competition.[105]

Interestingly, the DGA underscore the key role of providers of data sharing services, which act as data intermediaries, in the data economy. As per the DGA, data intermediaries which offer services that can connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing.[106] Conditions for providing data sharing services are also laid out in the DGA which include putting in place procedures to prevent fraudulent practice in relation to access of data, taking adequate technical, organisational and legal measures to prevent transfer or access to non-personal data that is unlawful and a high level of security for the storage and transmission of non-personal data.[107]

2.5.2.3 Relevance of the Data Governance Act for TwinERGY

At present, the proposal for the DGA will be discussed and negotiated between the European Parliament and the Council of the EU. Once approved, the DGA will enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It will be directly applicable in all member states and will apply 12 months after its entry into force. Given the preliminary stage the DGA is at the time of drafting this deliverable, its relevance to TwinERGY can be assessed definitively once the DGA is approved and adopted. This can be further touched upon in the subsequent deliverable D12.2 which is the 1st Legal and Ethical Compliance Report due in October 2023.The potential impact of the proposed Data Governance Act on the UK pilot and in the uptake of TwinERGY outcomes in the long run is quite unclear at this stage. Although the proposal it is intended to apply only within the EU, it does include rules concerning international transfers

[102] Proposal for Data Governance Act, art 3.
[103] Proposal for Data Governance Act, art 5.
[104] Proposal for Data Governance Act, art 5.
[105] Proposal for Data Governance Act, art 6
[106] Proposal for Data Governance Act, recital 22.
[107] Proposal for Data Governance Act, art 11.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

of non-personal data by a re-user that was granted access to such data by the public sector. Although it is currently provided that even sensitive public sector data may be transferred to third countries where it benefits from a similar level of protection as in the EU, the definition of this particular category as under the proposed earlier stated Act is not sufficiently clear. Note that it currently provided that European Commission will declare if a third country provides such protection, via a delegated act.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

3. TwinERGY Approach for Ethics

This section outlines certain ethical principles, especially, for pilots' leaders to consider, in view of further planning and conducting pilot activities within the respective local communities. These principles are grouped in thematic areas and are of horizontal relevance for all pilots. The list of the thematic areas identified is not meant to be exhaustive, but rather aims to stimulate pilots' approach and planning accordingly.

In terms of Ethics approvals, following the approval of TwinERGY project obtained by the Ethics Committee of the project coordinator, University of Patras, the piloting activities of TwinERGY were not subject to separate approvals by the competent Ethics Committees of the organizations acting as pilot leaders. More specifically, in principle, Ethics Committees are established within organizations that conduct research and that are assigned with a high institutional role within society, such as academic institutions and hospitals. In this context and taking into account the nature of the organizations leading the piloting activities of the project, namely, private sector organizations (MYTILINAIOS, Greek Pilot), municipalities (Municipality of Benettuti, Italian Pilot) and universities (e.g. University of Bristol, UK pilot), the requirement for an Ethics approval could be relevant for the UK pilot and the German pilot, which is officially jointly led by both TH-OWL and the City of Steinheim. However, following separate exchanges with the representatives of the German pilot, it was confirmed that there are no Ethics Committees established neither within TH-OWL nor by the City of Steinheim; it was not requested, therefore, that the respective TwinERGY piloting activities in Germany are approved by dedicated Ethics Committees. Furthermore, following the aforementioned approval of TwinERGY project obtained by the Ethics Committee of the project coordinator, University of Patras, University of Bristol considered that an additional approval by the respective Ethics Committee of another academic institution participating in the project was not necessary to be separately obtained.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

3.1 Pilots' Guide

Ethics Perspective

Based on considerations and recommendations that are discussed in the current chapter of this report

- Which groups of people do you recruit for taking part in the pilot program? Do the requirements for **participation** exclude certain groups of people? → *Please consult the EDI Section*
- Which information do you provide participants during the **recruitment process**? → *Please consult the Transparent Informed Recruitment Section*
- How to build a **sense of ownership and empowerment** among pilot participants? → *Please consult the Democratic and Empowering Participation Section.*
- What is the **core value** of the work in TwinERGY? → *Please consult the Societal Relevance Section*
- What is the **core value** of TwinERGY approach to **data collection and protection**? → *Please consult the Data Governance Section*

3.2 TwinERGY Ethical Principles

The definitions of ethics are very divergent and ambiguous. According to the Merriam-Webster encyclopaedia ethics are defined as (1) the discipline dealing with what is good and bad and with moral duty and obligation; (2a) a set of moral principles: a theory or system of moral values; (2b) the principles of conduct governing an individual or a group; (2c) a guiding philosophy; (2d) a consciousness of moral importance; and (3) a set of moral issues or aspects in light of the above,. this section takes the principles approach, particularly (2b) the principles of conduct. Whilst section 3.2.1 discusses principles primarily embedded in the technology, section 3.2.2 covers principles governing the community, focusing on participation and empowerment.

3.2.1 Making it work

Making it work does not simply mean putting effort into making technology function. Instead, it implies that the technology should be equipped by design with embedded non-functionals. These non-functionals are principles that prepare for potential risk the technology may encounter or cause. Including these non-functionals by design is therefore essential to make the technology work.

Accountability

Accountability is one of the key principles that flows from ethics. In moral interactions, it is essential that someone can be held *responsible* for their own actions. *Accountability* is a slightly stricter form of responsibility. There are three, non-exhaustive, examples of when it can become a pressing issue: in the energy exchange, in the data exchange, and in the interaction with machine interfaces.

Firstly, within the context of the TwinERGY pilots, where community members will consume, generate, store and exchange energy, accountability will be of considerable importance. Participants should in certain cases, for example, be able to hold someone accountable for not being able to deliver the required amount of electricity, if this is not due to their own in actions.

Secondly, in the data exchange market, this issue could become even more complex. Can residents hold the vendor of their smart meter accountable when their data processing activities do not comply with the terms of conditions in the contract? Who can be held accountable when the data on energy generation, consumption or storage, fall in the hands of the insurance company, who will then use insights derived from the data to tailor their insurance package to the energy behaviour of individual households, thereby disadvantaging certain families?

Finally, accountability could become an even more pressing issue when considering that participants are not only interacting with each other, but also with machine interfaces. In a questionnaire distributed by the Commission among more than 200 stakeholders in the consumer IoT sector, of which 70% consists of large multinational organisations, the sector has expressed their concern that voice assistants and smart device operating system providers will have a more direct relationship with the user than they have. They fear that this close relationship between the technology interfaces and the user will could weaken their role as intermediaries between user and technology. [108] As a result, the accountability of these intermediaries for actions caused by IoT devices towards users could be undermined. It is therefore recommended to prioritise keeping a human in the loop to be able to hold someone accountable for their actions or inactions.

In any of these scenarios, or in combined cases, the participants need a leg to stand on, that is, they need to be able to hold someone accountable for the harm, and, if appropriate, get a compensation. Generally speaking, participants and other stakeholders should be able to hold each other accountable for their actions or inactions. This also implies that people and participating organisations need to be aware that they can be held accountable for their actions, as an incentive for them to act more responsibly. Accountability it not only a theoretical moral principle, but it will also cater for becoming or being compliant to relevant standards and other applicable policy and legal frameworks.

[108] European Commission (9 June 2021). Commission Staff Working Document: Preliminary Report – Sector Inquiry into Consumer Internet of Things. Brussels: SWD(2021) 144 final. Retrieved from: https://ec.europa.eu/competition-policy/system/files/2021-06/internet_of_things_preliminary_report.pdf

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Accountability is about owning and co-owning roles and responsibilities, finding solutions, making things happen, and helping out if things may go wrong once in a while. In this respect, accountability is not an afterthought dealt with after something goes wrong.

Other built-in principles

Apart from accountability, there are more values and qualitative attributes that need to be embedded in the system in order to make it work, and to make them resilient to prepare for risks. These attributes, sometimes called 'non-functionals' in computer science jargon, are an integral part of any and every functionality. These principles, such as trust, security, safety, privacy, et cetera – will harness the system to prevent it from failing.

A thorough and holistic risk mapping approach allows for selecting the right principles, and giving each principle appropriate weight in comparison to the others. In the context of TwinERGY, risks could, for example, arise from the exchange of data between connected devices. The constant interactions between devices make the system more vulnerable for potential risk. It is therefore required to build in trust, privacy protection and security mechanisms, among others. Without taking care of the risks and mitigating them with these principles, the technological systems – devices, networks, algorithms – will eventually fail, possibly leading to unintended consequences.

3.2.2 Guiding principle sets

The ethical principles presented emerge from the participatory nature of the project, which implies the involvement of volunteer citizens in many stages of the innovation and development process. Indeed, engaging the public requires attention to how public participation is managed throughout the project, e.g., what is the role of participants and researchers, how this is made explicit and communicated, and what is promised to the public.

The principles are organized into areas of concern, for each of which a general description of the principle, within the context of TwinERGY, is provided (left), followed by some practical recommendations to bear in mind when planning and developing activities (right).

3.2.3 Equity, Diversity, and Inclusion (EDI)

Description	Recommendations
In accordance with the EDI metrics presented in *D2.1 - Best Practice Guidelines for Engaging Citizens in the Pilots and Metrics for Diversity and Inclusion*, TwinERGY is committed to **encourage and enable the participation of all groups in society**, regardless of	• Ensure that information and venues for meetings are accessible to all • Pay attention to the use of gendered language in all written and oral communications

race, ethnicity, religion, culture, disability, and gender. This includes avoiding marginalization or exclusion of underrepresented social groups, seeking actively to **include people whose voices are often ignored.**	• Ensure that the involvement of vulnerable populations in the pilot (e.g., those who suffer from energy poverty) do not add to participants' distress • Take into account and periodically assess the compliance with the EDI metrics when planning and developing pilot activities

3.2.4 Transparent and Informed Recruitment

Description	Recommendations
TwinERGY seeks to promote and establish **empathic, honest, and trustworthy relations with people** who are engaged in the pilot. This needs to start from **the recruitment process that establishes the first contact** with participants. During recruitment, in addition to following the EDI principles, pilot leaders are encouraged to provide complete and clear information about the involvement of participants in the project, in order to **ensure that decision whether to participate is made from an informed position**.	• Participants have the right to opt out of the pilot program at any time and to request the withdrawal of all their data. • Discuss the potential benefits and risks for their participation in the pilot program. However, you must avoid overpromising positive impact, for instance, savings in personal energy consumption. • Provide an overview of the activities that you expect to develop during the course of the pilot. Present a (tentative) timetable of the main pilot events can help participants to better estimate their effort. • If devices are provided to participants, be sure to clearly explain what happens with the devices at the end of the project or in case the participant decides to opt-out of the pilot program (e.g. must the device be returned? What happens if the device breaks?)

3.2.5 Democratic and Empowering Participation

Description	Recommendations
TwinERGY aims to promote and build a sense of empowerment among pilot	• Offer the participants relevant information to make their participation

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

participants, whose voices and opinions are valued and taken into account in the planning, execution, and evaluation of the project. TwinERGY puts **co-creation** at the heart of the process. The aim is to **equalize power relations** and foster the opinions of all groups in order to shape our work from different perspectives. Further, the stance is that everybody's thoughts are important and valuable and that **everyone is an expert** of own life.	genuine. • Communicate clearly using language everyone can understand. • Avoid looking at participants as only research/data subjects. • Avoid presenting project team members as the experts on the subject. It may generate an imbalance in power relations. • Provide feedback on how project outcomes were influenced by the participants' input.

3.2.6 Societal Relevance

Description	Recommendations
TwinERGY aims to **respond to actual societal needs and create positive changes** for communities. The consortium is moved by an honest desire to meet participants' goals and not only project/research's goals.	• Be aware of the local cultural, social, and economic context of pilot participants. • Plan research activities to understand societal and participants' needs and desires in relation to energy management. • Work towards including the goal of positive change in every stage of the project and research.

3.2.7 Citizen-Oriented Data Collection and Governance

Description	Recommendations
TwinERGY adopts a **human-driven approach to data**. A variety of data will be collected to run pilot activities. These range from contact details, information about homes and buildings, energy consumption and behavioural data, and personal opinions, for instance about comfort levels at home. Even though written consent is not required in all the pilot locations according to their	• Simple language has to be used when communicating with participants about what data are collected, how, and why. • Offer participants the opportunity and the means to exercise active governance over their data: e.g., decide which data to grant and under which condition, discuss the fate of the data when the project is finalised, etc. To this end, pilot leaders are

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

ethical formal procedures, the partners commit to ensuring that participants are informed, understand, and agree on the purpose of data collection, in accordance with requirements on valid consent set under D13.1 'H- Requirement No. 1'. The consortium will also work towards **providing pilot participants with better possibilities to participate in the entire data collection process**: from identification of data needs; selecting appropriate collection tools; collection, analysis, and interpretation. This will **ensure the relevance and reliability of the collected data**.	encouraged to participate and follow the activities conducted under *Task 12.4 -Data use licenses*. • Ensure that the data collected are shared appropriately with participants. This 'return' of data should be delivered in a meaningful and comprehensive way in order to support participant's learnings and demonstrate the value of their inputs.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

4. Concluding Remarks

By expanding on the work conducted under WP13 on Ethics Requirements, the present deliverable went beyond the area of personal data protection covered under WP13 by elaborating, for instance, on key legal aspects pertinent to other areas relevant for TwinERGY pilots, such as cybersecurity and consumer protection. To this end, the deliverable took into account not only currently applicable, but also proposed regulations aiming to put forward a future-looking approach that could contribute to the uptake of TwinERGY outcomes in the long run. Similarly, the approach on ethical aspects taken under this deliverable goes beyond the requirement regarding personal data protection by producing -among other- recommendations of broader societal relevance and regarding user empowerment. Note that as this project is still at a relatively early stage, the analysis of the subject matter remained essentially high-level and generic yet providing the opportunity to the pilot leaders and technical partners to familiarise themselves with the regulatory landscape they engage with, and to adopt a more critical attitude towards the ethical aspects of the project and its piloting activities.

The section on the legal requirements presented first a comprehensible list of questions, the 'Pilots' Guide, which aimed at helping the technical partners to navigate through the regulatory and ethical landscape by allowing them -among other- to draft a 'map' of the dataflows, their nature, origins, destinations and level of protection. The Pilot Guide is built upon the legal requirements discussed later under the set of the most relevant regulations systemized into four categories: the human-centric, system-centric, data-centric and market-centric. It can be argued that most obligations arise from the human-centric domain, which introduces rules for the protection of rights and freedoms of individuals whose data are collected, particularly the right to privacy. Whilst the system-centric regulations, currently existing and proposed, bring forth a list of important provisions for the trustworthy, safe and secure use of specific technologies, the data-centric frameworks could provide some guidance for the management and organisation of non-personal data flows. For the reasons explained, the market-centric frameworks may be considered of limited relevance for the project. Taking into account the plethora of both existing and proposed regulations, it became rather apparent that there are hardly any regulatory gaps to be filled at the level of EU law. It is, therefore, up to organizations how to contribute to the effective implementation of the applicable rules, maximizing the benefits of the capabilities, data and other assets available in this Digital Age, while observing continuous appropriate dynamic accountability on the main and related (sub)principles and rule-sets.

Furthermore, the ethics section of this report, mostly focusing on participation and empowerment of individuals that are directly involved in or otherwise affected by the piloting activities, provided a list of questions, which are based upon the five sets of ethics principles. These principles are meant to offer guidance to the pilots' partners through the critical and delicate ethical matters involved. The five principles sets are (1) equity, diversity and inclusion (EDI); (2) transparent and informed recruitment; (3) democratic and empowering participation; (4) societal relevance; and (5) citizen-oriented data collection and governance.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

It should be taken into account that Chapter 3 rather produced an overview of key issues form the ethics viewpoint. A more detailed discussion regarding, in particular, informed recruitment and personal data protection is provided under the earlier stated WP13 deliverables.

Note that Pilots' Guide on Ethics and Regulation, in essence, forms a user-friendly guide addressed to TwinERGY partners towards effective compliance and real citizen engagement. The subsequent deliverables D12.2 1st Year Legal and Ethical Compliance Report and 2nd Year Legal and Ethical Compliance Report respectively will produce an interim and final assessment on the extent to which the aspects covered by the present report are taken into account by TwinERGY.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

References

1. COM (2021) 206: Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence ('Artificial Intelligence Act') and Amending Certain Union Legislative Acts. [**Artificial Intelligence Act**]
2. 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**]
3. 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) [**ePrivacy Directive**]
4. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 [**NIS II**]
5. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance [**Data Governance Act**]
6. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC [**ePrivacy Regulation**]
7. 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 [**GDPR**]
8. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/201 [**Cybersecurity Act**]
9. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [**Regulation on Free Flow of Data**]
10. Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU [**Directive on common rules for the internal market for electricity**]
11. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [**eIDAS**]
12. TwinERGY Consortium. Grant Agreement – 957736 – TwinERGY, August 2020. [**Grant Agreement**]

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

Annex

The consent form below was drafted in response to a request of University of Lisbon, in order to be used in interviews with experts. Those interviews were a separate activity, falling outside the scope of the project's regular piloting activities.

Annex I - TwinERGY Interview Participation / Consent Form

This consent form relates to the participation in interviews and related content by certain participants, being either a consumer or an expert in energy solutions ('Participant').

This consent form governs the participation, privacy and related matters when participating in an interview by TwinERGY and how a Participant can exercise its rights regarding its Personal Data, in accordance with the General Data Protection Regulation ('GDPR') and other related laws and regulations.

TwinERGY Research Project background:
TwinERGY is a research project, which is run by a consortium of project partners and funded under the European Union Horizon 2020 research and innovation program under the grant agreement No. 957736 ('TwinERGY') that will develop, configure and integrate an innovative suite of tools, services and applications for energy consumers in order to:

1. empower citizens to track their energy use and actively participate in the energy market;
2. raise awareness and knowledge about consumption patterns and energy behaviours;
3. increase community participation in the energy market and engagement of consumers via the Digital Twin technology;
4. encourage a green ecosystem, more sustainable and accessible to all ('Research Project').

The Research Project will introduce a first of a kind demand response framework, which allows electricity retailers and local energy communities to introduce themselves in energy markets under the roles of an aggregator or a prosumer, facilitating consumer representation in the energy sector. Please find more details on the website: https://www.twinergy.eu/.

Interview Participation:
TwinERGY will conduct interviews with stakeholders, both consumers and experts, in order to identify relevant dimensions that can help in explaining the consumer behaviour towards the adoption and continuous use of energy solutions, and validate other solutions already identified in the literature.

You are kindly invited to participate in this Research Project to advance the general knowledge on energy solutions and Participants have the right to decline participation when not interested in this Research Project.

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

The interviewer will ask the Participant to answer honestly and in the best way, no wrong answer can be given or skip any question, at Participant's choice. Please note that participation in the interviews will be on a voluntary basis and Participant will have the right to withdraw its consent regarding participation to the interview and processing it's Personal Data, at any time.

All interviews will take place in 2021. The interviews will be performed by certain authorized researchers of the NOVA Information Management School, which is one of the consortium partners of the Research Project of TwinERGY.

The interview will take approximately 30 minutes of Participant's time. The interview will be held online and might be recorded. If Participant will give its consent to record the interview, the record will solely be used to transcript the interview. After transcription of the interview, the recording will be deleted. However, Participant will have the choice to do the interview without recording.

The results of the interviews will help the researchers to understand the consumers intention to adopt and continue using the energy solutions developed during the Research Project. This will provide relevant information to TwinERGY and its project partners, especially for the consumer engagement in the current energy solutions and the ones developed during this Research Project, and to the extent applicable exclusively for the benefit of TwinERGY.

Data Collection and Protection:

TwinERGY solely collects and processes Personal Data of Participants when a Participant provides its consent when a Participant is interested to participate in the interview with regard to the Research Project. In such case TwinERGY needs to collect the following Personal Data: name, surname, e-mail address, and organization (if applicable) in order to contact the Participant and to perform such interview. All Personal Data will be kept strictly confidential and to the extent applicable exclusively for the benefit of the Research Project of TwinERGY. However, when participating in the interview, TwinERGY does not further collect and process any Personal Data of the Participants without their consent and Personal Data will be requested and provided at the choice of the Participant when participating in the interview, under the conditions as set forth in this consent form.

When a Participant participates in the interview, TwinERGY may retain those communications, responses, output and results in order to process the interview. Information and responses that Participants provide in the interview will solely be used by TwinERGY in an anonymized way for further processing, use, modifications, storage, publications, and analyzations resulting in certain outputs and results with regard to the related TwinERGY Research Project, as described above.

Any Personal Data will be processed in a proper, careful and safe manner by taking technical and organizational security measures according to the GDPR, and in accordance with the applicable laws. All Personal Data collected during the interviews shall remain within

the European Union and will be stored in a password protected statistical file on the password-protected computer at the Nova Information Management School, or on the Principal Investigator's password-protected personal laptop during the COVID-19 pandemic. All Personal Data will be retained for as long as the TwinERGY Research Project runs, and deleted after completion of the Research Project. Personal Data will be shared with the TwinERGY consortium partners in order to perform and execute the Research Project under the grant agreement. Further, TwinERGY is obliged to share and disclose Personal Data with the European Commission in order to comply with the grant agreement and audit obligations thereto.

Consent:

Please tick the box if you either would like to participate or not want to participate in an interview regarding the TwinERGY Research Project.

- o I hereby give consent to TwinERGY to participate in the interview, to contact me by the provided contact details (name, email address, organization), and that the data and results of the interview will be stored, collected and used for the purpose of the TwinERGY Research Project.

- o I do not give consent to TwinERGY to participate in the interview and to contact me.

Please add below your contact information for the TwinERGY interviews:

Your Full Name:
Your E-mail:
Your organization (if applicable):

Thank you very much! You will help the TwinERGY Research Project to develop sustainable energy solutions.

Questions, Comments or Suggestions:

If you may have any questions, comments or concerns about the Research Project, the protection of your Personal Data or any queries regarding this consent form, you can contact the following researchers:

Tiago Oliveira: toliveira@novaims.unl.pt
Catarina Neves: cneves@novaims.unl.pt

When a Participant as Data Subject under the GDPR wishes to withdraw its consent, request for access to inspection, correction or deletion of its Personal Data or other Personal Data rights request, or may have any other comments or concerns that Participant would like to discuss, please call the NOVA IMS Ethics Committee +351 912 885 311. Alternately, you can write to: NOVA Information Management School (NOVA IMS), Campus de Campolide, 1070-312, Lisboa.

This consent form is governed by EU law and supplemented by the laws of Belgium if necessary. Any and all disputes that may arise with respect to this consent form will be

Twinergy has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 957736

referred exclusively to the competent court in Brussels, Belgium. In addition, a Participant has the right to file a complaint at the national Data Protection Authority.