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

1st Legal & Ethical Compliance Report

D12.2

October 2022

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

D12.2

1st Legal & Ethical Compliance Report

Revision: v1.0

AUTHORS

Toygar Hasan Oruc	Fa Somers	Dimitra Stefanatou	Giacomo Delinavelli
Arthur's Legal	Arthur's Legal	Arthur's Legal	Arthur's Legal

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

VERSION	DATE	AUTHOR	ORG...	DESCRIPTION
v0.1	17.08.2022	Toygar Hasan Oruc	Arthur's Legal	Table of Contents.
v0.2	25.08.2022	Toygar Hasan Oruc	Arthur's Legal	Initial Input under Introduction.
v0.3	05.09.2022	Toygar Hasan Oruc, Giacomo Delinavelli, Fa Somers	Arthur's Legal	Initial Inputs under Chapter 2.
v0.4	08.09.2022	Toygar Hasan Oruc	Arthur's Legal	Additional inputs under Chapter 2.
v0.5	16.09.2022	Toygar Hasan Oruc	Arthur's Legal	Integration of the partners' inputs under Chapter 2.
v0.6	20.09.2022	Toygar Hasan Oruc, Fa Somers	Arthur's Legal	Additional input under Chapter 2 and initial Input under Chapter 3.
v0.7	28.09.2022	Fa Somers	Arthur's Legal	Input under Chapter 3.
v0.8	05.10.2022	Fa Somers	Arthur's Legal	Integration of the partners' inputs under Chapter 3.
v0.9	12.10.2022	Toygar Hasan Oruc	Arthur's Legal	Integration of the partners' inputs under Chapter 2.
v0.10	14.10.2022	Toygar Hasan Oruc, Fa Somers, Dimitra Stefanatou	Arthur's Legal	Completion of the first draft.
v0.11	17.10.2022	Toygar Hasan Oruc	Arthur's Legal	Input across the entire document.

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

v0.12	27.10.2022	Stylianos Karatzas	UoP	Review and Input across document.
v0.13	31.10.2022	Toygar Hasan Oruc, Arthur's Legal Dimitra Stefanatou		Addressing the comments from the internal reviewers and submission to the coordinator.
v1.0	31.10.2022	Athanasios Chassiakos, Stylianos Karatzas, Vasiliki Lazari, Anthony Papamanolis	UoP	Draft submitted to EC by the PC

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

Legal Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced authors will have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the European Union. Neither the CINEA nor the European Commission is responsible for any use that may be made of the information contained therein.

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 covers ethics, legislation, and standardisation related aspects pertinent to the scope of the project. This deliverable falls under Task T12.2 "Legal & Ethical Compliance Monitoring" which builds on the work done in Task T12.1 "Identification of Legal & Ethics Requirements". It aims to provide an interim overview of the project compliance with the requirements set out under D12.1 "Legal & Ethical Compliance Guide" delivered in M9 and to update the consortium partners on the latest regulatory developments in the EU which deemed relevant to the TwinERGY activities. This deliverable adheres to the structure set out in D12.1 and discusses clusters of EU regulations across four perspectives, namely: (1) market-centric, (2) human-centric, (3) system-centric and (4) data-centric.

The chapter on the market-centric regulations notes that digital domain becomes one of the highly regulated domains under the EU Digital Decade 2030 policy programme and the TwinERGY solution will likely be influenced substantially by the recent regulatory developments in the EU. Therefore, from a market-centric perspective, the TwinERGY consortium partners are invited to be prepared for the evolving EU regulatory landscape with respect to the services to be provided by the TwinERGY solution. In that regard, it is recommended that robust cybersecurity measures are implemented within the TwinERGY solution by design as to ensure robustness and competitiveness of the digital solution, should it enter the market. Particularly, it would be beneficial for TwinERGY to ensure that any of the digital modules that facilitate the 'transmission of information through a communication network' has adequate safeguards in place not only to protect user safety from unlawful or illegal activity but also to ensure the provisions of critical services to the EU citizens.

From a human-centric perspective, it is noted that transparency and fairness are the key elements for the project and represent fundamental pillars of the European data protection framework. It is suggested that personal data used within the pilots is categorised and special categories of personal data, if any being processed, is distinguished from other types of personal data. To further enhance transparency and fairness in the project, it is recommended to inform participants in a clear manner of type of personal data being processed, identity and role of organisation involved in the processing activities of the pilots. Furthermore, considering the requirements set out in the upcoming European Digital Identity regulation, it would be beneficial for TwinERGY to develop digital authentication functions that could enable any EU citizen to easily access the TwinERGY modules and services using their national digital identities without having to use private identification methods or unnecessarily sharing personal data.

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

Regarding the system-centric perspective, the partners are informed of the importance of the security by design approach in the development of digital devices, systems and services under the EU cybersecurity strategy. Furthermore, the TwinERGY partners are invited to give particular attention to potential cybersecurity vulnerabilities arising from dependencies on third-party digital devices and services as well as the use of open-source software. Lastly, it is underlined that obtaining cybersecurity certification and ensuring compliance with certain security requirements will support the trustworthiness, robustness, and competitiveness of TwinERGY solution.

The data-centric perspective mostly covers regulatory instruments that are currently still voluntary or are proposed. Therefore, there are no immediate actions required to ensure adherence to the regulatory framework mentioned under this perspective. However, in order to be future-proof and truly present state-of-the-art solutions, it is recommended to adding certain function to TwinERGY solution that enables portability of both personal and non-personal data to third-party platforms and servers by end users. Furthermore, although the TwinERGY has high level of compatibility with third party devices, the technical partners are invited to enhance interoperability of the TwinERGY modules with third party digital services in order to ensure the project compliance with the future requirements on data sharing. It should also be noted that the upcoming regulations may enable technical partners to obtain access to high value datasets help by public sector bodies necessary for the project activities.

Moreover, this deliverable also carries out an assessment of the approach of the TwinERGY project to the ethical guidelines provided in D12.1 “Legal & Ethical Compliance Guide”. Based on the various applicable regulations and related EU perspectives identified in D12.1, the partners responsible for each pilot and each of the TwinERGY modules were requested to provide answers to questionnaires. The responses to these questionnaires together with the insights gained from observing the EU stakeholders workshop held in Benetutti in September 2022 have contributed to the assessments made in this deliverable. This deliverable represents an interim assessment of the extent to which the aspects covered in D12.1 are considered and the extent to which the existing and upcoming regulatory frameworks apply to the TwinERGY project.

The part of the work captured under this deliverable is directly related to the work conducted under WP13 on Ethics Requirements, particularly D13.1 “H-Requirement No.1” and D13.2 “POPD Requirements No.2” reports, submitted in January 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

1.1 Purpose and scope

The present deliverable D12.2 "1st Year Legal & Ethical Compliance Report" is the first of two deliverables to be submitted under Task 12.2 "Legal & Ethical Compliance Monitoring" which aims at providing legal and ethical assessments of the project based on the requirements identified within Task 12.1 "Identification of Legal & Ethics Requirements". The assessment performed under this deliverable will address the objective of the Work Package 12 "Ethics, Legislation and Standardization" to ensure regulatory, legal and ethics compliance of the project with the relevant EU regulations. Given that the key TwinERGY use cases are trialled across four (4) pilot sites, namely Bristol, Steinheim, Benetutti and Athens, special emphasis in the assessment is given on the pilots and on involvement of individuals by looking into issues such as the empowerment of consumers, trustworthy collaboration between consumers and commercial actors in EU energy market, appropriate handling of personal and non-personal data and secure, trustworthy, and sustainable digital transition. Moreover, the preservation of the freedom of choice and ensuring inclusion and participation of EU citizens in decision-making procedures in digital energy management should adhere to the principles set forth under Chapters II, III & IV of the Declaration on European Digital Rights and Principles.[1] These principles, therefore, represent core aspects of the digital transformation of energy management undertaken by the TwinERGY project. With this in mind, the TwinERGY aim to develop and implement appropriate strategies, and procedures for using digital twin technology and optimising electricity demand response management in the pilots.

Consequently, this deliverable follows the EU policy initiatives and strategies relating to fair, safe and open digital services, data availability, protection of personal data, cybersecurity, and ethical values such as transparency, fairness, accountability. Because these policy initiatives and strategies have been introduced as core enablers of the EU's digital growth under the EU Strategy for Energy System Integration[2] and the European

[1] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Establishing a European Declaration on Digital rights and principles for the Digital Decade, COM(2022) 27. Available at https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Communication.

[2] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Powering a climate-neutral economy: An EU Strategy for Energy System Integration, COM(2020) 299. Available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:299:FIN.

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

Strategy for Data[3]. In this context, these initiatives and values are considered guiding principle for achieving trustworthy digital transition of energy management in local communities within the project. Therefore, this deliverable uses these values and initiatives as reference points for the legal and ethical analysis of TwinERGY. Notably, the measures, strategies, and regulatory approaches introduced at the EU level through these policy initiatives are examined in relation to the pilot activities conducted under TwinERGY. Furthermore, the analysis of the ethics-related aspects of TwinERGY such as trustworthiness of digital twins, accountability, transparency, democratic participations are provided in consideration with the EU Declaration on European Digital Rights and Principles under the present deliverable.[4]

In this context, the legal and ethical aspects of digital twin-based energy management solutions developed and trialled in the four (4) TwinERGY pilots constitute core topics of this deliverable. It is of critical importance to the way for the adequate protection of the interests of pilot participants, local communities and businesses possibly exposed to certain risks by the implementation of TwinERGY solution throughout the project duration and beyond. Therefore, this deliverable aims to provide a high level legal and ethical overview of the TwinERGY pilot activities and digital solutions, -primarily- addressed to pilot partners and technical partners developing digital services, in accordance with both the existing and upcoming relevant EU laws and policies. The goal of the legal and ethical overview is to support the partners with the most relevant legal and ethical recommendations during the implementation of the project and also to point out potential future requirements or obstacles relevant for the technology solutions envisioned by TwinERGY. It will subsequently help the partners develop future-proof energy management models in the EU. This document is, thus, not intended to provide a detailed and comprehensive legal and ethical assessment of the TwinERGY project and of the pilot activities according to the applicable EU and national laws. Moreover, the legal and ethical analysis of TwinERGY wearables being developed under Work Package 7 "Development of TwinERGY System Modules" is kept outside of the scope. However, as the project starts producing exploitable business models and products, updates of the present legal and ethical assessment will be provided under the deliverables D12.3 "2nd Year Legal &Ethical Compliance Report", due in month 36 of the project.

To this end, the deliverable is building upon the inventory of the main applicable high level regulatory and ethical requirements of direct relevance for the project captured in D12.1 "Legal & Ethical Compliance Guide" submitted under Task 12.1 "Identification of

[3] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM(2020) 66. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.
[4] European Commission, (2022), European Declaration on Digital Rights and Principles for the Digital Decade.

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

Legal and Ethics Requirements". Furthermore, the work conducted under Work Package 13 "Ethics Requirements", as captured under D13.1 "H-Requirement No.1" and D13.2 "POPD Requirement No.2", submitted in January 2021, is taken into account for the ethics consideration regarding individuals' participation to the project and processing of their personal data. Likewise, the data use license template and the best practices for data sharing, use and storage within TwinERGY pilots which was developed under the deliverable D12.5 "Data Use License Template" in January 2022 are reviewed and furthered in this document. Lastly, the present document also considers the work conducted under Work Package 2 "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.

1.2 Methodology

Given that this deliverable aims to provide legal and ethical overview of TwinERGY project activities in accordance with some of the relevant legal and ethical requirements applicable at EU level identified in Deliverable D12.1 "Legal & Ethical Compliance Guide", its content is developed from the work provided in Deliverable D12.1 "Legal & Ethical Compliance Guide" and update, where necessary, the D12.1 in line with the recent developments in EU regulatory and policy landscape. In this way, the present deliverable also complements the legal and ethical guidance provided to the partners under Task 12.1 "Identification of Legal & Ethics Requirements". Furthermore, the legal review is built on the four perspectives: (1) market-centric, (2) human-centric, (3) system-centric and (4) data-centric whereas ethical review of the project follows the guiding ethical principles explained in D12.1. However, throughout the assessment of project's compliance, special emphasis is given to the TwinERGY piloting activities and to the interaction between TwinERGY digital modules and their users by looking into certain critical issues such as the use of personal and non-personal data, governance of TwinERGY online services and platforms, trustworthy deployment of digital twins, respect of the rights of vulnerable groups. It must be noted that this deliverable refrain from presenting comprehensive legal and ethical assessment of TwinERGY project in accordance with all applicable laws and ethical principles.

To have a clear overview of the ongoing TwinERGY activities at both pilot and project levels, two (2) separate questionnaires covering the most relevant ethical and legal issues, identified in Deliverable D12.1 "Legal & Ethical Compliance Guide" and in the deliverables of Work Package 13 "Ethics Requirements", were circulated to the partners leading the pilot activities and/or developing the eight (8) TwinERGY digital modules and the interoperability platform in collaboration with the project coordinator in August 2022.

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

For the purpose of having a user-friendly questionnaire, the questions do not make references to the specific regulations discussed under the subsequent sections of Chapters 2 and 3 but instead, the questions are formulated in a way that the inputs may capture the discussions following in these chapters on both the applicable and future EU regulatory and policy frameworks.

Although the project pilots and modules are still at early implementation phase, the inputs received directly from the relevant partners in response to the questionnaires suffice to provide meaningful insights into their activities within the interim period between M10 and M24 for the present deliverables. The inputs from the respective project partners are available on the TwinERGY project repository.[5] As the questionnaires are prepared in accordance with the legal and ethical guidance presented in Deliverable D12.1 "Legal & Ethical Compliance Guide" and in the deliverables of Work Package 13 "Ethics Requirements", they maintain high level of awareness about the some of the critical legal and ethical issues and allow TwinERGY partners to self-assess their activities. Moreover, by carefully compering the partners' inputs to the questionnaires with the legal and ethical guidance, this deliverable formulates appropriate recommendations addressed to the relevant partners in order to maintain a high level of legal and ethical considerations throughout the project. This approach is further visualised in the figure below.

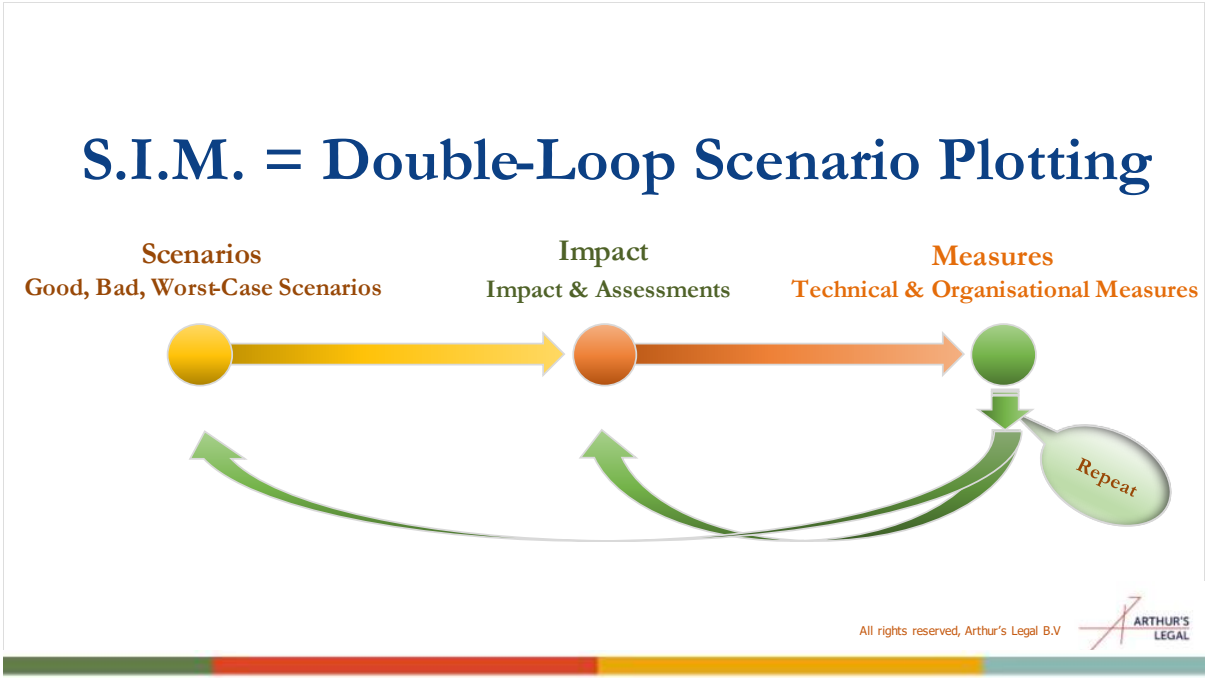

Figure 1: Double-Loop Scenario Plotting

[5] The partners' inputs to the questionnaires can be accessed at https://drive.google.com/drive/folders/1zE08nZxnvDkS8nm4adErv62FyJ9Xc2mB?usp=sharing.

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

To sum up, the legal and ethical assessment captured in the present document is based on the partners' inputs to the questionnaires and the existing applicable and forthcoming EU laws and ethical principles that have been consulted in the preparation of the questionnaire as well as in the previous legal and ethics deliverables such as Deliverable D12.1 "Legal & Ethical Compliance Guide", D12.5 "Data Use License Template", D13.1 "H-Requirement No.1" and D13.2 "POPD Requirement No.2", as listed in the References. However, it should be kept in mind that the inputs received were subject to further editing for the purpose of this document. Nevertheless, the substance of the inputs received has remained unaltered. For reference, the templates of the questionnaires addressed to the pilots and digital modules can be found in Annex I and II respectively.

1.3 Target audience

The present document builds upon the continuous dialogue with both the pilot leading partners and the partners responsible for the development of the eight (8) TwinERGY digital modules and the platform. It sheds light on the legal and ethical aspects of their activities under the existing applicable and forthcoming EU laws and ethical standards that should be upheld while pursuing the project's objectives. Therefore, this deliverable is primarily addressed to TwinERGY pilot partners and the technical partners responsible for the development of TwinERGY modules.

Furthermore, to provide appropriate level of protection for the interest of the project participants, the coherence and collaboration between the Ethics Manager, the Data Protection Officer Coordinator and TwinERGY pilot leading partners which will provide are also priorities of this document. As such coherence and collaboration bridges multiple backgrounds, angles, and perspectives, this deliverable aims to facilitate an informed and meaningful discussion among the partners and participants.

Finally, this Deliverable is addressed to the reviewers of the project and the EU Commission. For these audiences, the aim is to provide information about certain legal obligations and ethical standards that will form the development and implementation of the project. 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.

1.4 Structure

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

Following this Chapter which introduces the purpose, scope, methodology and structure of this deliverable, Chapter 2 look at the legal aspect of the project and capture the state of play in the TwinERGY pilot and modules extrapolated from the inputs to the questionnaires in Annex I and II respectively with the updated legal requirements under the most relevant, currently applicable and proposed laws at EU level. It further provides recommendations that aim to raise awareness among the pilot leaders and the technical partners responsible for TwinERGY modules of current and future legislative landscape in the EU. Similarly, Chapter 3 produces an updated guide for the ethical principles applicable in the context of TwinERGY and review the state of play in the TwinERGY pilots against the guiding ethical principles. Again, the recommendation provided thereunder assists the TwinERGY consortium in achieving trustworthy and sustainable digital transition of energy management. Finally, Chapter 4 provides for the concluding remarks, while the questionnaires for the pilots and the digital modules are presented in Annex I and Annex II respectively.

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

2 Digital Twin-Based Energy Management: Legal Aspects

In order to assess the legal aspect of Digital Twin-based Consumer-Centric Energy Management and Control Decision Support Mechanism, 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 the EU laws and legal requirements explained in D12.1 "Legal & Ethical Compliance Guide" make the spine of this chapter, it also expands the scope by providing reviews of the Digital Services Act, the Digital Markets Act, the Open Data Directive, the Data Act and Cyber Resilience Act which were not captured in D12.1"Legal & Ethical Compliance Guide".

The purpose of this expansion is to fully align the TwinERGY regulatory landscape with the key actions set out in the EU Strategy for Energy System Integration such as system-wide digitalisation of energy sector and development of a sustainable, (cyber)secure, transparent and competitive market for digital energy services, ensuring data privacy and sovereignty, and supporting investment in digital energy infrastructure.[6] Furthermore, considering that digitalisation and the required extensive use of data comes with a set of legal challenges, particular attention is given to the EU laws related to privacy and data protection, and cybersecurity. .

However, given the current implementation phase in the pilots, several EU laws focusing on products and services ready to be put on the EU market such as the Directive on common rules for the internal market for electricity[7], Consumer Rights Directive[8], Directive on Unfair Terms in Consumer Contracts[9], the Product Liability Directive[10] and

[6] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Powering a climate-neutral economy: An EU Strategy for Energy System Integration, COM(2020) 299. Available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:299:FIN.
[7] 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.
[8] 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.
[9] 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.
[10] 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.

General Product Safety Directive[11] will be further elaborated upon in the subsequent deliverable i.e. D12.3 which is the 2nd Legal and Ethical Compliance Report due in October 2024. For the scope of TwinERGY, contract law remains relevant for the TwinERGY output. However, any contractual arrangements in place should be managed in accordance with the relevant provisions dictated under the relevant applicable national laws.

Similar to the D12.1 "Legal & Ethical Compliance Guide", 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. 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 2: Key Aspects of Regulations in the TwinERGY Era

In light of above, the chapter below discusses legal requirements in EU laws which are of direct relevance for TwinERGY and assess TwinERGY pilots and modules against these legal requirements. However, it does not provide an exhaustive list of all legal requirements applicable to the project nor it constitute a comprehensive legal assessment of TwinERGY pilots and modules. In addition, it is important note that this Chapter elaborates only on legislations applicable at an EU level but does not conduct legal assessment with regard to applicable national laws pertaining to the pilots. The regulations discussed below are primarily relevant for the three TwinERGY pilots i.e. the pilots taking place in Steinheim, Benetutti and Athens pilots, and to the extent to which the regulations are applicable in the Bristol pilot. Furthermore, under each perspective,

[11] 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.

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

state of play in the pilots are captured in accordance with the reviewed legal requirements and then respective recommendations are provided to the partners accordingly.

2.1 Market-Centric Perspective

Keeping the relevant stakeholders of the TwinERGY Project in mind, it is pertinent to state at the outset the two primary relationships relevant for this section, i.e., regulatory relationship and the contractual relationship. In the TwinERGY project, the nature of contractual relationships will vary from situation to situation and may include contractual relationships that only require minimal interaction with a short duration. Conversely, it may also involve complex multi-party contractual relationships that may span for several years. Regardless, it is important to take cognizance of the contractual relationships in order to gain a better understanding of how the existing regulations impact the diverse group of stakeholders.

In relation to the regulatory environment of the energy sector, there are five layers that need to be taken into account: local, regional, national, European, and universal. These five layers are visualised in Figure 3, below. The following sections of this Deliverable will focus on the applicable legal framework specifically for the EU level. In the energy sector and its related prosumer ecosystems (small, medium or large), there are multiple personas at play. Therefore, the focus is not solely on energy demand and supply, but also the demand and supply of various other essentials, such as systems, data applications and networks.

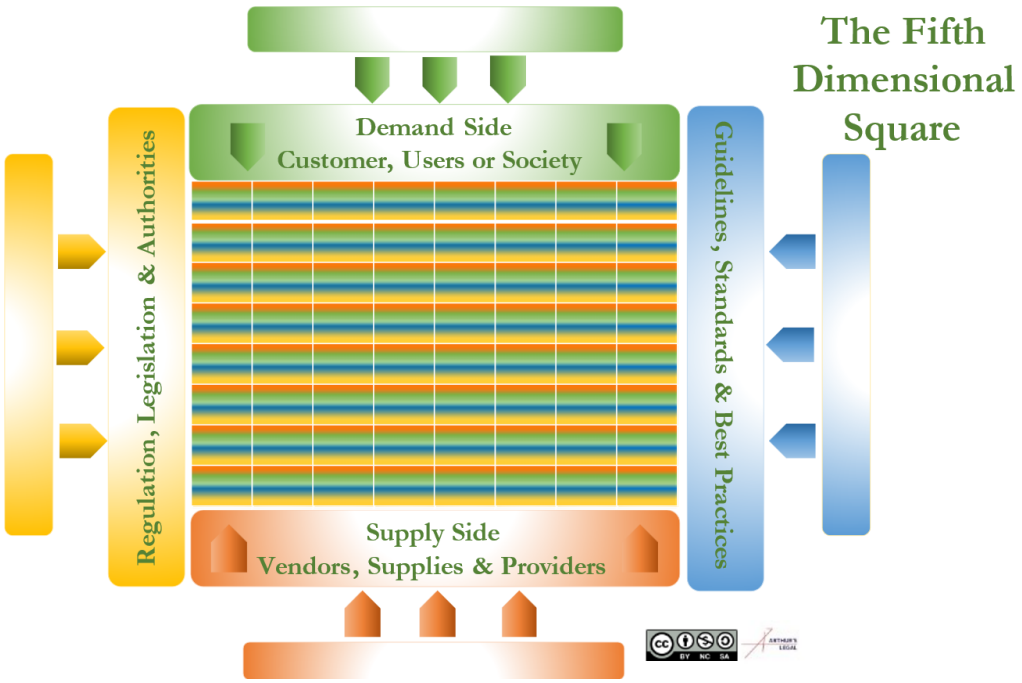

Figure 3: The Fifth Dimensional Square

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

The European Commission aims for a digital transformation of Europe by 2030. The EU's digital decade evolves around four cardinal points, namely, skills, government, infrastructures, and business. In relation to the market-centric perspective of the TwinERGY project, there are five regulatory frameworks that need to be considered; there are illustrated in Figure 4 below:

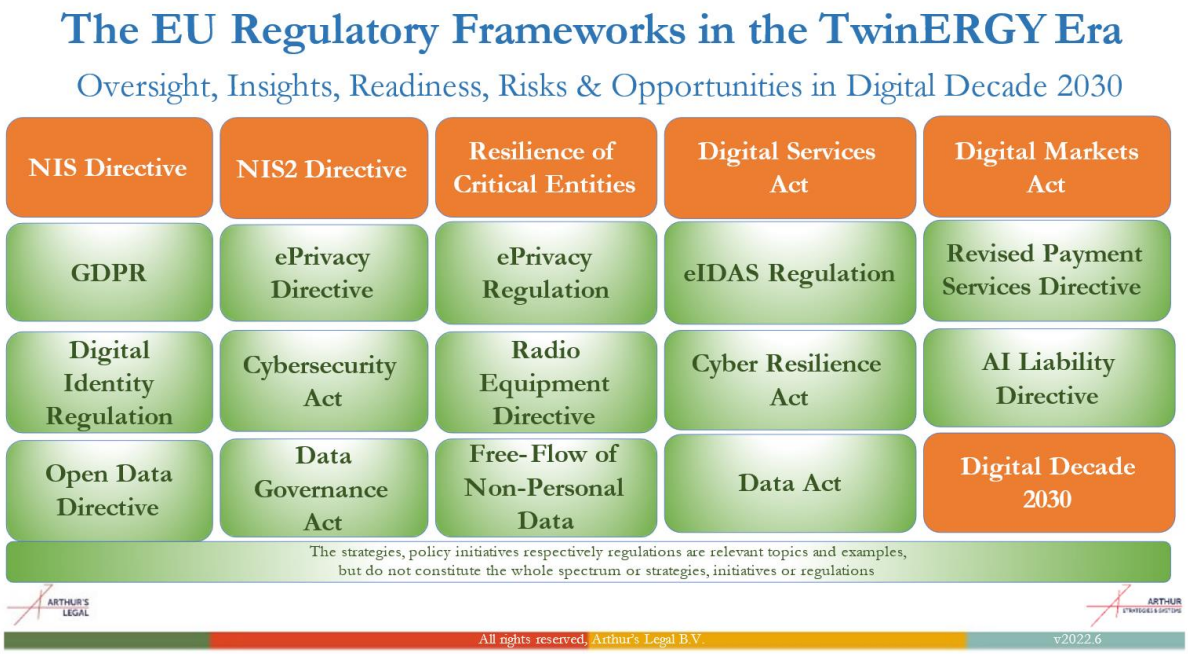

Figure 4: The EU Regulatory Frameworks from a Market-Centric Perspective

The TwinERGY project deals with the supply of electricity, which triggers applicability of the Directive concerning measures of a high common level of security of network and information systems across the Union ('NIS Directive'). Under the NIS Directive, services that provide the electricity supply fall under the Directive's definition of 'essential services'.

Moreover, the TwinERGY project also involves the development and offering of digital services to consumers. As such, triggering the applicability of the Digital Services Act package. The Digital Services Act package represents the European Commission's legislative initiatives to upgrade rules governing digital services in the EU. The package has two main goals, namely, to create a safer digital space in which fundamental rights of all users of digital services are protected and to establish a level playing field to foster innovation, growth, and competitiveness in the European Single Market and globally.

2.1.1 The Security of Network and Information Systems Used in TwinERGY Project

The NIS Directive intends to provide a risk-based framework on operational aspects and economic losses. Under the NIS Directive, Member States were required to ensure that

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

operators of essential services and digital service providers take appropriate and proportionate technical and organisation measure to manage the risks posed to the security of network and information systems utilised in their operations.[12] As a result, in the event of an incident, organisations are required to notify the relevant competent authorities without undue delay. In accordance with the NIS Directive, an 'incident' is any event having an actual adverse effect on the security of network and information systems.[13] As such, not all security incidents fall under the scope of the NIS Directive, only incidents that affect the availability, integrity, authenticity or confidentiality of network and information systems used for the provision of essential services under the Directive.

The NIS Directive has also been implemented in the United Kingdom through the Network and Information Systems Regulation 2018 ('NIS Regulation'). The UK government reviewed the NIS Regulation in May 2020, based on the evidence gathered for the review, it was determined that it was too early to establish the long-term impact of the regulations.

The NIS2 Directive, on which EU Parliament and the Council reached a political agreement on 13 May 2022, aims at extending and future-proofing the scope of the existing NIS Directive to keep up with the unprecedented digitalisation that has occurred in the last few years. Once adopted, the NIS2 Directive will replace the existing NIS Directive and Member States must transpose the Directive into their national laws within 21 months. The provisional agreement text of the NIS 2 Directive expands the scope of essential and important entities that would be subject to the security requirements under certain circumstance to the following three (4) categories that could be relevance of TwinERGY: i-) operators of demand response or energy storage services or aggregation services; ii-) operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider; iii-) cloud computing service providers and iv-) providers of online marketplaces or social networking platforms. Moreover, additional security requirements have been included under the NIS2 Directive, in addition to a list of focused measures, such as, incident response and crisis management, cyber security testing, use of encryption and vulnerability handling and disclosure. In accordance with the NIS 2 Directive, enhancing the overall level of cybersecurity could

[12] 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
[13] NIS Directive, art 4(7)

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

prevent environmental risk or damage in case of an attack on essential services, particular in energy, water supply, and distribution or transport sectors.[14]

In line with the NIS 2 Directive, the proposal for a directive on the resilience of critical entity on which EU co-legislators have reached a political agreement on 28 June 2022, ('RCE') considers providers of demand response or energy storage services or aggregation services as critical entities since these services are deemed vital for the livelihoods of EU citizens and the proper functioning of the internal market.[15] Although the RCE lays down obligations for Member States to take specific measures under national strategies aimed at ensuring the unobstructed provision of these essential services in the internal market, it also establishes direct obligations on critical entities to enhance their resilience such as requirements to carry out regular risk assessments, to take technical, security, and organisational measures and requirements for notification of incidents to competent authorities.

2.1.2 Providing Secure Digital Services for TwinERGY Participants

The Digital Services Act ('DSA') is envisioned to improve consumer protection and safeguard fundamental rights of individuals in the digital domain. Moreover, the DSA aims to increase transparency and accountability obligations for online platforms. Providers of intermediary services, hosting services, online platforms and very large online platforms fall under the scope of the DSA.

The rules specified in the DSA primarily concern online intermediaries and platforms. For example, online marketplaces, social networks, content sharing platforms, app stores and online travel and accommodation platforms. The obligations under the DSA vary for various online service providers, depending on their role, size and impact in the digital ecosystem.

The DSA will be entered into force on 16 November 2022 and will be directly applicable across all EU Member States as of 17 February 2024 except for certain obligations

[14] European Parliament, Final compromise text of EU Commission's Proposal for a Directive the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), repealing Directive (EU) 2016/1148, 17 June 2022. Available at https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/.

[15] European Parliament, Final compromise text of EU Commission's Proposal for a Directive the European Parliament and of the Council on the resilience of critical entities, 16 September 2022. Available at https://www.consilium.europa.eu/en/press/press-releases/2022/06/28/eu-resilience-council-presidency-and-european-parliament-reach-political-agreement-to-strengthen-the-resilience-of-critical-entities/.

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

regarding transparency of online service provider and very large online platforms which apply from 16 November 2022.

2.1.3 Creating A Level Playing Field for Digital Services in the EU

The Digital Markets Act ('DMA') sets out new rules that aim to foster innovation, growth, competitiveness, and facilitate the scaling up for smaller platforms, SMEs and start-ups. These new rules will rebalance the responsibilities of users, platforms and public authorities will place people at the centre, in accordance with European values. Aiming to promote fairness and contestability in the digital sector by regulating the gatekeeper power of large digital companies, the DMA establishes a set of criteria to classify certain platforms as "gatekeepers". These "gatekeepers" must comply with the rules set out under the DMA.

Gatekeeper platforms are digital platforms with a systemic role in the internal market that function as bottlenecks between businesses and consumers for important digital services.

Under the DMA, organisations that qualify as gatekeepers will be subject to a specific set of rules and are required to proactively implement certain behaviours that makes markets more open and contestable. The DMA will trigger obligations for ten core platform services. Relevant to the TwinERGY project are online intermediation services, online social networking services, operating systems, and number independent interpersonal communication services.

The DMA enters into force on 1 November 2022 and will be applicable as of 2 May 2023 except for certain obligations.

2.1.4 The State of Play in TwinERGY

Although the TwinERGY project undertakes activities with regards to electricity supply and transmission, which are considered 'essential services' under the existing NIS Directive, the inputs from the pilots and partners show that the TwinERGY solution, itself, does not 'supply' electricity nor 'operate' electricity distribution or transmission systems as defined in Art 2 of the Internal Market for Electricity Directive. Moreover, due to the fact that the project is still in the piloting phase; it is unlikely that the TwinERGY pilots would be identified as operators of essential services, as it does not provide 'a service which is essential for the maintenance of critical societal and/or economic activities.' On the other hand, if the NIS 2 Directive enter into force and depending on the future uptake of the TwinERGY solution when it is launched into the EU market, it might be subject to the security requirements set out under NIS 2 Directive as essential service. Particularly,

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

based on the inputs from the technical partners, considering the services provided by Deman Flexibility Module, DER Management Module, Transactive Energy Module and TwinEV Module, the TwinERGY solution might be considered as electricity demand response, energy storage services and aggregation services respectively under the NIS 2 Directive. However, this will not be enough to trigger the application of the NIS 2 Directive since it also requires additional conditions. For example, operators of essential services must also be qualified as medium-sized enterprises.

At the current stage and based on the input received by the Pilots, it is not envisioned that the activities of the TwinERGY project will trigger the applicability of the DMA. The DMA applies to digital platforms that classify as 'gatekeepers'. None of the activities currently undertaken by the TwinERGY project would result in its classification as a gatekeeper under the DMA. The activities undertaken by the TwinERGY project do not, as of yet, cause it to have a significant impact on the internal market nor enjoy an entrenched and durable position in its operations, now or in the foreseeable future.

Based on the input received from the TwinERGY partners involved in the development of the Social Network Module, the Module may be considered an 'intermediary service' under the DSA. The input received from the partners involved in the development of the Social Network Module states that there are appropriate measures in place to tackle unlawful or illegal activity of users that may arise through the use of the Social Network Module. The Social Network Module informs users regarding their terms and conditions of use. Through the Notification Board, the Social Network Module provides mechanisms to report any unlawful or illegal activity.

2.1.5 Key Takeaways

Although the TwinERGY solution is likely to fall outside the scope of the NIS Directive at the current stage, in general, the implementation of appropriate cybersecurity measures may significantly prevent risks or damage in case of an attack and, therefore, create benefits for the future exploitation of solutions such as TwinERGY. Such an implementation could, first, increase the robustness and competitiveness of related solutions. Secondly, as explained in the state of play section above, the NIS2 Directive may become directly relevant in the future as the TwinERGY use cases and practices scale and become substantial part of electricity market. Overall, adopting security by design approach increases the future proofness of the technological solutions, especially, of those addressed to the EU market, while facilitating compliance with national resilience strategy to be adopted once the RCE comes into force.

The only module under the TwinERGY project that potentially triggers the applicability of the DSA in the future is the Social Networking Module. This is because the Social Network

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

Module's Notification Board involves services 'consisting of the storage of information provided by, and at the request of, a recipient of the service' which may fall under the scope of intermediary service e as defined in the DSA.

At the current stage, the upcoming DMA is not immediately applicable to the TwinERGY project. This is due to the size and envisioned scale of the TwinERGY solution. The DMA may perhaps only be applicable to the TwinERGY solution once it enters into the market and starts to acquire more users. Currently, the DMA, thus, arguably acts as a tool that may help foster the scaling up of the TwinERGY solution.

2.2 Human-Centric Perspective

The involvement of individuals stands as an essential element during the project implementation as the TwinERGY energy management concept rely on both processing of participants' personal data via connected devices such as smart meters, smart plugs, EV, private PVs and the digital services used by the participants to execute electronic transactions to purchase electricity on dynamic tariffs and to sell their flexible energy loads on an open market to the (micro) grid operators or to each other. Therefore, this section focuses on the three (3) aspects of the TwinERGY concept, i.e., processing of personal data, electronic identification for digital services and secure online transactions, and it provides an overview of the legal requirements under the currently applicable and proposed EU laws highlighted in the Figure 5 below.

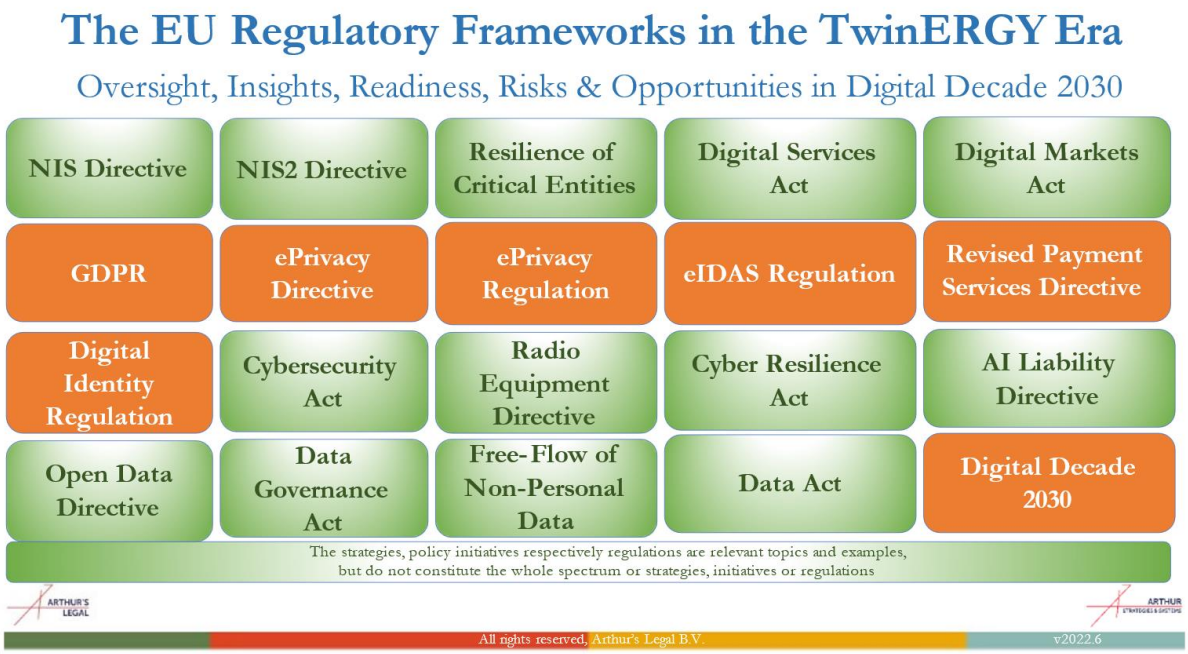

Figure 5: The EU Regulatory Frameworks from a Human-Centric Perspective

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

In light of these regulations and the inputs provided by the partners to the questionnaires attached to this deliverable, the state of play in TwinERGY pilots are identified. Furthermore, upon a review of the state of play, key takeaways are addressed to the relevant partner to assist them in improving the state of play. It should be noted that given that the project in still in early implementation stage, other human-centric EU laws such as Consumer Rights Directive, the Directive on Unfair Terms in Consumer Contracts, and the Digital Content Directive[16] are not discussed in this chapter. However, the relevant legal requirements under these laws will be analysed in D12.3 "2nd Legal & Ethical Compliance Report" to prepare the project partners for the exploitation of the TwinERGY outcomes in the European single market.

2.2.1 Protection of Personal Data

This section mainly focusses on the privacy and data protection aspects of TwinERGY pilot activities and builds upon the discussion made in D13.1 "H- Requirement No.1" and D13.2 "POPD - Requirement No. 2". The analysis and recommendations made under this section are supportive and ancillary to the work produced under the Work Package 13 "Ethics Requirements". Therefore, TwinERGY partners, particularly the partners leading the pilot activities, are advised to read this section in connection with the discussion in Work Package 13 deliverables.

Privacy and data protection as whole is of key importance to address when collecting and further processing personal data, both for measuring the well-beings of participants and the energy consumption and generation at households, or for tracking behaviours and mobility of the participants. For the purpose of producing a tangible overview of the data protection requirements relevant to TwinERGY, the sections below elaborate on the processing of special category of personal data, responsibility of data controller and data processor, and the legal requirement to carry out a data protection impact assessment under the EU data protection regulatory framework.

Processing of Sensitive Personal Data under the GDPR and the e-Privacy Directive

A definition of sensitive data is provided in Annex 1 of D12.5 "Data Use License Template". This definition is in line with the definition of special category of personal data under Art. 9(1) of the GDPR, '*data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data,*

[16] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136/1. Available at https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32019L0770.

biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.[17] The processing of sensitive personal data is in principle prohibited in the EU, except in specific circumstances. It can be processed only if the processing has at least one of the legal grounds set out in Art 6(1) GDPR and it satisfies one of the specific circumstances in Art 9 GDPR for instance, if the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on EU or Member State laws, or with explicit consent of the data subject. On the other hand, processing of personal data stored in the participants' connected devices including storing and gaining access to such information or processing of location data or behaviour data of participants by their personal devices such as wearable requires prior consent of participants according to Articles 5(3) and 9 of ePrivacy Directive.[18] Reading these two EU laws together, it can be concluded that storing and accessing sensitive personal data in personal connected devices require prior explicit consent of individuals.[19]

The concept of explicit consent and the acquisition of a valid consent in terms of human participation to research project have already explained in Chapter 3.3 of D13.1 "H-Requirement No.1" and in Chapter 4.4 of D13.2 "POPD - Requirement No. 2". As a follow-up discussion, this deliverable provides further information on some specific requirements regarding the use of explicit consent for the processing of sensitive personal data.

Consent for processing of personal data is defined under Article 4(11) of the GDPR as: 'any *freely given*, *specific*, *informed* and *unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*.'. This definition can be dismantled into 4 elements: freely given, specific, informed and unambiguous indication of the data subject's wishes. The element "free" implies real choice and control for individuals.

As a general rule, the GDPR prescribes that if the individuals have no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent of such individual will not be valid. The 'freely given' consent also requires that the individual concerned should be able to refuse or withdraw his or her consent without any detriment. The second element, the specificity of consent requires that consent must

[17]General Data Protection Regulation, Article 9(1).
[18] ePrivacy Directive, Articles 5 and 9.
[19] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, European Data Protection Board, 12 March 2019.

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

be given for a specific processing purpose. Different purposes should not be bundled up in a single consent which could result in use of personal data which was not anticipated by the individual and there his/er loss of control.[20] As for the third element, the consent form must inform individuals about the certain elements that are crucial to make a choice. According to European Data Protection Board (EDPB), at least the following information must be provided in clear and plain language to the individuals for obtaining valid "informed" consent: i) the identity of the data controller(s), ii) the purpose of each of the processing operations for which consent is sought, iii) what (type of) personal data including sensitive data will be processed, iv) the existence of the right to withdraw consent, v) information about the use of the data for automated decision-making and vi) on the possible risks of data transfers and vi) on the possible risks of data transfers.[21] The last element of a valid consent is a statement or a clear affirmative act of individuals that shows an unambiguous indication of his/her acceptance of processing.

The term "explicit" comes into the scene in this fourth element and it refers to the way how consent is expressed by individual. The explicit consent requires an express statement of individual. An obvious way to make sure consent is explicit would be to have the individual concerned to expressly confirm his/her consent in a signed written statement.

Even if a valid explicit consent is obtained, there are additional requirements that need to be fulfilled by the data controller in the processing of sensitive data. First, it is particularly important to make sure the data controller collect and retain only the minimum amount of sensitive personal data and specify which categories of sensitive data such as health data, ethnicity data etc., is processed. Furthermore, processing of sensitive data requires additional security measures than the processing of non-sensitive personal data. Thirdly, the data controller is required to keep record of its processing activities including documenting the categories of sensitive data; how the processing satisfies a lawful basis for processing sensitive personal data under Art 6 and 9 of the GDPR; and whether proper data retention and deletion policies are followed. Lastly, in case sensitive data are processed on a large scale, the data controller is required to carry out a data protection impact assessment before initiating processing activities.

Relationship Between Data Controller and Processor under the GDPR

Proper identification of the roles of data controller and processor is crucial for every data processing activity. Because the allocation of responsibilities, obligations, and liabilities

[20] Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, European Data Protection Board, 4 May 2020.
[21] Ibid, p 15.

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

arising from the GDPR regarding data processing operations depend on the actual roles of the parties. The data controller is defined in Art 4(7) of the GDPR as "*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*".[22] The important factor in identification of data controller is its power/control over the decisions on both purposes and means of the processing, i.e. the *why* and *how to process*. Once an entity is identified as data controller, then it becomes accountable for processing activities and responsible for the compliance with the GDPR requirements. This includes among other things that being responsible for protecting and respecting data subject rights, implementing appropriate technical and organisational effective measures to ensure and demonstrating that processing is performed in accordance with the GDPR. Furthermore, as per Art 82(2) of the GDPR, the liability for the damage caused by processing of personal data which infringes the GDPR primarily falls on the data controllers.[23] In case the determination of the purposes and means of a processing is made by two or more entities, then these entities may qualify as joint controllers. The joint controllership can take the form of a common decision or result from converging decisions taken by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing.[24]

On the other hand, data processor is defined in Art 4(8) of the GDPR as "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*". Accordingly, there are two basic conditions for qualifying as processor; first processor must be a separate entity in relation to the controller, and secondly, it processes personal data on the controller's behalf.[25] As processor must be a separate entity, a department within a data controller company cannot be a processor to that controller. Moreover, employees acting under the direct authority of the controller cannot be deemed as processors since they will process personal data as a part of the controller's entity. Second condition of acting "on behalf of" requires processor to implement the instructions given by the controller regarding the purpose of the processing and the essential elements of the means and to serve controller's interest in processing personal data.[26] Furthermore, this condition also requires that the processor cannot carry out processing for its own purpose. If processor goes beyond the controller's instructions and starts to determine its own purposes and means of the processing, the

[22] General Data Protection Regulation, Article 4(7).
[23] General Data Protection Regulation, Article 82(2).
[24] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, European Data Protection Board, 07 July 2021.
[25] General Data Protection Regulation, Article 4(8).
[26] General Data Protection Regulation, Article 28.

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

processor will then be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.[27]

Due to this secondary role in data processing activities, processor's responsibility is rather limited than the data controller.[28] However, some of the more specific rules are addressed to both controllers and processors, such as the rules on supervisory authorities' powers in Art. 58 of the GDPR. Both controllers and processors can be fined in case of non-compliance with the obligations of the GDPR that are directed to them, and both are directly accountable towards supervisory authorities by virtue of the obligations to maintain and provide appropriate regarding the data processing activities. In terms of liability toward individuals, processors shall be liable for the damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.[29] Moreover, the GDPR requires data controllers use only the processors that can provide sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the security requirements of the GDPR. Any processing of personal data by a processor must be governed by a legal act or a written contract, including in electronic form, and be binding. The required content of such contract is provided in Art. 28(3) of the GDPR, such as the subject-matter, duration, nature of the processing, type of personal data being processed, the obligations and rights of the controller and processor.

Data Protection Impact Assessment under the GDPR

As per Art. 35 of the GDPR, in principle, a data protection impact assessment (DPIA) is required where personal data processing "*is likely to result in a high risk to the rights and freedoms of natural persons*".[30] This means that data controllers are only required to carry out a DPIA if their envisaged data processing activities include i) processing of personal data, and ii) the processing constitutes a high risk in particularly where a type of processing includes use of new technologies. To determine whether processing is "likely to result in a high risk", the EDBP provides data controllers with a list of nine criteria together with some examples. According to the EDBP, personal data processing meeting two or more of these criteria are more likely to constitute a high risk to the rights and

[27] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, European Data Protection Board, 07 July 2021.
[28] General Data Protection Regulation, Article 24.
[29] General Data Protection Regulation, Article 82(2).
[30] It should be noted that there are exemptions to this requirement under Article 35 of the GDPR. For instance, the data controller is not required to carry out a DPIA if the nature, scope, context and purposes of the envisaged processing are very similar to the processing activity for which DPIA have already been carried out or, if a processing activity has a legal basis in EU or Member State law, where the law regulated the specific processing operation.

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

freedoms of individuals, and therefore the controllers are required to carry out a DPIA. However, the EDBP notes that in some cases where the risk is too serious, even only one of these criteria may obliges the data controller to carry out a DPIA. EDBP's criteria together with brief descriptions and examples is made available in Appendix I.

It should be further noted that even if the envisaged processing operation may correspond to one of the examples in Appendix I, such processing can still be considered by the controller not "likely to result in a high risk". In such cases the controller is advised to justify and document the reasons for not carrying out a DPIA and obtain the views of the data protection officer if any prior to the processing. Furthermore, given that national data protection authorities are required to establish, make public and communicate a list of the processing operations that require a DPIA in line with these nine criteria, as per Art 57(1)(k) of the GDPR, data controllers should take into account those lists published by the competent national data protection authority when assessing whether their envisaged data processing require a DPIA. As mentioned in D13.2 "POPD - Requirement No. 2", the controller must seek the advice of the data protection officer (DPO), and ask processor, if any, to provide assistance in carrying out the DPIA.

In case the data controller decides to carry out a DPIA, it must include at least: i) a description of the envisaged processing operations and the purposes of the processing; ii) an assessment of the necessity and proportionality of the processing; iii) an assessment of the risks to the rights and freedoms of data subjects and iv) the measures envisaged to mitigate the identified risks and to demonstrate compliance with the GDPR.[31] DPIA should be completed as early as is practicable in the design of the processing operation and updated throughout the lifecycle of the processing operation. DPIA is an on-going process, not a one-time exercise and therefore it should be continuously reviewed, and the risk should regularly be re-assessed by the controller.[32]

2.2.1 Digital Identification and Secure Cross-border Payments

To accomplish the interconnection of prosumers in local energy communities and to facilitate meaningful participation of consumers in energy transactions in the TwinERGY project, building trust between different actors in energy markets must be priority. Particularly, creating online environment where every actor can verify each other's identity and payments for electricity transactions can be securely concluded can realise

[31] General Data Protection Regulation, Article 35(7).
[32] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Article 29 Working Party, WP 248 rev.01, 4 April 2017.

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

these objectives. Therefore, this section reviews the EU laws aiming to build trust in digital ecosystem across the Union.

Establishing a Framework for a European Digital Identity

As explained in detail in D12.1 "Legal & Ethical Compliance Guide", the implementation of the Regulation on electronic identification and trust services for electronic transactions in the internal market ('eIDAS') is one of the first and most modern legal frameworks for cross-border electronic identification and authentication in the EU.[33] It provides the possibility for people and businesses of a Member State to make use of their national electronic identification schemes ('eIDs') to gain access to public services of other Member States where eIDs is available. The eIDAS also aims at establishing a framework for the use 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 current eIDAS legal framework relies on national eID schemes and reaches, de facto, only a relatively small segment of users' electronic identification needs. Therefore, in June 2021, the European Commission proposed a legal framework for a European Digital Identity for the benefit of EU citizens, residents and businesses in the EU. [34] The proposal aims to enlarge its scope from relying on national digital identity schemes to electronic attestations of attributes that are valid at across the EU and enable EU-wide secure electronic identification. Each Member State will be required to issue a European Digital Identity Wallet within 12 months after its entry into force.[35] The European Digital Identity wallets will be built on the basis of trusted digital identities provided by Member States under eIDAS and aim at extending the benefits to the private sector and offering personal digital wallets that are safe, free, convenient to use, and protect personal data. The use of the European Digital Identity will be voluntary and free of charge to natural person.

The proposal aims at empowering people by allowing them to choose which aspects of their identity and data they wish to share with third parties. Furthermore, the proposal requires providers of web browsers to facilitate the use of qualified certificates for website authentication which allows users to identify who is behind a specific website.

[33] 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, L 257/73. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

[34] European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM(2021) 281. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281.

[35] Ibid, Art. 1(7).

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

Creating An Integrated Market for Payment Services in the EU

The legal requirements set out by the Revised Payment Services Directive ('PSD II')[36] are reviewed in D12.1 "Legal & Ethical Compliance Guide" and they are found not to be of direct relevance for the TwinERGY outputs. However, considering the progress made in the TwinERGY project, this document re-assesses the applicability of the PSD II for the TwinERGY modules.

Pursuant to Art 2(1), the PSD II applies to payment services; enabling i) cash to be placed on or withdrawn from a payment account, ii) execution of payment transactions of direct debits, credit transfers or through a payment card, iii) issuing of payment instruments, iv) money remittance, v) facilitating the use of online banking to make payments online by creating an interface to bridge between the consumer's and the merchant's accounts and filling in the information needed for the bank transfer (payment initiation services), and vi) allowing customers to have a global view of their financial situation and to analyse their expenses and financial needs by collecting and storing information from a customer's different bank accounts in a single place (account information services), provided within the Union .[37]

On the other hand, Art 3 of the PSD II excludes certain payment transactions and services from its scope. For instance, payment services based on specific payment instruments that can be used only in a limited way such as within the issuer's premises or certain limited networks or used to only acquire a "limited range" of goods or services offered by a specific retailer or retail chain are excluded from the scope of this directive. However, the value of the payment transactions in this so-called limited network cannot exceed the threshold of EUR 1 million.[38] Furthermore, payment transactions carried out between the payer (e.g. a consumer) and the payee (e.g. a merchant or electricity retailer) through a commercial agent (e.g. a marketplace operator) authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer and/or the payee.[39] However, this only applies to transactions where the commercial agent is acting on behalf of one side of the transaction, either the payer or the payee and not both of them. In line with this, online marketplaces which manage the flow of payments for the transactions occurred on its own platform should carefully consider whether they act on behalf of

[36] 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, (Revised Payment Services Directive). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366.
[37] Revised Payment Services Directive, Articles 2 and 4, Annex I.
[38] Revised Payment Services Directive, Articles 3(k) and 37(2).
[39] Revised Payment Services Directive, Articles 3(b).

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

either the payer or the payee or on behalf of both, in order to assess whether they can rely on this commercial agent exclusion, or whether they may need to apply for a license under PSD II. These exemptions are the most relevant to the TwinERGY project among others stipulated under Article 3.

Although there are other exemptions stipulated in PSD II such as payment transactions within the framework of a non-profit or charitable activity or payment transactions by a provider of electronic communications networks for purchase of digital content where the cumulative payment value does not exceed EUR 300 per month, for the sake of delivering concise assessment, this section does not further discuss the rest of exemptions.

2.2.2 The State of Play in TwinERGY

This chapter discusses the state of play in TwinERGY project in terms of certain aspects of personal data protection, electronic identification, and payment services envisaged in TwinERGY.

Protection of Personal Data

According to D13.2 ""POPD - Requirement No. 2", the TwinERGY pilots collect, process, and share the following types of data which may contain personal data such as i) audio recordings, photos, videos of participants from interviews, workshops, questionnaires, ii) data from surveys, social media data, and observational analysis including name, surname, e-mail address, and affiliation of participants iii) user ID, password, smartphone GPS coordinates, and biometric information , iv) data related to energy generation, usage and consumption in households, and v) physiological state, mobility habits and preferences of participants. Considering this wide scope of personal data being processed in the pilots, it is likely to some of these data qualify as sensitive personal data under Art. 9(1) GDPR. Particularly, visuals such as photos or videos of participants and data related to physiological state and mobility habits under certain circumstances may reveal racial or ethnic origin, religious or philosophical beliefs, political opinions, and health data of participants. For example, a picture of an individual with a wheelchair may perhaps be considered as health data or location data of EV used by a particular participant may be linked to places of worship visited by him/her or participant's presence at political demonstrations. Furthermore, depending on the content of surveys and questionnaires, the pilots may also end up collecting sensitive personal data. For instance, in the very recent case from the Court of Justice of the European Union, it is concluded that not only inherently sensitive data, but also of data revealing information of that sensitive nature indirectly, following an intellectual operation involving deduction or cross-referencing can

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

qualify as sensitive personal data. In line with this judgement, information regarding marital status of participants, identities of cohabitee or partners or membership of undertakings, establishments, associations may result in processing of sensitive personal data. Given that the TwinERGY pilots rely on participant's consent for processing of their personal data as mentioned in D13.2 "POPD - Requirement No. 2", such consent should satisfy all conditions set out in Chapter 2.2.1 to be qualified as "explicit" consent under the GDPR.

In terms of data controller role in the pilots, the inputs collected from the pilots show that the Athens, Bristol and Steinheim pilots have more than one partner that determine the purpose and means of data processing activities. Therefore, there may be joint controllership in the processing of personal data in these pilots. Since data controllers are mainly responsible for the personal data collected and provided by the participants, the obligations of the implementation of the appropriate technical security measures are assigned to joint data controller partners. This requires joint controllers to arrange between themselves who will take primary responsibility for complying with GDPR obligations and in particularly transparency obligations and individuals' rights. This arrangement must reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects and the essence of the arrangement should be made available to the data subject. D12.5 "Data Use License Template" notes that the Bristol pilot have agreements in place such as data sharing agreement where the responsibilities and roles of the pilot partners are regulated. Furthermore, under Annex 1 of D12.5, the roles of joint controllers in Bristol pilot are conveyed to data subjects.

With respect to the use of data processor, the data controllers in Bristol and Athens pilots provide access to personal data of participants to other partners who will process this data for the pilot use cases. This access to personal data and processing of it by the pilot partners other than the data controllers may qualify other partners as data processors. Pursuant to Art 28 of GDPR, data controllers of Bristol and Athens pilots are required to govern processing by the data processors in a written arrangement which sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the processor. Deliverable D12.5 "Data Use License Template" indicates that the Bristol pilot have already agreements in place such as data processing agreement with those partners or third party which have access to personal data.

Lastly, the inputs from the pilots show that the Bristol and Athens pilots have assessed the necessity for carrying out DPIA. Bristol Pilot notes that their privacy impact assessment reveals that a full PIA was not necessary for the pilot. Athens Pilot plans to carry out a DPIA when they commence data processing and integrate into the TwinERGY platform.

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

Electronic Identification Requirements

The eIDAS Regulation and the proposal for a European Digital Identity are of relevance to TwinERGY given its focus on digital twins and the use of TwinEV Module and Transactive Energy Module where prosumers can conclude energy transactions. At the current stage, the identification of users in TwinEV Module are provided by single sign-on authentication scheme.[40] On the other hand, in other digital modules, personal credentials are used for the identification of individuals.

Secure Cross-border Payments

The inputs from technical partners and Deliverable D7.7 "Transactive Energy Module" indicate that TwinEV Module and Transactive Energy Module allows users to conduct transactions for services and products through smart contracts and to earn and spend TwinERGY token as fiat currency. The inputs reveals that the scope of the transactions occurred on the TwinERGY digital modules are limited with electricity and a few pre-identified rewards and the role of Transactive Energy Module is more like online marketplace in terms of payments. Therefore, it could be concluded that the PSD II is not of direct relevance for the TwinERGY framework at the current stage of the digital modules.

2.2.3 Key Takeaways

Transparency and fairness are among the main guiding principles of the European data protection framework and the TwinERGY Ethics Framework. Therefore, TwinERGY aims to ensure high level of transparency with respect to its data processing activities and provide fair processing for its participants. In that regard, it is recommended that the TwinERGY pilots make it explicit if their data processing activities include any special categorises of personal data. If it is established that the data processing activities of the pilot include special categories of personal data, the respective partners are suggested to inform the participants whose special categories of personal data processed, about such processing by means of the consent forms and privacy policies and to obtain their explicit consent. These steps may increase the level of transparency and fairness in the data processing activities of the pilots.

To further increase the level of transparency and fairness, the project participants could be notified about the identity of organisations or individuals which have access to and processes the personal data. In that regard, it is important for the pilot leading partners to explicitly identify other partners or third parties processing personal data of the

[40] The inputs to the questionnaire concerning TwinEV Module.

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

participants in the pilots. Once all parties that have access to and process personal data are identified, their respective roles as joint data controller or data processor should also be made explicit to the participants. For instance, there might be technical partners, or third parties processing personal data of the pilot participants to develop and deploy the digital modules or their components in the pilots. It is recommended that the pilot leading partners assess whether these technical partners act as joint controller or data processor and take necessary measures to ensure the compliance of the pilot activities with the GDPR.

Moreover, the creation of prosumers profiles on which decisions concerning the electricity supply are based in the project and the possibility to extend the processing of personal data in a large scale once the TwinERGY framework enters in the market may require the pilots to give special attention to the risks related to their data processing operations. DPIA could be considered as a useful tool for identifying the risks arising from the data processing activities. In that regard, it is thus suggested for the pilot leading partners to carry out a risk assessment with respect to their processing activities. This will allow the pilot leading partners to mitigate potential adverse effects of the processing activities on the participants and to implement proper safeguards for the rights and freedom of the participants. Furthermore, it is also a legal requirement under Article 35 of the GDPR for organisations conducting personal data processing activities which are likely to result in a high risk to the rights and freedoms of natural persons. For this purpose, it would be prudent for the pilot leading partners to evaluate whether their processing operations are likely to result in a high risk in accordance with the EDBP's criteria provided in Appendix-I and then to document their findings and the reasons for not carrying our DPIA. However, even if data processing operations do not trigger this particular legal requirement, carrying out a risk assessment prior to commencing data processing is always recommended. Nevertheless, it should be noted that DPIA is not only a key part of compliance with the GDPR where high risk data processing is planned but also allows organisations to proactively address to safeguard the rights and freedom of individuals.

With respect to the identification of the TwinERGY users and authentication of electricity transactions on the respective digital modules, the technical partners may give particular attention to possible functions that support any EU citizen to access TwinERGY services with national digital identity and without having to use private identification methods or unnecessarily sharing personal data. Moreover, the proposal for the European Digital Identity sets out provisions that will facilitate the digital verification of the identity of EU citizens by businesses and will allow organisations to benefit from trust, security and interoperability provided by the upcoming European Digital Identity framework. Therefore, the compatibility of TwinERGY modules with European Digital Identity

framework, particularly of those modules where the authentication of user identity is crucial for the provision of secure services such as TwinEV Module or Transactive Energy Module could be priority before launching TwinERGY onto the EU market.

Finally, although it is concluded the PSD II is not of direct relevance for the TwinERGY framework at the current stage of the digital modules, it is suggested that the technical partners responsible for digital modules where users can execute online transactions and payment take into account legal consequences of being subject to the PSD II and design the payment functions of the digital modules accordingly. For example, potential cooperation with third party payment service providers to facilitate the settlement of online transactions executed by TwinERGY users could be considered.

2.3 System-Centric Perspective

Digital technologies and digital services have transformed everyday life, how organisations do business and also how governments interact with their citizens. While these technologies have brought substantial benefits in different domains, they have also presented risks. While several regulations have been implemented or proposed to safeguard individuals from damage resulting from the use of such technologies or from misuse thereof by malicious actors, there is also a need for regulations that look at the lifecycle of such technologies. Manufacturers, operators and providers of digital products and services need to move away from the "Sell Now, Fix Later" approach and ensure that different aspects such as privacy, cybersecurity, cyber resilience, transparency and accountability are taken into account right from the design phase of such technologies.

This chapter focuses on proposed and existing EU laws that aim at doing so by ensuring that manufacturers and operators complied with certain standards before placing their technologies on the market and lays down responsibilities that continue even after the technologies have been put in use individuals or organisations. The safety of products on the EU single market and liability of damages caused by defective products in general are regulated in general by the General Product Safety Directive ('GPSD')[41] and Product Liability Directive ('PLD')[42]. Under the deliverable D12.1 "Legal & Ethical Compliance Guide", the scope of these two EU legislations and the legal requirements set out therein have already been discussed. As it was concluded that the PLD and GPSD become

[41] 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.
[42] 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.

applicable to TwinERGY once the TwinERGY solution enters the EU market, the legal assessment of TwinERGY project in terms of these legislations will be carried out under the deliverable of D12.3 "2nd Legal & Ethical Compliance Report" due in October 2023. In addition, this deliverable note that the proposal for an AI Act is still being discussed by the co-legislators, the European Parliament and the Council, and no amendments to the proposal have been officially accepted by either of them. Given that the current version of the proposal is already reviewed in detail in D12.1 and the lead engineers in the project state that there is no AI being used in the project, this deliverable does not further discuss the proposal.

On the other hand, considering the current stage of the project where the pilots start deploying IoT in participants households, integrating the TwinERGY digital modules and thus trialling the TwinERGY concept, this chapter addresses how to ensure the cybersecurity of the IoT. Furthermore, the most recent EU initiative addressing on civil liability rules for AI, the proposed AI Liability Directive[43], and its objectives are briefly discussed. In that regard, the EU laws subject to the legal review in this chapter are highlighted in the table below.

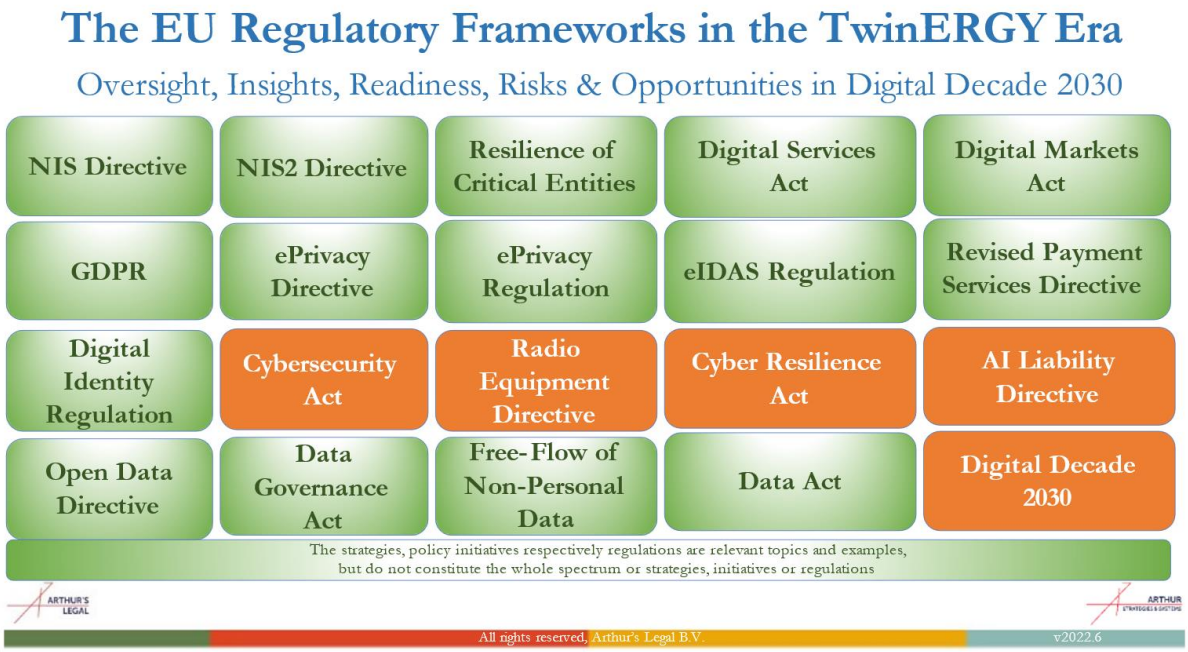

Figure 6: The EU Regulatory Frameworks from a System-Centric Perspective

In accordance with the review of these EU laws as well as the inputs provided by the partners to the questionnaires attached to this deliverable, the state of play in TwinERGY

[43] European Commission, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), 2022/0303. Available at https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en.

pilots is identified in this chapter. Upon a gap analysis, key takeaways are addressed to the relevant partner to assist them in improving the state of play.

2.3.1 The Cybersecurity of Connected Devices

Cybersecurity is an integral part of Europeans' security as the EU's economy, democracy and society depend more than ever on secure and reliable digital tools and connectivity.[44] Improving cybersecurity is therefore essential for building a resilient and secure digital Europe. It enables people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data. Particularly, cybersecurity is indispensable to the connectivity and the global and open Internet that must underpin the transformation of the economy and society.[45] IoT and digital products and services often contain vulnerabilities that can be exploited with potentially widespread ramifications and therefore people's concerns about security are a major disincentive to using them.

Given that connectivity and openness are two of the key elements of TwinERGY project, they can also cause vulnerabilities of the whole TwinERGY framework to cyber threats. As the Internet of Things proliferates and their use by the participant in the pilots increase in the following months, TwinERGY aims at boosting its resilience and cybersecurity capabilities by aligning project activities with the current and upcoming legal requirement at EU level.

The European Cybersecurity Certification Framework

The EU cybersecurity certification framework established under the Cybersecurity Act (CSA)[46] is a critical milestone in increasing trust and security in important digital devices, systems and services for the digital world. At the time of drafting this deliverable, the EU cybersecurity certification framework and the Union rolling work programme which will be published in advance of the cybersecurity certification scheme to allow businesses, government agencies, and standardization bodies to prepare for the future European cybersecurity certification schemes are still under the development by the Commission.

[44] European Commission, Joint Communication to the European Parliament and the Council, the EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN.
[45] Ibid.
[46] 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.

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

However, for the sake of developing future-proof solution, it is important for the TwinERGY partners to familiarise with the EU cybersecurity certification framework.

The four (4) objectives and three (3) assurance levels – basic, substantial and high – set out under the cybersecurity certification schemes have already been explained in D12.1 "Legal & Ethical Compliance Guide". Therefore, this section elaborates further on the conformity self-assessment and the supplementary information requirements for certified digital devices, systems and services. The CSA allows the manufacturer or provider of digital devices, systems and services, that present a low cybersecurity risk corresponding to assurance level 'basic', to carry out a self-assessment of the compliance of their products and services with the relevant European cybersecurity certification schemes developed under the common certification framework, and to issue an EU statement of conformity stating that such compliance.[47] However, by issuing such a statement, the manufacturer or provider become responsible for the compliance of their digital devices, systems and services with the requirements set out in that such scheme. In addition to the conformity self-assessment, the CSA also regulates additional obligation for the manufacturers and providers to provide supplementary information for their certified digital devices, systems and services to the public.

Furthermore, the CSA aims to help end users to make informed choices with these European cybersecurity certificates and EU statements of conformity. Therefore, under Art. 55 of the CSA, the manufacturers and providers of certified digital devices, systems and services are required to make publicly available the following supplementary information regarding their products: i) guidance and recommendations to help end users install, apply and maintain their products or services; ii) the duration they offer security support; iii) their contact details and iv) references to online repositories with information on known cybersecurity issues affecting their products or services.[48] Such information should also be provided in a structured format and adapted to the expected technical level of the intended end user.[49] Moreover, information should be available online, and, where appropriate, in physical form.

The Cybersecurity Requirements for Wireless Devices

Article 3(3)(d),(e) and (f) of the Radio Equipment Directive sets out the essential requirements that certain categories of radio equipment shall comply with in order to ensure i) protection of communication network, ii) safeguards to ensure that the

[47] Cybersecurity Act, Article 53.
[48] Cybersecurity Act Article 55, Recital 93.
[49] Ibid.

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

personal data and privacy of the user and of the subscriber, and iii) protection from fraud respectively.[50] The manufacturers are legally obliged to perform conformity assessment to prove that the radio equipment meets these requirements before it is placed on the market. In the Commission Delegated Regulation published on 29 October 2021, the categories or classes of radio equipment are concerned by each of these requirements are defined.[51] According to this Regulation, any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment, is capable of processing personal data, traffic data or location data, e.g. smartphones, tablets, smart plugs, wearables and other internet of things, wearables, must comply with essential requirements under Article 3(3)(d) and (e).[52] In other words, these devices must incorporate safeguards to protect the personal data and privacy of the user and of the subscriber and their use or misuse should not harm the communication network. In case internet-connected radio equipment enables its holder or user to transfer money, monetary value or virtual currency, the manufacturer of such devices must also ensure that the device provides protection from fraud. However, motor vehicles, their systems and components are exempt from the requirements regarding the protection of personal data and protection against fraud. The delegated act is currently in force, and compliance with the essential requirements become mandatory on 1 August 2024.

These essential requirements are deemed necessary for ensuring an adequate level of cybersecurity, personal data protection and privacy. The manufacturers will have the possibility to choose the specific technical solutions for the implementation of these objectives. In that regard, a harmonised standards describing specific technical solutions will be developed by the European Standardisation Organisations. The manufacturers will be allowed to perform a self-assessment when their product has been designed in accordance with harmonised standards or rely on a third-party assessment performed by an independent inspection body, regardless of whether or not a harmonised standard was used.[53]

The Proposal for a Cyber Resilience Act

In February 2022, the Commission started the Cyber Resilience Act initiative aiming to address market needs and protect consumers from insecure digital products or services

[50] 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.
[51] European Commission, Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive, C/2021/7672. available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.007.01.0006.01.ENG.
[52] Ibid, Article 2.
[53] Radio Equipment Directive, Articles 17 and 18.

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

by introducing common horizontally applicable cybersecurity rules for manufacturers and vendors of a wide range of tangible and intangible digital products and ancillary services.[54] The Commission noted that the existing framework does not cover all types of digital products, in particular, the Radio Equipment Directive fails to cover a variety of widely used hardware or non-embedded software products are not addressed in the current framework, even though vulnerabilities in software products are increasingly serving as a channel for cybersecurity attacks, causing significant societal and economic costs. Therefore, the Commission wishes to extend cybersecurity requirements to other digital products (wired) and non-embedded software, and their whole life cycle.

The Commission published the proposal for a regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 ('CRA') on 15 September 2022.[55] The CRA introduces comprehensive mandatory cybersecurity requirements for products that have digital elements, including IoT, to be placed on the internal market, with requirements applying throughout their lifecycle.[56] This means that manufacturers may need to provide ongoing security support and updates to patch emerging vulnerabilities. It that regard, the requirements mainly address two issues: one is the low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and more importantly, the insufficient and inconsistent provision of security updates provided by their manufacturers to address them and second is the insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner. The products with digital elements covered by this regulation include any software or hardware product whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.[57] However, as the regulation set out lays down horizontal cybersecurity rules which are not specific to sectors, product with digital elements fall under scopes of sector- or product-specific EU regulations such as motor vehicles, aircrafts, medical and vitro diagnostic devices are not covered.[58]
The CRA introduce obligations of hardware manufacturers, software developers, distributors, and importers to comply with cybersecurity requirements.[59] The

[54] European Commission, Call for Evidence for an Impact Assessment, (2022)1955751, 17/03/2022. Available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en.
[55] European Commission, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 COM 2022/0272, (Cyber Resilience Act) Available at https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.
[56] Cyber Resilience Act, Recital 2.
[57] Cyber Resilience Act, Articles 2 and 3(1).
[58] Cyber Resilience Act. Article 2(2).
[59] Cyber Resilience Act, Articles 10-17.

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

requirements are proposed the CRA include, among others: an 'appropriate' level of cybersecurity including providing security updates five (5) years from the placing of the product on the market, the prohibition to sell products with any known vulnerability, security by default configuration, protection from unauthorised access, limitation of attack surfaces, and minimisation of incident impact and performing conformity assessment to determine whether the product meets the cybersecurity requirements.[60] Furthermore, manufacturers and importers are required to provide certain information and instruction set out in Annex II to the users together with the product including information related to the intended use and essential functionalities of the product, any known or foreseeable circumstance that may lead to cybersecurity risks, the software bill of materials, how changes to the product can affect the security of data and the secure decommissioning of the product, including information on how user data can be securely removed.[61]

Based on the core functionality of products, the CRA also list critical products in two categories under Annex III which are subject to stricter conformity assessment procedures. Because it is noted that a potential cyber incident involving the products with certain core functionality may lead to greater negative impacts than an incident involving other products, for instance considering the nature of their cybersecurity-related function or intended use in sensitive environments.[62] The first category includes web browsers, password managers, antiviruses, firewalls, virtual private networks ('VPNs'), network management, systems, physical network interfaces, routers, and chips used for entities falling under the NIS2 Directive. Moreover, it also includes industrial IoT that are not intended to use by essential entities as defined under the NIS2 Directive. The second category includes higher-risk products such as operating systems for servers, desktops and mobile devices, virtualised operating systems, digital certificate and digital wallet issuers, general purpose microprocessors, card readers, robotic sensors, smart meters, industrial automation and control systems and all IoT, routers and firewalls for industrial use. The main difference between the two categories is the compliance process.

Lastly, Member States would also have to put in place conformity assessment bodies authorised to carry out conformity assessments and market surveillance bodies which foresee the effective implementation of the cybersecurity requirements.[63] The penalties for non-complying with the requirements can amount to EUR-15 million or 2.5% of the annual turnover, whichever is higher.[64]

[60] Cyber Resilience Act, Article 24, Annex I.
[61] Cyber Resilience Act, Annex II.
[62] Cyber Resilience Act, Recital 26.
[63] Cyber Resilience Act, Articles 26 and 41.
[64] Cyber Resilience Act, Article 53.

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

2.3.2 The Proposal for An AI Liability Directive

As a package of measures to support the roll-out of AI in Europe by fostering excellence and trust in AI and to complement the EU product liability framework, the European Parliament adopted a legislative own-initiative resolution of October 2020 and of May 2022 on civil liability for AI, and requested the Commission to propose legislation.[65] The overarching objective is to adapt the EU civil liability framework to take account of developments linked to the move towards a circular and digital economy on liability for damage caused by new and refurbished products. On 28 September 2022, the Commission published the proposal for an AI Liability Directive to address the legal challenges arising from the specific characteristics of AI, particularly its autonomous actions and opacity, which make it difficult or excessively expensive to identify the liable person and prove the causation for a successful liability claim.[66]

The proposal lays down uniform rules for certain aspects of non-contractual civil liability for damage caused with the involvement of AI systems including giving courts power to order providers of high-risk AI systems to disclose relevant and necessary evidence about their systems to persons who seek this information to initiate redress proceedings against the provider. Moreover, it sets out a number of circumstances in which a court may presume rebuttable causality between the fault of the provider or user of any AI system, and the output produced by the AI system or its failure to produce such an output. Together with the proposed product liability rules under the revised Product Liability Directive[67] which puts software and AI systems under its scope, the new liability framework ensures the victims of damage caused by AI systems obtain equivalent protection to victims of damage caused by other products in general. It is also expected that these new rules will reduce legal uncertainty of businesses developing or using AI regarding their possible exposure to liability and prevents the emergence of fragmented AI-specific adaptations of national civil liability rules.

[65] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL); European Parliament resolution of 3 May 2022 on artificial intelligence in a digital age (2020/2266(INI).

[66] European Commission, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), 2022/0303. Available at https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en.

[67] European Commission, Proposal for a Directive of the European Parliament and of the Council on on liability for defective products, 2022/0302. Available at https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en.

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

2.3.3 The State of Play in TwinERGY

Upon reviewing the inputs to the questionnaires, it is noted that the TwinERGY framework builds on various digital devices and products including IoTs and sensors installed in houses and local electricity infrastructure, and digital modules mainly used for transmission, storing, retrieving or processing of information collected by these devices. Considering the definitions of ICT product and ICT service set out under Art 2 of CSA, the TwinERGY framework and its digital modules are likely to fall under the scope of these definitions and therefore become subject to European cybersecurity certification schemes.

At pilot level, the IoTs and sensors forming essential part of the TwinERGY framework are off the shelf products and thus, the partners' capacity, as a user, to assure the cybersecurity level of these products might be limited. In addition, the dependencies on third-party products could pose additional cybersecurity risks as vulnerabilities found in third-party components could be exploited as attack vector to affect the security of the overall TwinERGY framework. At the current phase of the project, it seems that TwinERGY partners rely on the assurance and guarantees provided by third-party vendor with respect to the level of cybersecurity of the IoTs deployed in the project.

Furthermore, the digital modules developed by the TwinERGY consortium play crucial roles in the provision of digital service by the TwinERGY framework, it is very important to ensure an appropriate level of cybersecurity in these digital products. In that regard, the technical partners responsible for the development of digital modules implemented safeguards to keep data collected from participants in core data management platform which is the central repository for the whole project hosted within the TwinERGY project, i.e, at the local server of the project partner ETRA, and not by a third-party service provider.[68] Data Security Service implemented within the TwinERGY Core Data Management Platform includes various functionalities such as the Access Policies Controller and the Data Anonymization Handler to address users' data security and privacy concerns regarding data that will be processed. Detail information on data security measures and its functions can be found in Deliverable D5.3 'TwinERGY Integrated Data Management Platform – Alpha, Mockups Release'.

Furthermore, the TwinERGY interoperability platform builts on Neural Autonomic Transport System (NATS) to facilitate communication between different digital modules which uses Transport Layer Security (TLS) semantics to encrypt clients, route ad monitor

[68] TwinERGY, Deliverable D5.2 Data Collection, Security, Storage & Management Services Bundles – Beta Release, December 2021; The inputs to the questionnaire concerning TwinENRGY Consumer Wellbeing Platform; The inputs to the questionnaire concerning TwinENRGY Interoperability Platform.

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

connections. NATS is configured to force client authentication by its connection via password, token, NKEYs and credential files and it adopts secure communications that do not interfere with the security and processing of personal data of the subjects.[69] Last but not least, it is noted that the TwinEV module implemented Keycloak, identity and access management solution, to act as a single sign-on (SSO) method in order to reinforce the control of the users. It acts as a redirector for the user's credentials. The personal data such as username, address, email and other profile data is not exchanged as it is first cryptographically signed before the exchange between TwinEV Module and the interoperability platform.[70]

2.3.4 Key Takeaways

Under the EU Cybersecurity Strategy[71], it is expected from organisations, manufacturers or providers involved in the design and development of digital devices, systems and services to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised before entering in the market, namely security by design. In line with the legal requirements stipulated under the CSA, Radio Equipment Directive and the proposal for the CRA, cybersecurity should be ensured throughout the lifetime of digital devices, systems and services by design and development processes that constantly evolve to mitigate the risk of harm from malicious exploitation. In that regard, it could be beneficial for the consortium partners to take into account that cybersecurity as not only an issue related to technology, but one where human behaviour is equally important. Therefore, cybersecurity strategies composed of simple and routine measures that, where implemented and carried out regularly by consumers, organisations and businesses, could minimise exposure to cyber threats.

In the grand scheme of things, identifying and documenting dependencies on third-party components and services such as IoTs and cloud service could form the initial steps for creating a solid cybersecurity strategy. This would allow, for example, organizations to develop incident remediation procedures to address potential vulnerabilities posed by third party vendors. It should also be noted that open-source software might cause some cybersecurity vulnerabilities in the overall system. As open-source software is publicly available, malicious actors can also access the code to look for vulnerabilities. Furthermore, since it is developed and frequently updated in a distributed way by dozens

[69] The inputs to the questionnaire concerning TwinENRGY Interoperability Platform.
[70] The inputs to the questionnaire concerning TwinENRGY TwinEV Module.
[71] The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication, 'The EU's Cybersecurity Strategy for the Digital Decade', JOIN(2020).

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

or hundreds of people, it could be very difficult to keep track of security vulnerabilities identified by other community users. Lastly, carrying out a comprehensive security auditing might be very challenging as well. Therefore, the partners are invited to give particular attention to these cybersecurity vulnerabilities and employ cybersecurity strategy.

Moreover, although European cybersecurity certification under the CSA is still voluntary and there is not any EU-wide certification scheme in force at the time of drafting this deliverable, it will be certainly beneficial, in the future, to obtain certification under the CSA in the event that the TwinERGY solution enters the market. This is 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 important 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 Member States may assess and determine products, services and processes covered under a national certification scheme which should be covered by a mandatory certification scheme. Furthermore, given that the compliance with the essential security requirements for wireless devices stipulated under the Commission Delegated Regulation in line with the Radio Equipment Directive becomes mandatory in August 2024, if the TwinERGY project opt for manufacturing any wireless devices that can communicate itself over the Internet and is capable of processing personal data, it is advised to design such device in a way that it incorporates safeguards against digital frauds and cyberthreats to users' privacy.

2.4 Data-Centric Perspective

Data plays an essential role in economic growth, innovation, competitiveness and creating benefits for society as a whole. Keeping that in mind, the EU has taken great strides to ensure that public agencies, private organisations and individuals are able to leverage the potential of data in a sustainable and holistic manner. Several European leaders have also reiterated the need to ensure that European data is used for European countries in order to create value in Europe. In February 2020, the EU also published its communication on "A European Strategy for Data" which aims at making the EU a leader in a data-driven society. The Strategy is expected to create a single market for data where data slows across the various sectors in the EU and where the rules for access and use of data are fair, practical and clear. More relevant for TwinERGY is the proposal under the Strategy to create a Common European energy data space so as to promote a stronger availability and cross-sector sharing of data, in a customer-centric, secure and trustworthy manner, as this would facilitate innovative solutions and support the

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

decarbonisation of the energy system.[72] As per the Strategy, a common energy data space based on existing approaches towards data sharing could facilitates the interoperability in smart buildings and connected devices, with a view to improve their energy efficiency, optimise local consumption and broaden the integration of renewable energy sources.[73]

In line with the objectives of the European strategy for a common energy data space, this chapter provides focus on data sharing between public body and private entity as well as between two private entities in TwinERGY. Therefore, this chapter starts with outlining legal requirements in the EU regulatory framework regarding access to non-personal data held by public entities and interoperability of digital services and products are reviewed. In accordance with this review and the inputs provided by the partners to the questionnaires attached to this deliverable, the state of play in TwinERGY project is identified and upon a legal assessment, key takeaways are addressed to the relevant partner to assist them in improving the state of play.

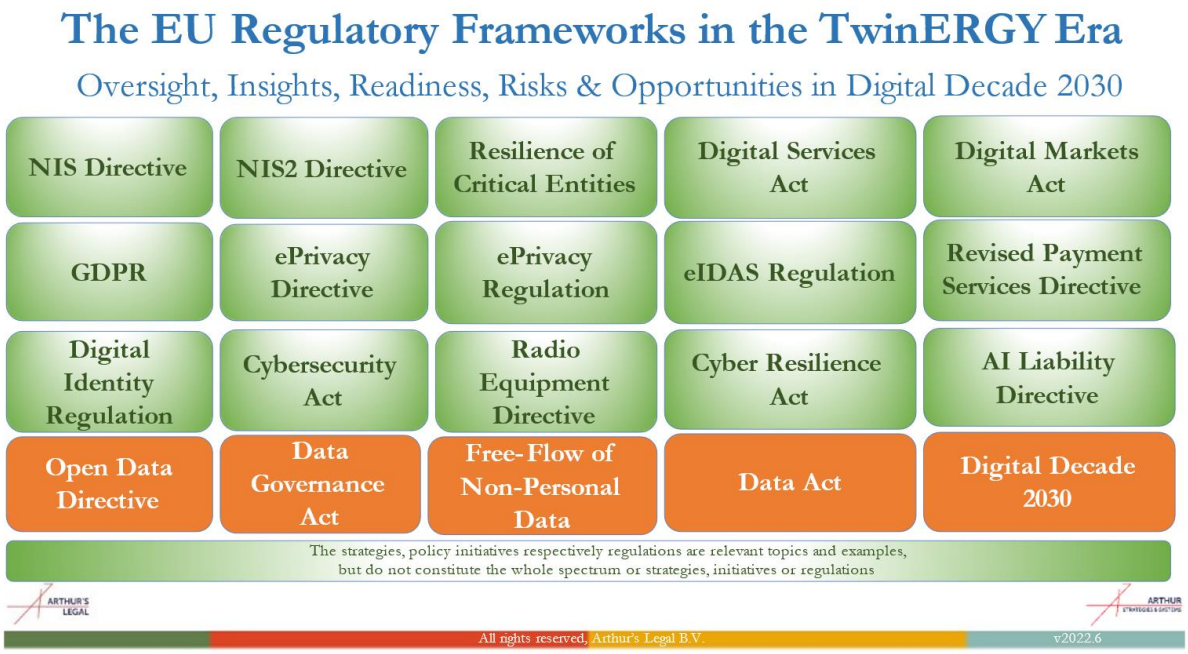

Figure 7: The EU Regulatory Frameworks from a Data-Centric Perspective

2.4.1 Opening Up Public Datasets

In support of the vision for a competitive European Digital Single market and to foster European digital sovereignty, the EU aims at facilitating the re-use of data held by public

[72] European Commission (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a European strategy for data. Available at: https://digital-strategy.ec.europa.eu/en/policies/strategy-data.
[73] Ibid.

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

sector bodies, for commercial and non-commercial purposes. In that regard, the rules contained in the Open Data Directive and the Data Governance Act, regulating access and re-use of public sector information, constitute fundamental pillars of the legal framework for the common European energy data space.

Open Data Directive

The Open Data Directive (ODD)[74], entered into force on 16 July 2019, focuses on making available for re-use documentation held by public sector bodies and undertakings. In the ODD, documentation that should be made available concerns "any content whatever its medium in paper or electronic form or a sound, visual or audiovisual recording, as well as any part of such content."[75] To facilitate re-use of public sector data, public-sector bodies and public undertakings are required to make their documents available in any pre-existing format or language and, where appropriate, by electronic means in formats that are open, machine readable, accessible, findable and reusable, complete with their metadata[76]

Public sector bodies and public undertakings

It should be noted that, by taking the legal form of a directive, the ODD is addressed to the Member States, which have implemented these provisions in their own legal systems.[77]. Therefore, in order to determine the exact applicability of these rules, the national rules implementing the ODD should be consulted. Nevertheless, it can be said, in principle, that the ODD requires European public sector bodies and public undertakings to make publicly funded data reusable for commercial or non-commercial purposes with fair, proportionate, and non-discriminatory conditions. The identification of the public sector bodies and public undertakings subject to the ODD should follow the criteria enlisted in Article 2(1) and (3). **Public sector body** means the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities or one or more such bodies governed by public law. **Public undertaking** includes entities operating in the water, energy, transport and postal services sectors over which the public sector bodies may exercise directly or indirectly a dominant influence by

[74] Directive (EU) 2019/1024 Of The European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information ("Open Data Directive").
[75] Open Data Directive, Article 2(6). As this Directive encourages Member States to go beyond the minimum requirements set therein and ensures the validity of higher standards already in place, pursuant to Recital (30), 'Member States may extend the application of this Directive to computer programmes'.
[76] Open Data Directive, Recital (34) and Recital (35): "A document should be considered to be in a machine-readable format if it is in a file format that is structured in such a way that software applications can easily identify, recognise and extract specific data from it.".
[77] An overview of the national implementation of this Directive is available on the EUR-Lex website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32019L1024

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

virtue of their ownership of it, their financial participation therein, or the rules which govern it.

Open by design and open by default

Article 5(2) ODD adopts the principle of open by design and by default. This principle requires public bodies and public undertakings to make their datasets available as "open data" in a pre-existing format or language. Additionally, where appropriate and possible, this data must be provided by electronic means in formats that are open, machine-readable, accessible, findable, and reusable, complete with their metadata for re-use by default at first instance. However, this requirement does not entail an obligation for public sector bodies to create and produce an extract from their datasets or modify the requested information format should it involve a disproportionate effort beyond a simple operation. Once open data is created, public sector bodies are also required to make necessary arrangements to facilitate the online search and discovery. The re-use of open data should be, in principle, free of charge. Moreover, the ODD prohibits public sector bodies or public undertakings holding the datasets from granting third parties exclusive access rights to their datasets.[78] In consideration of the activities carried out in the TwinERGY project, special emphasis needs to be given the following three categories of publicly held data: dynamic data, research data and high value data.

Dynamic data

This type of data refers to data whose economic value depends on the immediate availability of the information and regular updates because of their volatility, such as environmental, traffic, satellite, meteorological, and other sensor-generated data. Article 5 of the ODD requires that public sector bodies make their dynamic data available for re-use immediately on collection via an application programming interface (API). Furthermore, where relevant, such data should be available as a bulk download to facilitate the development of internet, mobile, and cloud applications based on such data.

Research data

This category contains all the data collected or produced in scientific research activities and is used as evidence in the research process or is commonly accepted in the research community. According to Article 10 ODD, Member States are obliged to adopt *open access policies* to provide researchers and the public access to research data as early as possible in the dissemination process and facilitate its use and re-use in line with the FAIR principles.[79] According to these *open-access policies*, once the research data is made

[78] 'Exclusive agreements' are regulated under Article 12 ODD and analysed more in details in the context of the Data Governance Act, which provides additional rules on the matter.

[79] The FAIR principles contain four principles for data, i.e. Findability, Accessibility, Interoperability, and Reuse of data. The principles emphasise the capacity of computational systems to find, access, interoperate, and

publicly available through an institutional or subject-based repository, its re-use must be available to everyone in the market, and any applicable re-use conditions should be objective, proportionate and non-discriminatory. As per Article 14 ODD, if the research data contains sensitive content such as personal data, trade secrets, and intellectual property rights of third parties, its re-use becomes subject to the principle "as open as possible, as closed as necessary."

High Value Data

Finally, the ODD acknowledges that certain data types are more valuable than others. The re-use of which offers significant benefits for society, the environment, and the economy. Therefore, the directive defines lists of six (6) thematic categories of high-value datasets in Annex I, namely: (1) geospatial data such as postcodes, national and local maps, (2) data on earth observation and environment, (3) meteorological data, (4) statistics, (5) data on companies and company ownership and (6) mobility data. Public sector bodies and public undertakings must make their data belonging to these thematic categories available in machine-readable formats and free of charge through APIs.

Area of exclusion from re-use

Article 1(2) ODD excludes the possibility of re-use for certain types of documents such as in cases for which third parties hold intellectual property rights, or access of which is excluded or restricted on the grounds of sensitive critical infrastructure protection, national security, statistical or commercial confidentiality or protection of personal data and privacy. Some of these exclusions have been amended by the Data Governance Act, as well as the possibility for exclusivity for re-use agreements. These provisions are outlined more in details below.

Data Governance Act

Since 23 June 2022, the Data Governance Act (DGA) is in effect and it becomes directly applicable in all member states as of 24 September 2023.[80] The DGA is a cross-sectoral instrument that aims to make more data available by regulating the re-use of publicly held, protected data, by boosting data sharing through the regulation of novel data intermediaries and by encouraging the sharing of data for altruistic purposes.

reuse data with none or minimal human intervention because humans increasingly rely on computational support to deal with data as a result of the increase in volume, complexity, and creation speed of data.

[80] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868.

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

In terms of the re-use of publicly held data, the DGA extends the scope of the legal framework for the re-use of data held by public sector bodies, for commercial or non-commercial purposes, already established under the ODD.[81] Specifically, four (4) categories of data that were previously exempted from the open data requirement, namely "commercially confidential data", "statistically confidential data", "the data protected by intellectual property rights of third parties" and "personal data" are conditionally available for re-use.[82] The conditions for re-use are outlined in Article 5 DGA, and primarily mandate Member States to make publicly available the conditions for allowing the re-use of one or more of these four (4) categories of data and the procedure to request it.[83] Moreover, the DGA requires that the conditions set for re-use and the procedure thereof must be non-discriminatory, transparent, proportionate, objective.[84] On the other hand, such categories of data held by public undertakings, over which the public sector bodies exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it, are exempted from the scope of the conditions for the re-use of such data.[85]

The DGA provides that in order to preserve the rights of third parties, Member States may provide, as conditions for the re-use of the data, that they are (i) anonymised, in the case of personal data or (ii) modified, aggregated or treated by any other method of disclosure control, in the case of commercially confidential information, including trade secrets or content protected by intellectual property rights. Other conditions suggested are that access is offered in a secure online environment or within the physical premises under controlled conditions,[86] as well as that confidentiality agreements are used.

Prohibition of exclusive arrangements

In coherence with the principle envisaged in Article 12(1) ODD, the DGA extends the prohibition of agreements and other practices that grant exclusive rights or that restrict the availability for re-use of data protected on the ground of commercial and statistical confidentiality, IP or personal data protection.[87] Derogations to this principle are envisaged both in the ODD and DGA. Specifically, the DGA mentions the possibility to grant an exclusivity to obtain a service or a product, which would not be possible to obtain otherwise, and this agreement should take the form of an administrative act or contractual arrangement, and be in compliance with the principles of transparency, equal

[81] Public undertakings are outside the scope of these provisions, Article 3(2) DGA.
[82] Data Governance Act, Article 3(1).
[83] Data Governance Act, Article 5(1).
[84] Data Governance Act, Article 5(2).
[85] Data Governance Act, Article 3(2).
[86] Data Governance Act, Article 5(3).
[87] Data Governance Act, Article 4(1).

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

treatment and non-discrimination. In any case, the duration of an exclusive right to re-use data shall not exceed 12 months, except for the cases envisaged in the ODD.[88]

Data Intermediation Services

Another breakthrough in the DGA is introduction of data intermediation services that provide pure facilitation of data sharing between the data users and an undetermined number of data subjects and data holders on other hand to establish bilateral or multilateral exchanges of data sharing for the establishment of commercial relationships. The concept of "data intermediary service" is limited to pure facilitation of data sharing and thus providers who enrich data or otherwise add value to it are not included. Providers who intermediate copyright protected content; closed group arrangements; and arrangements by a single data holder to allow exploitation of its own data; cloud service providers are all excluded, as are intermediation services provided by public sector bodies without "aiming to establish commercial relationships for purpose of data sharing".

Conditions for providing data sharing services are also set forth under the DGA which aims at ensuring the neutrality and independence in data sharing in the EU, i.e. data-as-a-neutral-service. Accordingly, the data intermediaries are obliged to notify the relevant competent authority and must ensure their compliance with certain conditions set forth under the Act before initiating their services. These conditions include, among other, employing procedures to prevent fraudulent or unfair practices concerning access and use of data sharing services and taking adequate technical, organisational and legal measures to prevent transfer or access to non-personal data that is unlawful.

2.4.2 Interoperability of Connected Devices and Digital Services

One of the obstacles before realising common European data spaces 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. In 2018, the GDPR has provided for general access and portability rights to avoid this from happening with regards to personal data. Under Art 20 of the GDPR, the data subject has the right to receive their personal data held by a controller and transmit it to another controller, or to have the data transmitted – where technically feasible – directly from one controller to another. This might include data generated by connected products and related services. With regards to non-personal data however, the Regulation on the Free Flow of Non-

[88] Similar derogation provisions, for more specific cases, such as digitisation of cultural resources, are envisaged also in Article 12 ODD.

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

Personal Data ('FFoD')[89] and the proposal for a regulation on harmonised rules on fair access to and use of data[90] promotes interoperability of the data. In particularly, both laws include legal requirements aiming to facilitate sharing and use of privately-held data by other companies.

The Regulation on the Free Flow of Non-personal Data

The FFoD addresses the problem of 'vendor lock-in' at the level of providers of data processing services, by introducing self-regulatory codes of conduct to facilitate switching data between cloud services.[91] The Commission has started facilitating self-regulation in this area, and formed the working group on switching cloud providers and porting data ('SWIPO') in order to develop voluntary codes of conduct regarding the conditions under which users can move data between cloud service providers and back into their own IT environments as defined in Art 6 of the FFoD. The objective of SWIPO is to reduce the risk of 'vendor lock-in', as it will be easier to switch providers when it is clear which processes, technical requirements, timeframes and charges apply in case a professional user wants to switch to another provider or port data back to its own IT systems. For this purpose, the working group has produced two codes of conduct, one for Infrastructure-as-a-Service ('IaaS') cloud services and another for Software-as-a-Service ('SaaS') cloud services in May 2020.[92] However, SWIPO codes of conducts are largely limited to an approach of pre-contractual transparency, instead of addressing also technical and economic hurdles as required by the FFoD. SWIPO codes also fail to set out certain specific commitments that are directly aligned with the objective such as formats to be followed by cloud service providers for data, exporting/importing, rules around determining charges and costs associated with porting and timescales for data porting. Instead, they provide a wide margin of discretion for the cloud service provider to determine its own standards, procedures and processes on key issues relating to switching and porting such as technical capabilities, contractual terms, associated costs. Furthermore, only a very small number of providers have signed for these codes since 2020. As a result, the Commission concluded that the self-regulatory approach seems not to have affected market dynamics significantly and presented the proposal for data act as a regulatory approach to the vendor lock-in issue.

[89] 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.

[90] European Commission, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN.

[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.

[92] SWIPO Codes of Conducts can be found at https://swipo.eu/download-section/copyrighted-downloads/.

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

The Proposal for Data Act

On 23 February 2022, the Commission published the proposal for the Data Act.[93] With this, the Commission aims to ensure fairness in allocating value from non-personal data among actors in different sectors of the data economy. Specifically, this proposed legislation fosters data sharing with users of digital products (IoT devices) and third parties' competitors. Furthermore, it provides for switching provisions and provisions regarding the interoperability of products and systems. In consideration of TwinERGY's stage of development of design and implementation, it seems appropriate consider the upcoming provisions regarding interoperability.

The proposed Data Act requires that an effective level of interoperability among digital systems be achieved. In Article 2(19), interoperability is defined as "*the ability of two or more data spaces or communication networks, systems, products, applications or components to exchange and use data to perform their functions*." Simply put, interoperability can be understood as a characteristic of a product or system to work with other products or systems. The term is coined by the digital industry to define an ideal way for computers and other electronic devices to relate.

Accordingly, certain specific obligations for operators of data spaces are provided. Pursuant to the proposed Article 28 Data Act, operators of data spaces shall comply with the following essential requirements to facilitate interoperability of data, data sharing mechanisms, and services:

> (a) the dataset content, use restrictions, licenses, data collection methodology, data quality, and uncertainty shall be sufficiently described to allow the recipient to find, access, and use the data;
> (b) the data structures, data formats, vocabularies, classification schemes, taxonomies, and code lists shall be described in a publicly available and consistent manner;
> (c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format;
> (d) the means to enable the interoperability of smart contracts within their services and activities shall be provided.

[93] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final, Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN.

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

These requirements can have a generic nature or concern specific sectors, while taking fully into account the interrelation with requirements coming from other Union or national sectoral legislation. Pursuant to the proposed Article 29(1) Data Act, open interoperability specifications and European standards for the interoperability of data processing services shall:

> (a) be performance oriented towards achieving interoperability between different data processing services that cover the same service type;
> (b) enhance portability of digital assets between different data processing services that cover the same service type;
> (c) guarantee, where technically feasible, functional equivalence between different data processing services that cover the same service type.

Furthermore, pursuant to the proposed Article 29(2) Data Act, open interoperability specifications and European standards for the interoperability of data processing services shall address:

> (a) the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability;
> (b) the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability;
> (c) the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability, and application policy portability.

The concept of interoperability is not new to the public sector. The Interoperable Europe Initiative aims to introduce a cooperative interoperability policy for a modernised public sector. The Initiative arose out of the ISA2, a Union funding programme that ran from 2016 to 2021 and supported the development of digital solutions to enable interoperable cross-border and cross-sector public services. In the context of TwinERGY, observing the interoperability requirements mentioned in the Data Act might favour the creation of products that are “future-proof” and useful beyond the duration of this project and for both commercial and non-commercial actors, that are not immediately involved in the project.

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

2.4.3 The State of Play in TwinERGY

Re-use of Public Sector Data

The assessment of the state of play in TwinERGY in terms of legal requirements set out under the ODD and the DGA should begin with the determining whether any public or publicly funded data is being used in the project. As per Art 2 of the ODD, public-sector body is defined as the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities or one or more such bodies governed by public law. Based on this definition, the EU municipalities involved in the TwinERGY pilots are, in principle subject to the provisions of the ODD, and are likely required to make their data generated within the scope of their public tasks, available as "open data" in a pre-existing format or language and complete with their metadata. In addition to the municipalities, depending on the national provisions, Mytilineos might be considered as public undertaking defined by the ODD as entities operating in the water, energy, transport and postal services sectors over which the public sector bodies may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it. In this case, the dynamic data generated in the TwinERGY pilots might be required to be available to third parties. However, the respective pilot leading partners should note that certain sensitive data related to electricity infrastructure in the respective pilot regions are exempted from the open data requirements pursuant to Art 1(2)e ODD.

Considering that the TwinERGY is funded by the European Commission, it is likely that data generated by the TwinERGY project will be qualified as research data and thus become openly available following the principle of 'open by default' and compatible with the FAIR principles. TwinERGY Grant Agreement has already stipulated provisions regulating the reuse of the project outcomes. In this regard, the TwinERGY interoperability platform provides necessary digital infrastructure and API for facilitating the re-use of research data as well as of the publicly held data. In any case, considering that the ODD is a directive and addressed to the Member States, which have implemented these provisions in their own legal systems, the pilot leading partners are subject to the open data requirements stipulated under the relevant national legislations.

Furthermore, once the DGA becomes applicable, the EU municipalities involved in TwinERGY might be required to allow, under certain conditions, third parties to re-use their data that were previously exempted from the open data requirement under the ODD, namely "commercially confidential data", "statistically confidential data", "the data protected by intellectual property rights of third parties" and "personal data". Given that municipalities have granted the technical partners access for re-use of their datasets containing the "protected data" within the pilots, they might be required to publicize the

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

conditions for allowing re-use of their datasets and the procedure to request such re-use, particularly by third parties in the EU under the DGA. Lastly, assessment of whether any of TwinERGY module qualifies as data intermediary under the DGA will be also carried out in the next deliverable D12.3 "2nd Legal & Ethical Compliance Report" as the project and the service will be at higher maturity level.

Interoperability of TwinERGY Modules

In light of the legislative review carried out above, there are no directly applicable legal requirements on portability and interoperability of non-personal data generated by the use of connected devices and digital modules in TwinERGY at the time of drafting of this deliverable. In terms of personal data, however, Art 20 of the GDPR entitles individuals to receive their personal data in a structured, commonly used and machine-readable format and to port their personal data to another service providers. According to the inputs from the technical partners responsible for digital modules, Home & Tertiary Real-Time Energy Monitoring Module which mainly process personal data collected through sensors, allows the participants to be in control of their data and to export the data in standard formats. Furthermore, other digital modules that process personal data such as Transactive Energy module, Social Network Module and TwinEV Module could also enable portability of personal data.

With respect to the interoperability between the digital modules and IoTs provided by third party vendors, it is noted that Social Network Module, Home & Tertiary Real-Time Energy Monitoring, TwinEV Module and Transactive Energy Module are designed to operate with connected devices including mobiles, sensors, smart plugs, smart meters, PVs and charging stations provided by third parties. These modules can interact with third party IoTs and their ancillary applications through standard APIs and SAREF and thus there is a high level of compatibility in the project. Furthermore, TwinEV Module, which is composed of three different applications, i.e., TwinEV Drivers App, TwinEV Grid Operators app and TwinEV Dashboard facilitate the interconnection and the interoperability with third-party services such as the third-party charging station operators. In this way, the TwinERGY framework successfully prevent vendor lock-in risks and gives its end users freedom to use third party devices that comply with standards APIs in the future.

2.4.4 Key Takeaways

The EU Data Strategy aims to empower individuals with respect to their data through tools and means and enable them to decide at a granular level about what is done with their data. The Commission's proposal for a Data Act is prepared in line with this purpose and as explained above, it will give individuals more control over who can access and use

machine-generated data, for example through stricter requirements on interfaces for real-time data access and making machine-readable formats compulsory for data from certain products and services, e.g. data coming from smart home appliances or wearables.[94] In order to be future proof, TwinERGY modules could benefit from design that enables portability of personal and non-personal data from their platforms to third party platforms and servers by end-users. Furthermore, as the Data Act aims to enable business to business data sharing under certain circumstances, TwinERGY interoperability platform might, to some extent, be configured in a way that facilitates secure interconnection between TwinERGY modules and third part digital services in the future. Strengthening cross-sectoral interoperability and data exchange between TwinERGY modules and third-party services related to electricity market, in line with the European Commission's action plan for Digitalising the energy system,[95] could facilitate market-uptake of TwinERGY across the EU and ensure its readiness -for the future Common European Energy Data Space.

Regarding the re-use of public sector data, TwinERGY may also benefit from the open data requirements under the ODD for its data harvesting and collections operations. According to the national implementations of the ODD, the technical partners may obtain access to the high value datasets held by respective public sector bodies necessary for the project activities in machine-readable formats and free of charge through APIs. In addition, once the DGA becomes applicable, the TwinERGY partners may have opportunity to access and benefit from "commercially confidential data", "statistically confidential data", "the data protected by intellectual property rights of third parties" and "personal data" held by public sector bodies.

[94] European Commission (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a European strategy for data. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68611.
[95] European Commission (2022), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digitalising the Energy System - EU Action Plan, COM/2022/552, 18 October 2022. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0552&qid=1666369684560.

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

3 TwinERGY Approach to Ethics

As outlined under the Introduction, the implementation of Digital Twin technology in energy management under TwinERGY will have impact on the individuals participating in the project. Digital Twins create energy profiles of individuals, their households and communities through continuous data collection. The energy profiles created by the Digital Twins are utilised on both the household and community levels to make automated decisions based on the predictions, giving a rise to various ethical implications.

Although one of the objectives of the TwinERGY project is to change energy consumption patterns of citizens and communities. Citizens and communities are dependent on electricity supply in order to be able to carry out their day-to-day activities. Therefore, in the creation of local energy communities, active citizen engagement and the democratic process must be safeguarded. Otherwise, there may be a risk that individual autonomy and well-being may be undermined in the attempts to reduce energy consumption.

In light of these ethical concerns, this chapter discusses TwinERGY pilot activities under the five (5) sets of ethical principle identified under Deliverable D12.1 "Legal & Ethical Compliance Guide" and to support the partners leading the TwinERGY pilots in the achieving trustworthy and sustainable digital transformation of energy management in the EU. It should be noted that these principles and the assessments 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 striving towards a trustworthy and sustainable digital transition of the energy sector, the TwinERGY project focuses on the consumption patterns of citizens and communities, through the creation of tools for energy consumers and aggregators and citizen engagement. Therefore, to ensure that the digital transition is trustworthy, efforts must be made to ensure that individual citizens and their respective communities, including their motivations and concerns, have been adequately identified and involved in the design and deployment of the technologies. Moreover, to ensure that trustworthiness is maintained throughout the project, relevant changes throughout the lifecycle of the project must be measurable and any outcomes must be appropriately reflected upon.

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

3.1 Adherence to the Guiding Ethical Principles in TwinERGY

In the previous TwinERGY deliverable D12.1, submitted in July 2021, ethical principles primarily embedded in the technology and principles governing the community, focusing on participation and empowerment were outlined. This section will assess the extent to which the Pilots have adhered to the guiding ethical principles as set out in D12.1.

3.1.1 Making It Work

Making it work does not simply mean putting effort into making technology function. Instead, making it work implies that the design of technologies should be embedded with 'non-functionals'. These non-functionals are principles that take into account potential risks and impacts that may arise in the deployment of technologies. Therefore, including these non-functionals by design is essential in making the technology work.

Accountability

One of the key ethical principles is accountability highlighted in D12.1. In the context of the TwinERGY project, the notion of accountability emerges in energy exchange, data exchange, and human-machine interactions.

In the TwinERGY pilots, community members will consume, generate, store and exchange energy. Therefore, it is crucial that participants have the ability to hold someone accountable in the case where there is a failure to deliver the required amount of electricity, if the insufficient energy is as a result of a circumstances beyond the participant's control.

Based on the input received by the Pilot leaders, all Pilots, data of participants will be continuously collected during the course of the piloting activities. Therefore, it is of utmost importance that there are procedures in place where participants are able to hold the vendor of their smart meter accountable when the data processing activities do not comply with the terms and conditions set out in the contractual agreement. Relevant stakeholders must be made aware of their rights and obligations in relation to data processing and exchange.

In addition, participants of the TwinERGY pilots will also be interacting with machine interfaces. Based on the input received from the Pilot leaders, several workshops, training sessions, and training materials will be provided to the participants of Pilots to ensure

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

that the amount of 'human errors' in the operations of these devices are reduced. The Pilots aim to visit participants multiple times to provide explanation of the technology provided and its use.

Non-Functionals

There are additional values and qualitative attributes that must be embedded into the system in order to ensure ethical soundness and resilient. These attributes, referred to as 'non-functionals', represent an integral part of the functionality of digital systems. These principles include, but are not limited to, trust, security, safety, and privacy. Collectively, these non-functionals assist in risk mitigation and prevent potential system failures.

A holistic risk mapping approach enables the selection of the right principles; allowing the each of the principles to be appropriately balanced against one another. In the TwinERGY project, continuous data exchanges between connected devices and modules subject systems to vulnerabilities. Therefore, it is crucial to that appropriate levels of trust, privacy-preserving and security mechanisms are achieved, among others. Without appropriate risk mitigation measures, the technological systems – devices, networks, and algorithms – may eventually fail, possibly giving rise to unintended consequences.

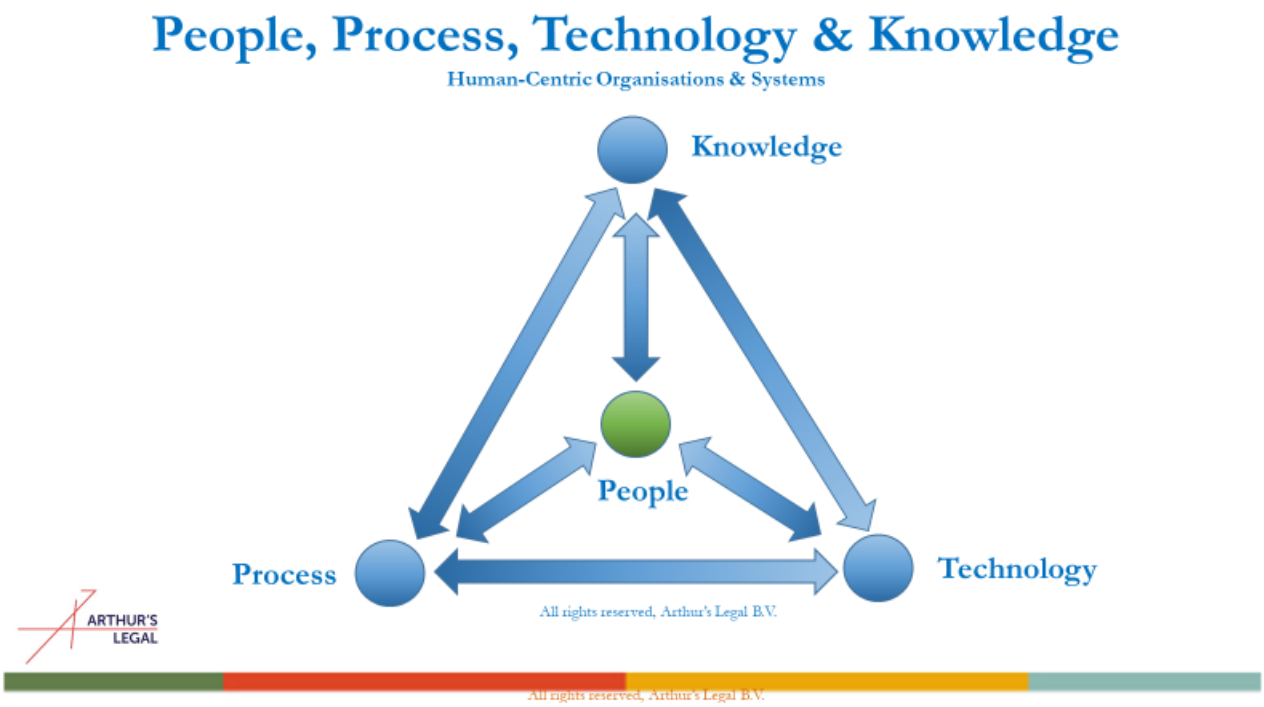

Figure 8: People, Process, Technology & Knowledge

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

3.1.2 Leave Nobody Behind

In accordance with the diversity, and inclusion metrics presented in D2.1 "Best Practice Guidelines for Engaging Citizens in the Pilots and Metrics for Diversity and Inclusion", the TwinERGY project has committed to leave nobody behind and enable the participation of all groups in society, regardless of race, ethnicity, religions, cultural background, disability, and gender. This includes the avoidance of marginalisation or exclusion of underrepresented social groups, seeking actively to include people whose voices are often ignored.

Adhering to the recommendations provided in D12.1 "Legal & Ethical Compliance Guide", throughout the duration of the project the following must be taken into consideration:

1. Ensure that information and venues for meetings are accessible to all.
2. Pay attention to the use of gendered language in all written and oral communications.
3. Ensure that the involvement of vulnerable population in the pilot, do not add to the participants' distress.
4. Periodic assessment of the compliance with diversity and inclusion metrics when planning and developing pilot activities.

Based on the insights gains through the plenary sessions, it is recommended that the user interfaces envisioned to be utilised by the pilots are inclusive to all participants involved. Currently, the technological interfaces envisioned to be used by the participants of the pilots are in English. Therefore, to ensure that participants engagement with the technological elements of the project remain equitable, diverse and inclusive, it is recommended that these interfaces should also be available in the respective languages of each of the pilot locations.

3.1.3 Transparent and Informed Recruitment

The TwinERGY project seeks to promote and establish empathic, honest, and trustworthy relations with people who are engaging in the pilots. As set out in D12.1, the starting point was the informed recruitment process of the participants. During the initial recruitment process, it was recommended that the Pilots adhered to the guiding principles for Leave Nobody Behind and Pilot leaders were encouraged to provide complete and clear information about the involvement of participants in the project, in order to ensure that the decision whether to participate is made from an informed position.

Based on and in adherence to these recommendations, participants should be clearly communicated regarding their right to opt-out of the Pilot program and to request the

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

withdrawal of their data. Therefore, with regard to the participant data held by the Pilots, appropriate technical measures must be put in place to ensure that should a participant decide to opt-out, they are able to also request the deletion of their data from the project.

Building on the notion of the right to opt-out of participation in the project, it is recommended that Pilot leaders avoid overpromising on aspects of the project. This is to ensure that participants are fully informed on the expected outcomes of the project and have expectations that match the envisioned outcomes. In any event and as further elaborated under WP13 deliverables, it should be stressed that individuals involved in the piloting activities are legally entitled both to withdraw from participation in the specific activities and withdraw their consent for the related processing of their personal data. Note that, in case of the latter, personal data relating to these specific individuals should be deleted, as there would no longer be a legal ground allowing for its processing.

3.1.4 Democratic and Empowering Participation

The TwinERGY project envisions the promotion of a sense of empowerment among pilot participants, through taking into account the planning, execution and evaluation of the project. The project aims to put co-creation at centre of the process with the aim to equalise power relations and foster the opinions of all groups to shape their work from different perspectives. The TwinERGY engagement framework visualised below is the envisioned framework for democratic and empowering participation of citizens.

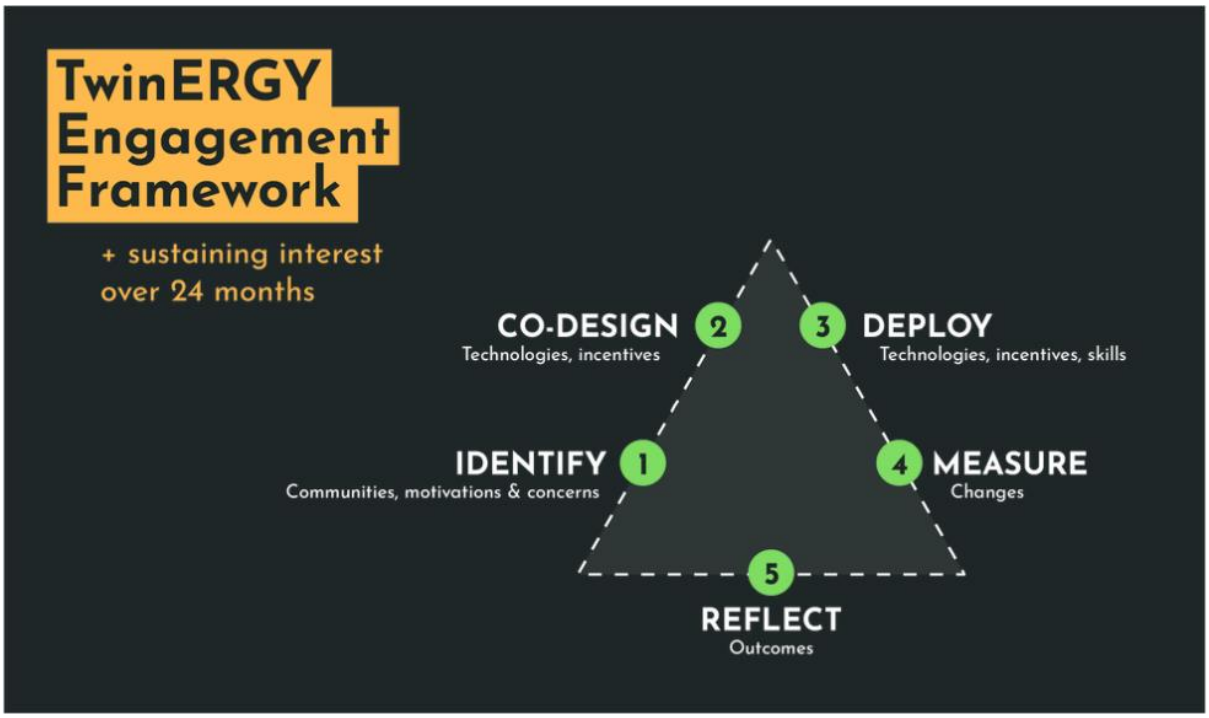

Figure 9: TwinERGY Engagement Framework

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

Based on the discussions observed during the plenary sessions, there are discrepancies between how the various partners view participants of the project. Considering the interdisciplinarity of TwinERGY consortium, some partners view the participants as research subjects whilst others view them as partners in the project. Moreover, this discrepancy is, also, due to the fact that different partners involved in different stages of the project. For example, while some partners are only involved in the technical development phase, others take part in the real-life deployment phase.

3.1.5 Societal Relevance

One of the aims of the TwinERGY project is to respond to actual societal needs and create positive changes for communities. In order to respond to actual societal needs, it is crucial to understand the various cultural, social and economic aspects across all the pilots and their participants. To create positive changes for the communities, the relevant societal challenges in relation to energy management must be identified through participant engagement initiatives. The identification of societal challenges will enable the creation of community-based value models that will aid in the creation of positive changes for the community.

3.1.6 Citizen-Oriented Data Collection and Governance

The TwinERGY project envisions a human-driven approach to data. The project requires various data points to effectively run the pilot activities. To effectively engage citizens and facilitate understanding around data collection and governance, simple language must be used when communication what data are collected, how and why. Participants should be offered the opportunity and means to exercise active governance over their data. For example, participants should be free to decide which data they would like to grant and under which conditions. Moreover, because the data collected will be shared back to the participants, it should be ensured that the data shared with participants are delivered in a meaningful and comprehensive way in order to support participant's learnings and demonstrate the value of the input they have provided through the course of the project.

3.2 Towards Trustworthy and Sustainable Digital Transition

Sustainable digital transitions incorporate two main notions, namely, the environmental sustainability of the digital transition and the sustainability of the project's envisioned outcomes. In reference to the sustainability of the project's envisioned outcomes trust and trustworthiness play an important role in ensuring a successful digital transition.

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

The TwinERGY projects involves the use of digital twin technologies to create virtual models of real-world objects. In the project, the real-world objects that will be virtually modelled are the buildings of the pilots' participants. These digital twins are envisioned to be used to aid in participants' decision making surrounding their energy consumption. Therefore, it is crucial for participants that they are able to trust the digital twins and the underlying data used to create them.

Based on input from the pilot leaders, there was a questionnaire circulated by IES, the partners responsible for the creation of the digital twins in order to collect data from the homes and buildings of the participants involved in the pilots. Notably, the Bristol Pilot took the approach of allowing the participants to fill in their own information and subsequently undertook site visits to each of the sites to ensure the accuracy of the information. Accuracy of the underlying data to create digital twins will ensure that the decisions undertaken by the individuals interacting with these technologies are based on trustworthy information. Moreover, involving the participants in the creation of these digital twins reinforces the notion of co-design as set forth in the TwinERGY engagement framework.

Overall, it seems that the presence of AI anywhere in the project, if any, will be on the module level and will be used to optimise any predictions made to the participants. However, the Bristol Pilot has further communicated that some machine learning will be deployed by a third party in order to ascertain predictive behaviours and consumption profiles for battery management optimisation. In any event, based on the input received and the insights gained from the plenary meeting in Benetutti, it seems that there will be no direct interaction of participants in TwinERGY piloting activities with AI systems.

3.3 Key Takeaways

It is of utmost importance that there are procedures in place where participants are able to hold the vendor of their smart meter accountable when the data processing activities do not comply with the terms and conditions set out in the contractual agreement. Relevant stakeholders must be made aware of their rights and obligations in relation to data processing and exchange.

Moreover, it is recommended that long-term support of participants should be provided if they may so require. Meaningful human control will ensure that the right level of accountability of all stakeholders involved in the project is achieved and sustained. Accountability is about owning and co-owning roles and responsibilities, finding solutions, making things happen, and helping out if things may go wrong. Therefore,

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

accountability must not be an afterthought but is a notion that must exist throughout the entire project.

In adherence to the project's Engagement Framework, it is aimed to keep a high level of citizens' involvement in the co-designing and deploying of the various technologies envisioned to be utilised within the project. For example, in the deployment of the wearable devices envisioned to be provided to the participants of the pilots, participants' engagement in how the device should be used with in the project could be further encouraged. In order to facilitate meaningful participation by the participants, it should be stressed the importance of offering to the participants relevant information in clear language, understandable by non-experts. Moreover, the presentation of project team members as experts to the data subject may be further considered as it may foster an imbalance of power between project partners and participants respectively. Project partners are also encouraged to implement feedback mechanisms to outline how the outcomes of the project were influenced by input from the participants.

In adhering to the previous ethical guidelines, it should be noted that participants should be aware when any information or predictions presented to them are made through the use of AI. Importantly, there should be transparency to the participants in terms of how these decisions or predictions were made and what data was used. The project should put appropriate measures in place to ensure any data fed into AI systems are in no way inaccurate or bias, as they may reinforce pre-existing negative outcomes and undermine the trustworthiness of the system and the project as a whole.

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

4 Concluding Remarks

This deliverable is an interim legal and ethical assessment of the work conducted in the TwinERGY project thus far. The assessments captured in this document took into account the answered questionnaires provided by the pilot leaders and technical partners on the individual pilots and the modules of the TwinERGY project. In addition, the assessment also took into account observations made during the EU Stakeholders Workshop which was held in Benetutti in September 2022.

The TwinERGY project has several overarching project objectives. One of these overarching objectives is to introduce residential energy consumers as active players in the energy markets in order to ensure significant benefits through facilitating engagement in human-centric demand response programs. Moreover, the project also seeks to deliver an open standards-based modular solution that ensure interoperability between smart grids, energy management systems and smart home devices that hold a high replication potential across the EU. To this end, WP12 ties in well to assist in achieving these project objectives. The objective of WP12 is to ensure regulatory, legal and ethics compliance of the project with respective EU regulations and legislation.

The observations on the legal overview of the project and pilot activities presented by this deliverable were laid down in four perspectives, taking into consideration the maturity levels of the project and the pilots under each perspective. Notably, the key takeaways set out under the market- and system-centric perspectives aim to enhance the safety and security of the TwinERGY solution. With the recommended actions, the project partners are supported in the development of future-proof digital systems and services. Furthermore, due to the central role of consumers in the Digital Twin-based Consumer-Centric Energy Management and Control Decision Support mechanism, this deliverable gives emphasis on the key takeaways under the human-centric perspective and encourages the pilot leading partners to take additional measures to improve the project compliance. It is further noted that the project and pilots have already taken several measures set out in the human-centric perspective chapter to protect interests of human participants. From a data-centric perspective, the technical partners are also invited to pay particular attention to the interoperability and portability functions of the TwinERGY solution. Overall, the TwinERGY partners are invited to walk the talk presented as the key takeaways.

Based on the insights gained from the face-to-face plenary sessions that took place in Benetutti in September 2022 , the technical partners are invited to evaluate the use of AI in the project, also, by taking into account of the legal definition of AI under the European

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

legal framework as explained in D12.1 "Legal & Ethical Compliance Guide. More specifically and in light of the aforementioned definition, it is highly recommended that TwinERGY partners assess again in Year 3 whether the project actually uses any AI system and if so, in what context it will be exactly used. This will help for the further legal and ethics assessment in the subsequent deliverable, namely, D12.3 "2nd Year Legal and Ethical Compliance Report" due at month 36 of the project. It is aimed that the latter produces a final assessment on the extent to which aspects covered by the present report are taken into account by the TwinERGY partners during the last year of the project.

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

References

1. COM(2017) 10: 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**]
2. COM(2020) 66: A European strategy for data.
3. COM(2020) 299: Powering a climate-neutral economy: An EU Strategy for Energy System Integration.
4. COM (2020) 823: 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 Directive**]
5. COM (2020) 825: Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. [**Digital Services Act**]
6. COM (2020) 842: Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act). [**Digital Markets Act**]
7. COM (2021) 118: 2030 Digital Compass: the European way for the Digital Decade.
8. 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**]
9. COM (2021) 281: Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. [**European Digital Identity**]
10. COM (2022) 28: European Declaration on Digital Rights and Principles for the Digital Decade.
11. COM (2022) 68: Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). [**Data Act**]
12. COM (2022) 272: Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. [**Cyber Resilience Act**]
13. COM (2022) 496: Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) [**AI Liability Directive**].
14. COM (2022) 552: European Commission, Digitalising the Energy System - EU Action Plan, 18 October 2022.

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

15. 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. [**Product Liability Directive**]
16. Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts OJ L 95/29. [**Directive on Unfair Terms in Consumer Contracts**]
17. Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive, 29 October 2021.
18. Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety OJ L 11/4. [**General Product Safety Directive**]
19. 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**]
20. 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. [**Consumer Rights Directive**]
21. 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. [**Radio Equipment Directive**]
22. 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. [**Revised Payment Services Directive**]
23. 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**]
24. 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**]
25. Directive (EU) 2019/1024 Of The European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. [**Open Data Directive**]

26. European Parliament, Final compromise text of EU Commission's Proposal for a Directive the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union repealing Directive (EU) 2016/1148, 17 June 2022. [**NIS 2 Directive**]
27. European Parliament, Final compromise text of EU Commission's Proposal for a Directive the European Parliament and of the Council on the resilience of critical entities. [**Directive on the Resilience of Critical Entities**]
28. Joint COM(2020) 18: The EU's Cybersecurity Strategy for the Digital Decade.
29. 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, L 257/73. [**eIDAS**]
30. 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**]
31. 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**]
32. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). [**Data Governance Act**]
33. TwinERGY Consortium. Grant Agreement – 957736 – TwinERGY, August 2020. [**Grant Agreement**]
34. 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. [**Free Flow of Data Regulation**]
35. TwinERGY Consortium, Deliverable D2.1 "Best Practice Guidelines for Engaging Citizens in the Pilots and Metrics for Diversity and Inclusion", June 2021.
36. TwinERGY Consortium, Deliverable D5.2 Data Collection, Security, Storage & Management Services Bundles – Beta Release, December 2021.
37. TwinERGY Consortium, Deliverable D5.3 'TwinERGY Integrated Data Management Platform – Alpha, Mockups Release', December 2021.
38. TwinERGY Consortium, Deliverable D7.7 "Transactive Energy Module", April 2022.
39. TwinERGY Consortium, Deliverable D12.5 "Data Use License Template", January 2022.
40. TwinERGY Consortium, Deliverable D13.1 "H- Requirement No.1", January 2021.
41. TwinERGY Consortium, Deliverable D13.2 "POPD Requirement No.2", January 2021.

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

Appendix – I

EDPB's Nine Criteria of High-Risk Data Processing Operations[96]

No	Criteria	Description	Example
1	Use of Innovative Technologies	This refers to processing involving both the use of new technologies, and the novel application of existing technologies such as DL/ML models of AI technology. This is because the personal and social consequences of the use of such technology may be unknown and could result high risk for data subjects.	• Smart Mobility Systems. • Public Infrastructure Management based on ML/DL models.
2	Automated-Decisions with Legal or Similar Significant Effect	Fully automated decision-making procedure that has an impact on legal rights, legal status, social status, or the life standards of individuals.	• Entitlement to or denial of a particular social benefit or public services granted by law.
3	Systemic Monitoring	This type of processing covers organised or methodical tracking of individual's behaviour or geolocation in publicly accessible space including the online realm. It is often conducted according to a pre-arranged organised system and as part of a general plan for data collection.	• The use of a camera system to monitor driving behaviour on public roads. • A company systematically monitoring its employees' workstation.
4	Processing of Data with Highly Personal Nature	The concept of "data with highly personal nature" includes the special categories of personal data defined under Article 9(1) of the GDPR, the data relating to criminal	• A hospital processing its patients' genetic and health data. • The use of facial recognition systems.

[96] The content of this table is largely based on the information provided under WP29' Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Guidelines on Data Protection Officers ('DPOs') and the Information Commissioner's Office Guidance on DPIAs.

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

No	Criteria	Description	Example
		convictions or offences and other categories of sensitive data which can be considered as increasing the possible threats to the rights and freedoms of individuals.	
5	Matching Datasets	This means combining, comparing, or matching personal data obtained from multiple sources or originating from two or more data processing operations performed for different purposes.	• Monitoring personal use/uptake of statutory services or benefits. • Automated fraud prevention techniques. • Federated identity assurance services.
6	Processing on a Large-Scale	When assessing whether the processing is performed on a large scale, the EDPB recommends data controllers to consider i) the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; ii) the volume of data and/or the range of different data items being processed; iii) the duration, or permanence, of the data processing activity; iv) the geographical extent of the processing activity.	• Processing of travel data of individuals using a public transport system such as tracking via public transportation cards.
7	Evaluation or Scoring	This type of processing covers profiling and the use of these profiles to make predictions about the future of individuals such as their performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location, or movements.	• Credit checks for mortgage applications. • Risk assessment for insurance premiums. • Identification of high net-worth individuals for the purposes of direct marketing.
8	Data Concerning Vulnerable Individuals	Vulnerable individuals refer not only to a certain segment of the population that are traditionally deemed vulnerable such as children, mentally ill persons, asylum seekers, or the elders but also to those that are in disadvantageous position in their relationship with the data controller such as employees. Due to the increased imbalance between data controller and subject in the data processing within such contexts, it is presumed that data subject is often unable to knowingly and carefully oppose or consent to the processing or exercise their rights. Therefore, processing of the personal data of vulnerable individuals is deemed to be high-risk processing.	• Data collection through connected toys • Monitoring of the employees' online activities at work.

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

No	Criteria	Description	Example
9	Denial of Service or Right	This includes processing activities including but not limited to the automated decision making that aims at allowing, modifying, or refusing data subjects' access to a product, service, opportunity, or entry into a contract.	• A credit institution screens its customers against a credit reference database in order to decide whether to offer them a loan

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

Annex - I

TwinERGY Pilot Specific Questionnaires

Input for D12.2 – 1st Legal & Ethical Compliance Report

Questions on the Legal and Ethical Aspects of Athens Pilot

1. **Why this questionnaire?**

   This questionnaire has been created to gather input regarding the TwinERGY Athens pilot for Deliverable D12.2 under Task T12.2 on Legal & Ethical Compliance Monitoring, forming part of Work Package 12 on Ethics, Legislation and Standardization. However, it is important to note that the goal of this questionnaire to collect the information that are currently available considering the current stage of the pilots. Therefore, some questions may not be answered or fall out of the scope of the pilot. The pilot inputs to this questionnaire will assist in the creation of the 1st Legal & Ethical Compliance Report, in line with the requirements under D12.2.

2. **What kinds of questions are in this questionnaire?**

   This questionnaire provides for three (2) sets of questions concerning the legal and ethical aspects of the Athens Pilot. The first set of questions focus on connected devices, i.e., IoT, personal/non-personal data and AI systems and it will address the legal aspect of TwinERGY's piloting activities in the Athens Pilot in accordance with the applicable existing and upcoming EU legal frameworks identified under Deliverable D12.1. The second set covering the ethical aspect of the pilot aims at clarifying the potential impact of the project on the participants of the Athens pilot as well as to what extent values and interest of human participants have been considered during the development and deployment of the pilot pursuant to the existing ethics principles and requirements. However, should there be any information that is particularly relevant to the Athens Pilot and is not addressed by the questions, please provide this information on the last box of the questionnaire on 'Additional Information'.

3. **For whom is this questionnaire?**

   This questionnaire is addressed to the Athens Pilot leader, to be disseminated, if deemed necessary, among the relevant partners of the TwinERGY project.

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

QUESTIONS ON THE LEGAL ASPECTS	
Question	**Answer**
1. What devices will be used by the participants of the Athens Pilot? i. Who owns these devices? ii. Please specify the devices that connect and exchange data with other devices/systems over the Internet and/or other communication networks.	*Please provide all the devices used, including those already installed or will be installed in participants' homes.*
2. Are there specific risks identified in the Athens Pilot with respect to use of these devices that might affect the user? If so, to what extent these risks concern the participant safety and health?	
3. To what extent the person responsible for the deployment of these devices is prepared to deal and possible minimize the occurrence of the risks listed above?	
4. To what extent independent auditor and/or public sector bodies are involved in the process of identification and minimisation of those risks?	*For example, any certification confirming the compliance with international safety standards, such as CE.*
5. What measures, if any, will be taken to ensure the safety and reliability of these devices?	
6. What measures, if any, have been implemented to secure the network and information systems of the Athens Pilot?	*For instance, measures taken to prevent unauthorised access to the TwinERGY network, the EV charging stations, servers, and grids via the distributed devices, prevent the accidental loss of data, home energy management device malfunction, or fire in the data room? Please list all the measures taken.*
7. Who will be responsible for the maintenance, safety and operations of the charging stations installed in the residential and public buildings of the Athens Pilot?	
8. Who has ultimate control over the operation of the charging stations installed both in residential and public buildings?	*For example, is a participant able to shut down the charging station that has been installed.*
9. Please list all the data sources of the Athens Pilot. From the data sources provided, what kinds of information are collected from these data sources?	

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

10. What happens to the data collected in the Athens Pilot?	*Please include, where the data is stored, whether it is combined with any other data sets, who processes the data, and who has access to it.*
11. What kinds of output are generated by the data collected in the Athens Pilot and how will the output be used?	
12. Are participants able to transfer the data they generated (including data generated through the use of the Pilot's services and distributed devices) to another service provider at the end of the Athens Pilot?	
13. Does any of the data used in the Athens Pilot come from public bodies?	*Please include, the type of data and what purpose the data is used for.*
14. Are there any exclusive access rights to the data held by public sector bodies that have been granted the Athens Pilot?	
15. What is the legal ground for the sharing of data between the Athens Pilot and the public sector body concerned?	
16. Does the Athens Pilot intend to transfer the data received from the public sector bodies to a country outside the EU?	
17. What measures, if any, will be put in place in order to respond to and notify competent authorities of cyber (security) related incidents occurred in the Athens Pilot?	
18. What artificial intelligence (AI) systems, if any, are used in the Athens Pilot? If the Athens Pilot uses AI systems, please include the following information: i. What does the AI system do? What purpose does it serve in the Pilot? ii. Who developed the AI system? iii. Who makes the AI system available to the participants of the Pilot? iv. Who uses the AI system? v. How were the users of the AI systems chosen?	*For example, purposes of AI system can be determination of electricity tariff, biometric identification of the users or the system operators, as safety components in the management and operation of electricity.*
19. Are users of the AI system in the Athens Pilot able to audit, query, dispute, seek to change or object to the activities of the AI systems?	

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

20. How will the Athens Pilot supervise the decision-making and operations of the AI system during the course of the project?	
21. Has the Athens pilot obtained consent from each adult residing within the household participating in the pilot activities?	
22. Could you please confirm if the Steinheim pilot used the templates of the informed consent form and the information sheet provided in Deliverable D13.1 as such or these templates were updated before being used?	
23. Who determines, alone or jointly, the purposes and means of processing of the personal data in the Athens Pilot (e.g., collection, storage, transmission of the personal data of participants)?	*For example, who determines why and how the personal data of the participant is processed?*
24. Who can access and/or process the personal data collected on behalf of the party who determines the purposes and means of data processing?	
25. What is the purpose of granting the party(ies), identified under Q24, access to the personal data collected?	
26. What is the current arrangement, if any, with those parties (from Q23&Q24) which can access and/or process the data collected?	*For example, is there any data processing agreement in place between these parties?*
27. Has the Athens Pilot adopted any additional criteria that the pilot participants have to meet for being considered for the project apart from those described in the project proposal and in Deliverable D13.1.	
28. Are there any technical and/or organizational measures implemented in the Athens pilot site to safeguard the rights and freedoms of the data subjects/research participants other than anonymization/pseudonymization techniques and the informed consent procedures defined in Chapter 5.5.4 of D13.2.	
29. Is there any specific procedure in place in the Athens Pilot enabling participants to exercise their rights in accordance with the GDPR?	*For example, how do the participants exercise the right to access to their personal data processed in the Athens Pilot?*
30. Has MYTILINAIOS, in its capacity as data controller, carried out data protection impact assessment? Please elaborate what	

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

risks have been identified and/or what mitigating measures have been implemented to address these identified risks.	
31. Do the participant of the Athens Pilot have the right to obtain human intervention on the part of the pilot, to express his or her point of view and to contest the decision based on profiling.	

QUESTIONS ON THE ETHICAL ASPECTS[97]	
Question	**Answer**
1. How will participants of the Athens Pilot be trained to reduce "human errors" in the operations of the devices, as referred under Q1 of the questions concerning the legal aspect above?	
2. Can these connected devices, as referred under Q1 of the questions concerning the legal aspect above, be used by the participants for any other purpose apart from those intended?	
3. Will the data collection happen on a continuous basis through the devices distributed to participants or is it activated upon participant's demand?	
4. How will AI system operators in the Athens Pilot be trained to reduce "human errors" in the operations of AI?	
5. How will users be made aware that they are interacting with an AI system?	
6. What are the measures put in place to contact and inform users of the AI systems of the purpose, capabilities, limitations, benefits, risks, decisions made and consequences of the system, if any?	
7. What kind of 'feedback and review' mechanism, if any, are in place that utilises user feedback/review to re-design the AI system?	
8. Are there any other measures put in place to empower users and promote	*For example, measures to ensure that the operators and/or the end-users i) are not*

[97] Questions concerning the ethical aspects are largely based on various EU ethics policies including the Commission's Guidelines on Ethics By Design and Ethics of Use Approaches for Artificial Intelligence dated 25 November 2021, the Commission's Communication on European Declaration on Digital Rights and Principles for the Digital Decade dated 26 January 2022.

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

users' autonomy when interacting with the AI system?	*subordinated by the AI system, or ii) they do not develop attachment to the AI systems, or iii) their judgement are not stimulated by the system*
9. In case of a conflicting assessment between the operator and the AI system, whose assessment will prevail?	
10. In case of a conflicting interest between the operator of the shared EV and the users, whose interest will prevail?	
11. Which groups of end-users does the Athens Pilot recruit for taking part in the project? Do the requirements for participation exclude certain groups of people? If so, why?	
12. To what extend does the Athens pilot accomplish to build a sense of ownership of the overall pilot activities and empowerment among the participants, apart from collecting feedback and reviews from the stakeholders described in Q6?	*For instance, how does the Athens Pilot avoid presenting project team members as the experts on the subject in a way that may generate an imbalance in power relations.*

ADDITIONAL INFORMATION

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

Input for D12.2 – 1st Legal & Ethical Compliance Report

Questions on the Legal and Ethical Aspects of Benetutti Pilot

1. **Why this questionnaire?**

   This questionnaire has been created to gather input regarding the TwinERGY Benetutti pilot for Deliverable D12.2 under Task T12.2 on Legal & Ethical Compliance Monitoring, forming part of Work Package 12 on Ethics, Legislation and Standardization. However, it is important to note that the goal of this questionnaire to collect the information that are currently available considering the current stage of the pilots. Therefore, some questions may not be answered or fall out of the scope of the pilot. The pilot inputs to this questionnaire will assist in the creation of the 1st Legal & Ethical Compliance Report, in line with the requirements under D12.2.

2. **What kinds of questions are in this questionnaire?**

   This questionnaire provides for three (2) sets of questions concerning the legal and ethical aspects of the Benetutti Pilot. The first set of questions focus on connected devices, i.e., IoT, personal/non-personal data and AI systems and it will address the legal aspect of TwinERGY's piloting activities in the Benetutti Pilot in accordance with the applicable existing and upcoming EU legal frameworks identified under Deliverable D12.1. The second set covering the ethical aspect of the pilot aims at clarifying the potential impact of the project on the participants of the Benetutti pilot as well as to what extent values and interest of human participants have been considered during the development and deployment of the pilot pursuant to the existing ethics principles and requirements. However, should there be any information that is particularly relevant to the Benetutti Pilot and is not addressed by the questions, please provide this information on the last box of the questionnaire on 'Additional Information'.

3. **For whom is this questionnaire?**

   This questionnaire is addressed to the Benetutti Pilot leader, to be disseminated, if deemed necessary, among the relevant partners of the TwinERGY project.

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

QUESTIONS ON THE LEGAL ASPECTS	
Question	**Answer**
1. What devices will be used by the participants of the Benetutti Pilot? i. Who owns these devices? ii. Please specify the devices that connect and exchange data with other devices/systems over the Internet and/or other communication networks.	*Please provide all the devices used, including those already installed or will be installed in participants' homes.*
2. Are there specific risks identified in the Bristol Pilot with respect to use of these devices that might affect the user? If so, to what extent these risks concern the participant safety and health?	
3. To what extent the person responsible for the deployment of these devices is prepared to deal and possible minimize the occurrence of the risks listed above?	
4. To what extent independent auditor and/or public sector bodies are involved in the process of identification and minimisation of those risks?	*For example, any certification confirming the compliance with international safety standards, such as CE.*
5. What measures, if any, will be taken to ensure the safety and reliability of these devices?	
6. What measures, if any, have been implemented to secure the network and information systems of the Benetutti Pilot?	*For instance, measures taken to prevent unauthorised access to the TwinERGY network, servers, and grids via the distributed devices, prevent the accidental loss of data, home energy management device malfunction, or fire in the data room? Please list all the measures taken.*
7. Who will be responsible for the maintenance and operations of the batteries and Solar PVs installed in the residential and public buildings of the Benetutti Pilot? If it is provided by a party other than the participants, what is the legal arrangement/basis for this service?	
8. What measures, if any, will be taken to ensure the safety and reliability of these Solar PVs and batteries?	

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

9. Who has ultimate control over the operation of these batteries and Solar PVs?	
10. Please list all the data sources of the Benetutti Pilot. From the data sources provided, what kinds of information are collected from these data sources?	
11. What happens to the data collected in the Benetutti Pilot?	*Please include, where the data is stored, whether it is combined with any other data sets, who processes the data, and who has access to it.*
12. What kinds of output are generated by the data collected in the Benetutti Pilot and how will the output be used?	
13. Are participants able to transfer the data they generated (including data generated through the use of the Pilot's services and distributed devices) to another service provider at the end of the Benetutti Pilot?	
14. Does any of the data used in the Benetutti Pilots come from public bodies?	*Please include, the type of data and what purpose the data is used for.*
15. Are there any exclusive access rights to the data held by public sector bodies that have been granted the Benetutti Pilot?	
16. What is the legal ground for the sharing of data between the Benetutti Pilot and the public sector body concerned?	
17. Does the Benetutti Pilot intend to transfer the data received from the public sector bodies to a country outside the EU?	
18. What measures, if any, will be put in place in order to respond to and notify competent authorities of cyber (security) related incidents occurred in the Benetutti Pilot?	
19. What Artificial Intelligence (AI) systems, if any, are used in the Benetutti Pilot? If the Benetutti Pilot uses AI systems, please include the following information: i. What does the AI system do? What purpose does it serve in the Pilot? ii. Who developed the AI system? iii. Who makes the AI system available to the participants of the Pilot? iv. Who uses the AI system?	*For example, purposes of AI system can be determination of electricity tariff, biometric identification of the users or the system operators, as safety components in the management and operation of electricity.*

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

v. How were the users of the AI systems chosen?	
20. Are users of the AI system in the Benetutti Pilot able to audit, query, dispute, seek to change or object to the activities of the AI systems?	
21. How will the Benetutti Pilot supervise the decision-making and operations of the AI system during the course of the project?	
22. Could you please confirm if the Benetutti pilot used the templates of the informed consent form and the information sheet provided in Deliverable D13.1 as such or these templates were updated before being used?	
23. Has the Benetutti pilot obtained consent from each adult residing within the household participating in the pilot activities?	
24. Who determines, alone or jointly, the purposes and means of processing of the personal data in the Benetutti Pilot (e.g., collection, storage, transmission of the personal data of participants)?	*For example, who determines why and how the personal data of the participant is processed?*
25. Who can access and/or process the personal data collected on behalf of the party who determines the purposes and means of data processing?	
26. What is the purpose of granting the party(ies), identified under Q25, access to the personal data collected?	
27. What is the current arrangement, if any, with those parties (from Q24&Q25) which can access and/or process the data collected?	*For example, is there any data processing agreement in place between these parties?*
28. Did the Benetutti Pilot adopt any additional criteria that the pilot participants have to meet for being considered for the project apart from those described in the project proposal and in Deliverable D13.1.	
29. Are there any technical and/or organizational measures implemented in the Benetutti pilot site to safeguard the rights and freedoms of the data subjects/research participants other than anonymization/pseudonymization techniques and the informed consent procedures defined in Chapter 5.4.4 of D13.2.	

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

30. Is there any specific procedure in place in the Benetutti Pilot enabling participants to exercise their rights in accordance with the GDPR?	*For example, how do the participants exercise the right to access to their personal data processed in the Benetutti Pilot?*
31. Has any of partner taking part in the Benetutti pilot, in its capacity as data controller, carried out a data protection impact assessment? Please elaborate what risks have been identified and/or what mitigating measures have been implemented to address these identified risks.	
32. Do the participant of the Benetutti Pilot have the right to obtain human intervention on the part of the pilot, to express his or her point of view and to contest the decision based on profiling.	
33. Provide us with an overview of your pilot demonstration as planned based on the proposal?	

QUESTIONS ON THE ETHICAL ASPECTS[98]	
Question	**Answer**
1. How will participants of the Benetutti Pilot be trained to reduce "human errors" in the operations of the devices, as referred under Q1 of the questions concerning the ethical aspect above?	
2. Can these connected devices, as referred under Q1 of the questions concerning the ethical aspect above, be used by the participants for any other purpose apart from those intended?	
3. Will the data collection happen on a continuous basis through the devices distributed to participants or is it activated upon participant's demand?	
4. How will AI system operators in the Benetutti Pilot be trained to reduce "human errors" in the operations of AI?	
5. How will users be made aware that they are interacting with an AI system?	

[98] Questions concerning the ethical aspects are largely based on various EU ethics policies including the Commission's Guidelines on Ethics By Design and Ethics of Use Approaches for Artificial Intelligence dated 25 November 2021, the Commission's Communication on European Declaration on Digital Rights and Principles for the Digital Decade dated 26 January 2022.

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

6. What are the measures put in place to contact and inform users of the AI systems of the purpose, capabilities, limitations, benefits, risks, decisions made and consequences of the system, if any?	
7. What kind of 'feedback and review' mechanism, if any, are in place that utilises user feedback/review to re-design the AI system?	
8. Are there any other measures put in place to empower users and promote users' autonomy when interacting with the AI system?	*For example, measures to ensure that the operators and/or the end-users i) are not subordinated by the AI system, or ii) they do not develop attachment to the AI systems, or iii) their judgement are not stimulated by the system*
9. In case of a conflicting assessment between the operator and the AI system, whose assessment will prevail?	
10. Which groups of end-users does the Benetutti Pilot recruit for taking part in the project? Do the requirements for participation exclude certain groups of people? If so, why?	
11. To what extend does the Benetutti pilot accomplish to build a sense of ownership of the overall pilot activities and empowerment among the participants, apart from collecting feedback and reviews from the stakeholders described in Q6?	*For instance, how does the Benetutti Pilot avoid presenting project team members as the experts on the subject in a way that may generate an imbalance in power relations.*

ADDITIONAL INFORMATION

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

Input for D12.2 – 1st Legal & Ethical Compliance Report

Questions on the Legal and Ethical Aspects of Bristol Pilot

1. **Why this questionnaire?**

   This questionnaire has been created to gather input regarding the TwinERGY Bristol pilot for Deliverable D12.2 under Task T12.2 on Legal & Ethical Compliance Monitoring, forming part of Work Package 12 on Ethics, Legislation and Standardization. However, it is important to note that the goal of this questionnaire to collect the information currently available considering the current stage of the pilots. Therefore, some questions may not be answered or fall out of the scope of the pilot. The pilot inputs to this questionnaire will assist in the creation of the 1st Legal & Ethical Compliance Report, in line with the requirements under D12.2.

2. **What kinds of questions are in this questionnaire?**

   This questionnaire provides for two (2) sets of questions regarding the ethical and legal aspects of the Bristol Pilot. The first set of questions focus on connected devices, i.e., IoT, personal/non-personal data and AI systems and it will address the legal aspect of TwinERGY's piloting activities in the Bristol Pilot in accordance with UK regulations identified under Deliverable D12.1 to extent that the obligation and requirements of identified UK regulations correspond to applicable existing and upcoming EU legal frameworks. The second part related to the ethical aspect of the pilot aim at clarifying the potential impact of the project on the participants of the Bristol pilot as well as to what extent values and interest of human participants have been considered during the development and deployment of the pilot pursuant to the existing ethics principles. However, should there be any information that is particularly relevant to the Bristol Pilot and is not addressed by the questions, please provide this information on the last box of the questionnaire on 'Additional Information'.

3. **For whom is this questionnaire?**

   This questionnaire is addressed to the Bristol Pilot leader, to be disseminated, if deemed necessary, among the relevant partners of the TwinERGY project.

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

QUESTIONS ON THE LEGAL ASPECTS	
Question	**Answer**
1. What devices will be used by the participants of the Bristol Pilot? i. Who owns these devices? ii. Please specify the devices that connect and exchange data with other devices/systems over the Internet and/or other communication networks.	*Please provide all the devices used, including those already installed or will be installed in participants' homes.*
2. Are there specific risks identified in the Bristol Pilot with respect to use of these devices that might affect the user? If so, to what extent these risks concern the participant safety and health?	
3. To what extent the person responsible for the deployment of these devices is prepared to deal and possible minimize the occurrence of the risks listed above?	
4. To what extent independent auditor and/or public sector bodies are involved in the process of identification and minimisation of those risks?	*For example, any certification confirming the compliance with international safety standards, such as CE.*
5. What measures, if any, will be taken to ensure the safety and reliability of these devices?	
6. What measures, if any, have been implemented to secure the network and information systems of the Pilot?	*For instance, measures taken to prevent unauthorised access to the TwinERGY network, servers, and grids via the distributed devices, prevent the accidental loss of data, home energy management device malfunction, or fire in the data room? Please list all the measures taken.*
7. Who will be responsible for the maintenance and operations of the batteries and Solar PVs installed in the residential and public buildings in the Bristol Pilot? If it is provided by a party other than the participants, what is the legal arrangement/basis for this service?	
8. What measures, if any, will be taken to ensure the safety and reliability of these Solar PVs and batteries?	
9. Who has ultimate control over the operation of these batteries and Solar PVs?	

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

10. Please list all the data sources of the Bristol Pilot. From the data sources provided, what kinds of information are collected from these data sources?	*Please indicate if there are changes in information provided in table 2 of D12.5.*
11. What happens to the data collected in the Bristol Pilot?	*Please include, whether the data is still stored in the Research Data Storage Facility of UNIVBRIS, whether it is combined with any other data sets, who processes the data, and who has access to it. Please indicate if there are changes in information provided in table 2 of D12.5 and Chapter 5.2.4 of D13.2.*
12. What kinds of output are generated by the data collected in the Bristol Pilot and how will the output be used?	
13. Are participants able to transfer the data they generated (including data generated through the use of the Pilot's services and distributed devices) to another service provider at the end of the Pilot?	
14. Does any of the data used in the Bristol Pilots come from public bodies?	*Please include, the type of data and what purpose the data is used for.*
15. Are there any exclusive access rights to the data held by public sector bodies that have been granted to the Bristol Pilot?	
16. What is the legal ground for the sharing of data between the Bristol Pilot and the public sector body concerned?	
17. Does the Bristol Pilot intend to transfer the data received from the public sector bodies to a country outside the EU and the UK?	
18. What measures, if any, will be put in place in order to respond to and notify competent authorities of cyber (security) related incidents occurred in the Bristol Pilot?	
19. What artificial intelligence (AI) systems, if any, are used in the Bristol Pilot? If the Bristol Pilot uses AI systems, please include the following information: i. What does the AI system do? What purpose does it serve in the Pilot? ii. Who developed the AI system? iii. Who makes the AI system available to the participants of the Pilot?	*For example, purposes of AI system can be determination of electricity tariff, biometric identification of the users or the system operators, as safety components in the management and operation of electricity.*

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

iv. Who uses the AI system? v. How were the users of the AI systems chosen?	
20. Are users of the AI system able to audit, query, dispute, seek to change or object to the activities of the AI systems?	
21. How will the Bristol Pilot supervise the decision-making and operations of the AI system during the course of the project?	
22. Has the Bristol Pilot obtained consent from each adult residing within the household participating in the pilot?	
23. Could you please confirm if the Bristol pilot used the templates of the informed consent form and the information sheet provided in Deliverable D13.1 as such or these templates were updated before being used?	
24. Who determines, alone or jointly, the purposes and means of processing of the personal data in the Bristol Pilot?	*For example, who determines why and how the personal data of the participant is processed?*
25. Who can access and/or process the personal data collected on behalf of the party who determines the purposes and means of data processing?	*Please indicate if there are changes in information provided in table 2 of Deliverable D12.5.*
26. What is the purpose of granting the party(ies), identified under Q25, access to the personal data collected?	
27. What is the current arrangement, if any, with those parties (from Q24&Q25) which can access and/or process the data collected?	*For example, is there any data processing agreement in place between these parties? Please indicate the legal arrangement with those parties that have been designated as the receiver of the data in table 2 of Deliverable D12.5.*
28. Did the Bristol Pilot adopt any additional criteria that the pilot participants have to meet for being considered for the project apart from those described in the project proposal and in Deliverable D13.1.	
29. Are there any technical and/or organizational measures implemented in the Bristol pilot to safeguard the rights and freedoms of the data subjects/research participants other than secure storage facility, anonymization/pseudonymization techniques and the informed consent procedures defined in Chapter 5.2.4 of Deliverable D13.2.	

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

30. Is there any specific procedure in place in the Bristol Pilot enabling participants to exercise their rights in accordance with the GDPR?	*For example, how do the participants exercise the right to access to their personal data processed in the Bristol Pilot?*
31. Has any of partner taking part in the Bristol pilot, in its capacity as data controller, carried out data protection impact assessments? If yes, please elaborate what risks have been identified in this assessment and/or what mitigating measures have been implemented to address these identified risks.	
32. Do the participant of the Bristol Pilot have the right to obtain human intervention on the part of the pilot, to express his or her point of view and to contest the decision based on profiling.	

QUESTIONS ON THE ETHICAL ASPECTS[99]	
Question	**Answer**
1. How will participants of the Bristol Pilot be trained to reduce "human errors" in the operations of the devices, as referred under Q1 of the questions concerning the legal aspect above?	
2. Can these connected devices, as referred under Q1 of the questions concerning the legal aspect above, be used by the participants for any other purpose apart from those intended?	
3. Will the data collection happen on a continuous basis through the devices distributed to participants or is it activated upon participant's demand?	
4. How will AI system operators in the Bristol Pilot be trained to reduce "human errors" in the operations of AI?	
5. How will users be made aware that they are interacting with an AI system?	
6. What are the measures put in place to contact and inform users of the AI systems of the purpose, capabilities, limitations, benefits, risks, decisions	

[99] Questions on the ethical aspects of the pilot are largely based on various EU ethics policies including the Commission's Guidelines on Ethics By Design and Ethics of Use Approaches for Artificial Intelligence dated 25 November 2021, the Commission's Communication on European Declaration on Digital Rights and Principles for the Digital Decade dated 26 January 2022.

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

made and consequences of the system, if any?	
7. What kind of 'feedback and review' mechanism, if any, are in place that utilises user feedback/review to re-design the AI system?	
8. Are there any other measures put in place to empower users and promote users' autonomy when interacting with the AI system?	*For example, measures to ensure that the operators and/or the end-users i) are not subordinated by the AI system, or ii) they do not develop attachment to the AI systems, or iii) their judgement are not stimulated by the system*
9. In case of a conflicting assessment between the operator and the AI system, whose assessment will prevail?	
10. Which groups of end-users does the Bristol Pilot recruit for taking part in the project? Do the requirements for participation exclude certain groups of people? If so, why?	
11. To what extend does the Bristol pilot accomplish to build a sense of ownership of the overall pilot activities and empowerment among the participants, apart from collecting feedback and reviews from the stakeholders described in Q6?	*For instance, how does the Bristol Pilot avoid presenting project team members as the experts on the subject in a way that may generate an imbalance in power relations.*

ADDITIONAL INFORMATION

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

Input for D12.2 – 1st Legal & Ethical Compliance Report

Questions on the Legal and Ethical Aspects of Steinheim Pilot

1. **Why this questionnaire?**

   This questionnaire has been created to gather input regarding the TwinERGY Steinheim pilot for Deliverable D12.2 under Task T12.2 on Legal & Ethical Compliance Monitoring, forming part of Work Package 12 on Ethics, Legislation and Standardization. However, it is important to note that the goal of this questionnaire to collect the information that are currently available considering the current stage of the pilots. Therefore, some questions may not be answered or fall out of the scope of the pilot. The pilot inputs to this questionnaire will assist in the creation of the 1st Legal & Ethical Compliance Report, in line with the requirements under D12.2.

2. **What kinds of questions are in this questionnaire?**

   This questionnaire provides for three (2) sets of questions concerning the legal and ethical aspects of the Steinheim Pilot. The first set of questions focus on connected devices, i.e., IoT, personal/non-personal data and AI systems and it will address the legal aspect of TwinERGY's piloting activities in the Steinheim Pilot in accordance with the applicable existing and upcoming EU legal frameworks identified under Deliverable D12.1. The second set covering the ethical aspect of the pilot aims at clarifying the potential impact of the project on the participants of the Steinheim pilot as well as to what extent values and interest of human participants have been considered during the development and deployment of the pilot pursuant to the existing ethics principles and requirements. However, should there be any information that is particularly relevant to the Steinheim Pilot and is not addressed by the questions, please provide this information on the last box of the questionnaire on 'Additional Information'.

3. **For whom is this questionnaire?**

   This questionnaire is addressed to the Steinheim Pilot leader, to be disseminated, if deemed necessary, among the relevant partners of the TwinERGY project.

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

QUESTIONS ON THE LEGAL ASPECTs	
Question	**Answer**
1. What devices will be used by the participants of the Steinheim Pilot? i. Who owns these devices? ii. Please specify the devices that connect and exchange data with other devices/systems over the Internet and/or other communication networks.	*Please provide all the devices used, including those already installed or will be installed in participants' homes.*
2. Are there specific risks identified in the Steinheim Pilot with respect to use of these devices that might affect the user? If so, to what extent these risks concern the participant safety and health?	
3. To what extent the person responsible for the deployment of these devices is prepared to deal and possible minimize the occurrence of the risks listed above?	
4. To what extent independent auditor and/or public sector bodies are involved in the process of identification and minimisation of those risks?	*For example, any certification confirming the compliance with international safety standards, such as CE.*
5. What measures, if any, will be taken to ensure the safety and reliability of these devices?	
6. What measures, if any, have been implemented to secure the network and information systems of the Steinheim Pilot?	*For instance, measures taken to prevent unauthorised access to the TwinERGY network, the shared EV, servers, and grids via the distributed devices, prevent the accidental loss of data, home energy management device malfunction, or fire in the data room? Please list all the measures taken.*
7. Do users of the shared EV have to agree to specific terms and conditions in order to use the vehicles? Or is there any other legal arrangement /basis in place for this purpose?	
8. Who will be responsible for the maintenance, safety and operations of the shared EV and the charging stations installed in the residential and public buildings of the Steinheim Pilot?	
9. Who has ultimate control over the operation of the charging stations as well as the shared EV?	*For example, is a participant able to shut down the charging station that has been installed.*

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

10. Who will be responsible for the maintenance and operations of the batteries and Solar PVs installed in the residential and public buildings of the Steinheim Pilot? If it is provided by a third-party other than the participants, what is the legal arrangement/basis for this service?	
11. What measures, if any, will be taken to ensure the safety and reliability of these Solar PVs and batteries?	
12. Who has ultimate control over the operation of these batteries and Solar PVs?	
13. Please list all the data sources of the Steinheim Pilot. From the data sources provided, what kinds of information are collected from these data sources?	
14. What happens to the data collected in the Steinheim Pilot?	*Please include, where the data is stored, whether it is combined with any other data sets, who processes the data, and who has access to it.*
15. What kinds of output are generated by the data collected in the Steinheim Pilot and how will the output be used?	
16. Are participants able to transfer the data they generated (including data generated through the use of the Pilot's services and distributed devices) to another service provider at the end of the Steinheim Pilot?	
17. Does any of the data used in the Steinheim Pilot come from public bodies?	*Please include, the type of data and what purpose the data is used for.*
18. Are there any exclusive access rights to the data held by public sector bodies that have been granted the Steinheim Pilot?	
19. What is the legal ground for the sharing of data between the Steinheim Pilot and the public sector body concerned?	
20. Does the Steinheim Pilot intend to transfer the data received from the public sector bodies to a country outside the EU?	
21. What measures, if any, will be put in place in order to respond to and notify competent authorities of cyber (security) related incidents occurred in the Steinheim Pilot?	
22. What artificial intelligence (AI) systems, if any, are used in the Steinheim Pilot?	*For example, purposes of AI system can be determination of electricity tariff, biometric identification of the users or the system*

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

If the Steinheim Pilot uses AI systems, please include the following information: i. What does the AI system do? What purpose does it serve in the Pilot? ii. Who developed the AI system? iii. Who makes the AI system available to the participants of the Pilot? iv. Who uses the AI system? v. How were the users of the AI systems chosen?	*operators, as safety components in the management and operation of electricity.*
23. Are users of the AI system in the Steinheim Pilot able to audit, query, dispute, seek to change or object to the activities of the AI systems?	
24. How will the Steinheim Pilot supervise the decision-making and operations of the AI system during the course of the project?	
25. Has the Steinheim pilot obtained consent from each adult residing within the household participating in the pilot activities?	
26. Could you please confirm if the Steinheim pilot used the templates of the informed consent form and the information sheet provided in Deliverable D13.1 as such or these templates were updated before being used?	
27. Who determines, alone or jointly, the purposes and means of processing of the personal data in the Steinheim Pilot (e.g., collection, storage, transmission of the personal data of participants)?	*For example, who determines why and how the personal data of the participant is processed?*
28. Who can access and/or process the personal data collected on behalf of the party who determines the purposes and means of data processing?	
29. What is the purpose of granting the party(ies), identified under Q28, access to the personal data collected?	
30. What is the current arrangement, if any, with those parties (from Q27&Q28) which can access and/or process the data collected?	*For example, is there any data processing agreement in place between these parties?*
31. Has the Steinheim Pilot adopted any additional criteria that the pilot participants have to meet for being considered for the project apart from those described in the project proposal and in Deliverable D13.1.	

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

32. Are there any technical and/or organizational measures implemented in the Steinheim pilot site to safeguard the rights and freedoms of the data subjects/research participants other than anonymization/pseudonymization techniques and the informed consent procedures defined in Chapter 5.3.4 of D13.2.	
33. Is there any specific procedure in place in the Steinheim Pilot enabling participants to exercise their rights in accordance with the GDPR?	*For example, how do the participants exercise the right to access to their personal data processed in the Steinheim Pilot?*
34. Has any of partner taking part in the Steinheim pilot, in its capacity as data controller, carried out data protection impact assessment? Please elaborate what risks have been identified and/or what mitigating measures have been implemented to address these identified risks.	
35. Do the participant of the Steinheim Pilot have the right to obtain human intervention on the part of the pilot, to express his or her point of view and to contest the decision based on profiling.	

QUESTIONS ON THE ETHICAL ASPECTS[100]	
Question	**Answer**
1. How will participants of the Steinheim Pilot be trained to reduce "human errors" in the operations of the devices, as referred under Q1 of the questions concerning the legal aspect above?	
2. Can these connected devices, as referred under Q1 of the questions concerning the legal aspect above, be used by the participants for any other purpose apart from those intended?	
3. Will the data collection happen on a continuous basis through the devices distributed to participants or is it activated upon participant's demand?	

[100] Questions concerning the ethical aspects are largely based on various EU ethics policies including the Commission's Guidelines on Ethics By Design and Ethics of Use Approaches for Artificial Intelligence dated 25 November 2021, the Commission's Communication on European Declaration on Digital Rights and Principles for the Digital Decade dated 26 January 2022.

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

4. How will AI system operators in the Steinheim Pilot be trained to reduce "human errors" in the operations of AI?	
5. How will users be made aware that they are interacting with an AI system?	
6. What are the measures put in place to contact and inform users of the AI systems of the purpose, capabilities, limitations, benefits, risks, decisions made and consequences of the system, if any?	
7. What kind of 'feedback and review' mechanism, if any, are in place that utilises user feedback/review to re-design the AI system?	
8. Are there any other measures put in place to empower users and promote users' autonomy when interacting with the AI system?	*For example, measures to ensure that the operators and/or the end-users i) are not subordinated by the AI system, or ii) they do not develop attachment to the AI systems, or iii) their judgement are not stimulated by the system*
9. In case of a conflicting assessment between the operator and the AI system, whose assessment will prevail?	
10. In case of a conflicting interest between the operator of the shared EV and the users, whose interest will prevail?	
11. Which groups of end-users does the Steinheim Pilot recruit for taking part in the project? Do the requirements for participation exclude certain groups of people? If so, why?	
12. To what extend does the Steinheim pilot accomplish to build a sense of ownership of the overall pilot activities and empowerment among the participants, apart from collecting feedback and reviews from the stakeholders described in Q6?	*For instance, how does the Steinheim Pilot avoid presenting project team members as the experts on the subject in a way that may generate an imbalance in power relations.*

ADDITIONAL INFORMATION

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

Annex - II

TwinERGY Module Specific Questionnaire

Input for D12.2 – 1st Legal & Ethical Compliance Report

Questions on the Legal and Ethical Aspects of the TwinERGY Project

1. **Why this questionnaire?**

   This questionnaire has been created to gather input regarding the TwinERGY project in general for Deliverable D12.2 under Task T12.2 on Legal & Ethical Compliance Monitoring, forming part of Work Package 12 on Ethics, Legislation and Standardization. However, it is important to note that the goal of this questionnaire is to collect the information currently available considering the current stage of the project. Therefore, some questions may not be answered or fall out of the scope of the current project activities. The inputs to this questionnaire from the relevant partners will assist in the creation of the 1st Legal & Ethical Compliance Report, in line with the requirements under D12.2.

2. **What kinds of questions are in this questionnaire?**

   This questionnaire provides for two (2) sets of questions regarding the ethical and legal aspects of the TwinERGY Project. The first set of questions focus on TwinERGY system modules, the interoperability capabilities of these modules and the datasets used to create digital representation of buildings and it will address the legal aspects of TwinERGY project in accordance with the applicable existing and upcoming EU legal frameworks identified in Deliverable D12.1. The second part focuses on the ethical aspects of the project, and it aims at examining the ethics risks of AI systems and the digital twin concept and their potential impact on the participants. However, should there be any information that is particularly relevant to the project and is not addressed by the questions, please provide this information on the last box of the questionnaire on 'Additional Information'.

3. **For whom is this questionnaire?**

   This questionnaire is addressed to the partners responsible for the TwinERGY and at the discretion of the coordinator team, the questionnaire will be disseminated to the partners who are actively involved with the relevant fields of the TwinERGY project

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

QUESTIONS ON THE LEGAL ASPECTS	
Question	**Answer**
1. What are the features of the Social Network Module? Please include any features like direct messaging, upload or share features that enable interaction between different users and discover other users and contents across the application.	*For example, Does the main function of the Social Network Module include **the storage of information provided by**, and at the request of, their users? Or **the dissemination of such information to the public**, to other users.*
2. To what extent does the project take measures to tackle any unlawful or illegal activity of the users that may occur on the Social Network Module?	*For instance, **terms and conditions** forbidding users to carry out certain activities or notice & takedown procedures that allow users to **report unlawful activities**.*
3. Could you please indicate which of the following services is provided by the TwinERGY Modules? i) services which allow business users to offer goods or services to consumers, with the aim to facilitate the initiating of direct transactions between those business users and consumers; ii) services that consist of the storage of information provided by, and at the request of, a user of the service; iii) payment services including the execution of direct debits, payment transactions etc. iv) online search engines; v) online social networking services; vi) video-sharing platform services; vii) number-independent interpersonal communications services; viii) operating systems; ix) web browsers; x) virtual assistants; xi) cloud computing services;	*Please note that this information, among others, will be used to determine whether the provider of any TwinERGY modules fall under the scope of* the ***Revised Payment Services Directive**, the proposed **Digital Services Act**, and the proposed **Digital Markets Act**. Please also elaborate briefly on how the indicated service(s) will be provided. The outcome of this assessment aims to **future-proof the modules**. Although the types of modules are explained under the Grant Agreement, this question aims to gather input concerning the core services and functions of each module directly from the developers.*

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

xii) online advertising services.	
4. Could you please provide us the current number of users for each TwinERGY module?	*Please also provide us an **estimated number of users**. This information, among others, will be used to determine whether the provider of any TwinERGY modules falls under the scope of proposed **Digital Services Act** and **Digital Markets Act**.*
5. How will these services on TwinERGY modules be offered to users?	*Please note that this question aims to elaborate on **the legal basis of the provision of services to the users**, for example, **subscription base**, **free of charge** etc. Please also state if there is any terms and conditions for the provision of these services in place.*
6. To what extent does the project provide the interoperability of the eight (8) TwinERGY modules and the Interoperability Platform with other third-party services and/or products for the users?	*For instance, can **the Home & Tertiary Real-Time Energy Monitoring be used with any smart meter or Solar PV from a third-party vendor**? Or, will the DER Module be able to operate with an RES Forecast application developed by a third-party?*
7. To what extent does the project allow the stakeholders to easily switch, and transfer data generated by their use of the TwinERGY Modules and devices to different premises or third-party service providers without losing their data?	*Stakeholders include, among others, transmission system operators, distribution system operators, and charging station owners or operators. For instance, does the Core Data Management Platform allow both the business and/or consumer users to transfer all their data to another platform, cloud service provided by a third-party or to port their data to their on-premise server?*
8. Are the datasets used to create the digital twins or the datasets generated based on digital twins open source, open access or otherwise accessible or shareable? i. If not, why is the accessibility limited? ii. If yes, to your knowledge, what is the legal ground allowing to share such data? iii. If yes, how will the project make these datasets available to the public?	*Please note that **'open source' and 'open access' refer to access to these datasets by a third-party outside the project consortium**. For instance, due to IP rights or data protection rights. Please elaborate on how access by third parties to these datasets will be shared and the procedure for the third party to access these datasets.*

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

9. Is there any verification system within the project to ensure the accuracy of the data used to create real-time representation of the buildings, i.e., digital twins, and of the interactions within these buildings between humans and electric devices?	*For example, a system to verify that the data collected through sensors are not polluted intentionally by a human user or due to sensor malfunction etc.*
10. To what extent does the project implement technical and/or organizational measures to safeguard the rights and freedoms of the individual participants with respect to the processing of their data in the Core Data Management Platform?	
11. To what extent does the project allow the participants to exercise their rights in accordance with the GDPR with respect to the processing of their personal data in the Core Data Management Platform? Is there any special procedure for this purpose in place?	*For example, how do the participants exercise the right to access to their personal data processed in the project*

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

QUESTIONS ON THE ETHICAL ASPECTS[101]	
Question	**Answer**
1. What measures, if any, are in place to avoid bias? *Please account for:* *i) historical and selection bias in data collection;* *ii) representation and measurement bias in algorithmic training aggregation;* *iii) evaluation bias in modelling;* *iv) automation bias in deployment?*	
2. To what extent does the project Has the data training process/dataset used by the AI systems been audited by an independent auditor and/or stakeholders' representatives, or other public sector bodies?	
3. How does the project envision building the AI systems that are inclusive and accessible for all users?	*For instance, whether varied abilities and disabilities have been accounted for.*
4. To what extent will decisions made through the use of AI systems be validated so as to assess that they are fair, unbiased and non-discriminatory?	
5. Do you envisage any negative social impacts of the project on relevant groups? How will these negative social impacts be prevented, detected and stopped from reoccurring?	*Please include impacts other than those arising from algorithmic bias or accessibility.*
6. To what extent do the AI systems enable system operators and end-users the ability to control and/or intervene in the basic operations of the system?	

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

7. Do the AI systems in the project provide an overview of how decisions are made and the reason behind the decisions?	*Please also include whether there are records of these decisions.*
8. To what extent can the Digital Twins accurately and realistically represent the actual?	
9. What are the expected shortcomings of the digital twins used within the Project which may lead to inaccurate representations of the buildings?	
10. Has the choice of data (both sources and types) and/or materials/sensors used within the Project been considered, specifically in relation to how these choices will impact the accuracy of the creation of digital twins in the Project?	
11. To what extent does the project implement measures to ensure that the decisions regarding energy optimisation are effectively balanced the real-world elements, the interests of diverse stakeholders and the data from the digital twins?	
12. Does the project foresee any risk of undermining the autonomy of the participants by the recommendations of the digital twins that are shaped by the project objective of energy optimisations?	*For example, to what extent will the digital twins continue to respect participants' choices regarding their energy consumption even if these choices contradict with the project objectives.*

[101] Questions on the ethics aspects are largely based on the ethics principles and requirements identified under Deliverable D12.1 as well as in various EU ethics policies including the Commission's Guidelines on Ethics By Design and Ethics of Use Approaches for Artificial Intelligence dated 25 November 2021, the Commission's Communication on European Declaration on Digital Rights and Principles for the Digital Decade dated 26 January 2022.

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

13. What considerations have been made by the project to ensure the sustainability/environmental impact of both the project and its sub-systems and the supply chain to which it connects?	*Please consider, for instance, the high energy consumption of blockchain-based systems, sustainability of the materials used to make smart devices, the lifespan of the devices to be distributed in the project etc.*

ADDITIONAL INFORMATION